

# Using BitLocker in a Higher Education Environment

Zeb Bowden, Virginia Polytechnic Institute and State University

[zbowden@vt.edu](mailto:zbowden@vt.edu)

04/20/2007

## Abstract

This paper provides an overview of a new technology included in Microsoft Windows Vista called BitLocker and how it can be used to address the threat of unintentional data disclosure, particularly in a higher education environment. A general overview of this threat is provided as well as a look at the prevalence of the threat in higher education environments. It will discuss the potential benefits of BitLocker which include data security, system integrity checking, centralized management, and Active Directory integration. The difficulties that may be introduced with BitLocker, particularly in the areas of configuration and policy management are also discussed.

In higher education environments there are additional issues that can hinder the implementation of a solution to address unintentional data disclosure. These issues include:

- The large amounts and diverse nature of the data
- Decentralized management of laptops and mobile devices
- Prevalence of newer mobile devices
- Difficulty to enforce overarching policies, such as a key escrow or data retention policy
- Lack of accountability for data security

Some of these issues are not technical in nature and therefore cannot be addressed purely with technology like BitLocker. For instance, BitLocker cannot create a key escrow policy but it will provide mechanisms to support the key escrow policy you define. This paper shows that BitLocker is flexible enough to be used effectively in environments like higher education.

## Introduction

In recent years there have been many computing advancements that have led to an improved user experience. Among these are increased security in the operating system (OS) and ease of mobility. These are welcome improvements for end users, however as devices become more mobile, their attack surface is also increased because the systems themselves are becoming physically more accessible to an attacker. If the number and frequency of security incidents involving lost or stolen laptops is any indication<sup>1</sup>, not enough effort has been focused on this additional attack vector. The increased OS security prior to Windows Vista is simply not enough to provide this protection.

As an example, OS security was improved between Windows XP Service Pack 1 and Service Pack 2<sup>2</sup>. However, there was always the caveat (spoken or not) that if the attacker has physical access to the machine then they could defeat most, if not all, of these security improvements. During the same timeframe, laptops and other portable computing devices have become more popular and easier to use. These devices are smaller and easier to carry but at the same time have actually gained storage space, memory, and processing power. This leads these devices, laptops and tablets in particular, being used as a replacement for desktop machines. It is predicted that by 2011, laptops will replace desktops as the primary form factor of computers<sup>3</sup>. Sensitive data that previously was confined to a non-portable, desktop machine can now be carried with the user wherever they go.

Stolen, misplaced, or lost laptops are not a new phenomenon. This has happened, as it has with any portable asset, since people started using laptops. Previously, the resulting cost was primarily the replacement of the hardware. The volume of information carried was relatively small and people were not using laptops for as many different tasks as they are today. As recent, highly publicized incidents have shown the cost incurred will include much more than hardware. Example incidents include the FBI<sup>4</sup>, Department of Veterans Affairs<sup>5</sup>, and numerous universities<sup>6,7</sup> and other organizations<sup>1</sup>. The power of today's laptops combined with their growing popularity increases the threat of a laptop thief stealing not only your hardware, but also your sensitive data.

With Windows Vista, Microsoft has introduced a technology called BitLocker that is aimed at preventing unauthorized data disclosure on lost or stolen laptops by encrypting all of the data on your system and by verifying the integrity of boot components. Because your data is encrypted, BitLocker is still effective when an attacker has physical access to the machine. BitLocker can also leverage Active Directory to provide centralized policy management and secure storage of related recovery information.

---

<sup>1</sup> <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

<sup>2</sup> <http://www.us-cert.gov/cas/alerts/SA04-243A.html>

<sup>3</sup> <http://news.bbc.co.uk/2/hi/technology/6474581.stm>

<sup>4</sup> <http://www.usdoj.gov/oig/reports/FBI/a0718/final.pdf>

<sup>5</sup> <http://www.usa.gov/veteransinfo.shtml>

<sup>6</sup> [http://news.com.com/UCLA+laptop+theft+exposes+ID+info/2100-1029\\_3-5230662.html](http://news.com.com/UCLA+laptop+theft+exposes+ID+info/2100-1029_3-5230662.html)

<sup>7</sup> <http://www.cnn.com/2005/TECH/03/29/stolen.laptop/index.html>

## Threat of Physical Access

It is a trivial process for an attacker to access data stored on a hard drive if they are given physical access to the drive. A variety of tools and techniques exist, both hardware and software based, to accomplish this relatively quickly. Once an attacker has physical control of a drive, strong passwords, good software security policies, firewalls, and anti-virus software are of little effect.

As laptops become increasingly smaller and more portable, it becomes easier for an attacker to steal and conceal them. The more prevalent these devices become the greater the number of opportunities an attacker will have to get to them.

The scope of this threat, in relation to this paper, is limited to data that is at rest; also known as data that is offline. It would be much more difficult for a laptop thief to steal your computer while you are actively using it. There is still a need to protect data that is in use or in transit; however that is outside of the scope of this document.

## Costs and Regulations

New government regulations<sup>89</sup> combined with the amount of negative publicity<sup>10</sup> have made the unintended disclosure of sensitive data increasingly costly. After factoring in these costs, the hardware costs become almost negligible. The government imposed fines that result from regulatory non-compliance is at least measurable<sup>11</sup>. It is extremely difficult, if not impossible, to quantify the cost of negative publicity.

According to a survey conducted by the FBI/CSI<sup>12</sup> losses from laptop or mobile hardware theft increased from \$19,562 per respondent in 2005 to \$30,057 per respondent in 2006 for a total cost of roughly \$6.6M. Those figures show the increase in popularity of mobile devices, but do not include the nearly \$17M combined cost resulting from unauthorized access to information and theft of proprietary information. Adding to the problem, most organizations do not have a good way of knowing what data actually is contained on laptops that are unaccounted for<sup>13</sup>. This results in having to treat each case as a worse case scenario and assume sensitive data has been disclosed.

Unintended data disclosure is not just the result of theft; it can also be from improper decommissioning procedures. For instance, retiring an old laptop and then reselling it. In many cases the remnants of the data previously contained on the laptop can be recovered. In 2003 two MIT graduate students recovered “significant personal information” from 49 out of 158 used hard drives they purchased on eBay<sup>14</sup>.

---

<sup>8</sup> <http://www.pgp.com/newsroom/regulations/index.html>

<sup>9</sup> <http://www.pirg.org/consumer/credit/statelaws.htm#breach>

<sup>10</sup> <http://www.msnbc.msn.com/id/17584255/>

<sup>11</sup> [http://www.consumeraffairs.com/news04/2006/01/choicepoint\\_fine.html](http://www.consumeraffairs.com/news04/2006/01/choicepoint_fine.html)

<sup>12</sup> <http://www.abovesecurity.com/doc/CommuniquesPDF/FBISurvey2006.pdf>

<sup>13</sup> <http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/08-15-2006/0004416275&EDATE>

<sup>14</sup> <http://www.detto.com/erase-hard-drive-ap-01-2003.html>

### **The Threat in Higher Education**

Institutes of higher education are faced with the same threat of unintended data disclosure similar to the industry as a whole. The real differences lie in the data that is being disclosed and the prevalence of mobile devices on campuses.

The data contained on university owned machines is extremely diverse, ranging from student medical records to governmental research documents to alumni information. The unintentional data disclosure of any of these types of data has the potential to be very damaging to any institution. It is also unlikely that these institutions do a better job of know what information is on mobile devices than the respondents of the survey noted above.

Mobile computing devices are commonly used in conjunction with wireless Internet access which is currently available on many campuses in the United States. Some universities are requiring students to use laptops or tablets in their coursework<sup>15</sup>. Faculty members are taking advantage of the increased flexibility these devices offer as well. These factors have contributed to an increase of mobile computing devices being used on campuses nationwide, a trend that is expected to continue<sup>16</sup>.

### **Combating the Threat**

One of the best ways to combat unintended data disclosure is to require more than just physical access to read the data. Encrypting the data is an effective way to enforce this because a key is required to decrypt the data in order to read it. Data encryption itself is not new, however it can introduce its own set of challenges which may hinder its adoption.

Among these challenges are:

- Deciding what to encrypt
- Accidental storing of unencrypted files (for example, offline files cache)
- Encrypting system files
- Data loss resulting from lost keys
- Securely storing the keys
- Encryption policy enforcement
- Impact on performance

In higher education environments, these challenges are amplified by issues that include:

- Large amounts and diverse nature of the data
- Laptops and mobile devices that are not centrally managed
- Prevalence of newer mobile devices

---

<sup>15</sup> <http://www.vtnews.vt.edu/story.php?relyear=2006&itemno=232>

<sup>16</sup> <http://www.educause.edu/ir/library/pdf/ERM0547.pdf>

- Difficulty to define and enforce overarching policies, such as a key escrow or data retention policy
- Lack of accountability for data security

### **BitLocker Introduction**

BitLocker is a new data protection feature introduced in Microsoft Vista (Enterprise and Ultimate versions), its primary goal is to protect data on the Windows volume of a system. BitLocker is a full drive encryption solution; it will encrypt everything on the Windows volume of your system. This means that the user does not have to make a decision about what to encrypt and it also eliminates the possibility of accidentally storing an unencrypted copy of a file. System files are also encrypted and this all occurs without modifying the user's experience. Additionally, BitLocker can perform system integrity checking at boot time to ensure that the hard drive is actually being used in the intended machine and that no boot components have been modified.

Ideally, BitLocker will be used in conjunction with a hardware component called a Trusted Platform Module (TPM) version 1.2. This is required to use the integrity checking functionality of BitLocker and also has the potential to increase the security of how the keys are stored. A TPM is like a smart card located on the system motherboard; it manages the keys used with BitLocker and also maintains the information used to verify system integrity. Many laptops and tablets on the market today are available with a compatible TPM.

For systems without a compatible TPM, a USB flash drive can be used to store the keys. The system integrity checking of BitLocker is not available without a TPM however.

BitLocker uses what is known as sector level encryption. This means that it encrypts data below the file system. Other encryption technologies, such as Encrypting File System (EFS), encrypt data at the file system level and are thus limited in their ability to encrypt certain files. This lower level of operation allows BitLocker to encrypt every file and folder in a volume, including system files, because it is not limited by the file system. The actual encryption of data by BitLocker is completely transparent to the end user. While no formal benchmarks have been published, BitLocker was designed with a requirement that the performance impact be minimal<sup>17</sup>.

BitLocker uses the AES (128 or 256 bit) encryption algorithm along with an optional Diffuser algorithm that can make the encrypted data more resilient to attacks. By default, AES 128 with Diffuser is used. For more information, Microsoft has published a paper<sup>17</sup> that discusses the actual encryption processes used by BitLocker.

### **BitLocker Prerequisites**

In order to turn on BitLocker your machine must meet two minimum requirements:

---

<sup>17</sup> <http://download.microsoft.com/download/0/2/3/0238acaf-d3bf-4a6d-b3d6-0a0be4bbb36e/BitLockerCipher200608.pdf>

1. Your computer must have two volumes for BitLocker to work: your standard operating system volume, which will be encrypted, and an additional NTFS formatted volume that is at least 1.5GB in size. This additional volume will need to be marked as “active”; it will be used to store hardware specific files (for instance the master boot record) needed to load Windows. Figure 1 below shows an example of two properly configured volumes. See [Appendix I](#) at the end of this document for more details.

<b>BITLOCKER ENCRYPTED VOLUME (C:)</b> 91.69 GB NTFS (BitLocker Encrypted) Healthy (Boot, Page File, Crash Dump, Primary Partition)	<b>UNENCRYPTED VOLUME (S:)</b> 1.5 GB NTFS Healthy (System, Active, Primary Partition)
---	--

*Figure 1: Volumes configured for BitLocker*

2. Your system BIOS must support reading and writing of USB devices.

An optional third requirement is that your system have a TPM v1.2 along with a v1.2 TCG-compliant BIOS. BitLocker can still be used without a compliant TPM; however the functionality and provided security will be reduced.

### TPM Usage

As mentioned earlier, a TPM is similar to a smart card that is physically attached to your system’s motherboard. With BitLocker, the TPM is used to protect keys and to verify that the appropriate environmental conditions are present (for instance: the BIOS has not been modified). In actuality, BitLocker does not use all of the features and functionality provided by a TPM. More information regarding the TPM can be found on the Trusted Computer Group website: <https://www.trustedcomputinggroup.org/home>.

The following conditions will need to be met before you can use a TPM with BitLocker on your system:

- The TPM must be version 1.2
- The TPM must be enabled in the BIOS
- The TPM must be activated (or turned on)
  - `Manage-bde.wsf -tpm -TurnOn`
- Ownership of the TPM must be taken
  - This requires setting an ownership password
  - `Manage-bde.wsf -TakeOwnership <password>`

Included in Windows Vista is a TPM management console, `tpm.msc`, which can be used to complete the last two tasks. Once these conditions are met, the TPM is available for use. For more detailed instructions for initializing the TPM for use with BitLocker, see [Appendix I](#) at the end of this document.

### BitLocker Keys

BitLocker utilizes several different types of keys in its operation. It is helpful to understand the primary function of each key, which is listed below:

April 20, 2007

© 2007 Zeb Bowden, Virginia Polytechnic Institute and State University. All rights reserved.

- **Startup Key:** This key is stored on a USB device that must be plugged into the machine at boot up (or return from hibernation). There are two scenarios when a startup key is required:
  - When BitLocker is configured to use a TPM + Startup key
  - When BitLocker is configured to operate in a Startup key only scenario.
- **Recovery Key:** This key is also stored on a USB device and can be used in the event a recovery operation needs to take place.
- **Full Volume Encryption Key:** BitLocker actually uses this key to encrypt the data.
- **Volume Master Key:** This key is used to protect the full volume encryption key mentioned above. This key in turn is protected by the TPM (or startup key in the event you are not using a TPM).
- **Recovery Password:** This is a 48 numerical character password that can be manually entered by a user in the event a recovery operation is needed and a recovery key is not available.

### **BitLocker Modes**

There are several different modes in which BitLocker can be used. In the standard mode it is used in conjunction with a TPM to encrypt the Windows volume and also to ensure the integrity of the boot components. No user interaction is required in this configuration; this will likely be the most common deployment mode for BitLocker.

Additional, more advanced options for deploying BitLocker are available; these include:

- **TPM + PIN:** In this configuration the user will be prompted to enter a PIN via function keys each time the system starts up or resumes from hibernation.
- **TPM + Startup Key:** In this configuration the user will need to insert a USB device that contains the startup key each time system starts up or resumes from hibernation.
- **Startup Key Only:** This configuration only provides encryption of the Windows volume; no system integrity checking is performed. The user will need to insert a USB device that contains the startup key each time system starts up or resumes from hibernation.

The standard mode of BitLocker can be configured relatively quickly once your system has the volumes configured correctly. The advanced options require additional configuration, particularly configuring the “Enable advanced startup options” policy setting. The advanced options add an additional layer of security by providing user interaction at startup; they must provide either something they have (USB device) or something they know (PIN). It is important to educate users to not keep the USB devices with their laptops or to not use 1-2-3-4 as their PIN; otherwise the additional security provided by user interaction is worthless. The PIN or USB device is not a substitute for password authentication; it is not intended as a single-sign on type of solution. In both the advanced and standard modes of BitLocker security best practices (including strong passwords) are still essential to the overall process of protecting data.

A TPM will protect against brute force PIN guessing by using a technique known as anti-hammering. This will throttle the number of allowed PIN attempts per timeframe and also will lockout the TPM if the number of failed guesses crosses the allowed threshold. This lockout period will expire and allow you to gain access to the computer so manual intervention is not required. In the event you needed to unlock the TPM immediately, you may do so through WMI after booting into the Windows Recovery Environment; an example script is included in the following article: <http://support.microsoft.com/kb/926187>. The specifics of the anti-hammering technique employed, such as lockout threshold and lockout time period will vary depending on the TPM manufacturer.

### **BitLocker Management**

One of the big benefits of using BitLocker is that it can be managed using Active Directory and Group Policy. This includes not only configuring policy settings, such as the type of encryption to use, but also securely backing up and storing recovery information used by BitLocker. This recovery information includes recovery passwords, TPM owner passwords, and recovery key packages. Recovery key packages can be used for specialized recovery, for instance to recover data on damaged drives. The backup of recovery information can be made mandatory through policy as well. This ensures that data that has been encrypted by BitLocker can be recovered by not allowing the user to change the recovery information without storing that information in Active Directory. The ability to backup this information into an established directory system such as Active Directory is extremely valuable, especially in centrally managed environments. A more detailed outline of the BitLocker and TPM settings that can be configured via group policy is included in [Appendix II](#).

More fine grained, technical management (which can be performed locally or remotely) is controlled through WMI or a script included in Vista called manage-bde.wsf. The manage-bde.wsf script actually uses the WMI providers for BitLocker and can be modified to suit your advanced configuration needs.

In Microsoft Vista Ultimate, there is also an optional component called “Secure Online Key Backup” that will allow you to store your recovery passwords in your digital locker<sup>18</sup>. This feature is available as part of an Ultimate Extra called “BitLocker and EFS Enhancements”. In short, this allows you to store your recovery password on a secure website to provide you with a backup copy that you can conveniently access. This feature is not available in the Enterprise Edition of Vista and does require administrative privileges to run.

In a higher education environment, where there are often laptops that are not centrally managed, there may be no way to force users to backup recovery information. The effective enforcement of policies that require this recovery information to be backed up will help to address this. The two backup solutions offered with BitLocker (Active Directory or Digital Locker), are not difficult to implement and require little overhead.

---

<sup>18</sup> <http://windowsmarketplace.com/content.aspx?ctId=302>



### BitLocker in Active Directory

In order to backup recovery information to the Active Directory, the schema must be extended to provide a place to store this data. Microsoft has released a package entitled “Configuring Active Directory to Back up Windows BitLocker Drive Encryption and Trusted Platform Module Recovery Information”<sup>19</sup> that contains the necessary schema extensions. In addition to extending the schema, permissions must be granted to your BitLocker enabled computers to be able to write the recovery information to their associated computer objects. This can be done manually or from a script (which can be modified) provided in the package called Add-TPMSelfWriteACE.vbs.

Other scripts are included in the package that will allow you to view the recovery information and TPM owner information. Additionally, there is an extension to the Active Directory Users and Computers management console called “BitLocker Recovery Password Viewer”. It adds a tab to computer objects that will display the recovery password information that has been backed up to AD and also a way to search for recovery password information. This extension is available through the same channels as the BitLocker Drive Preparation Tool.

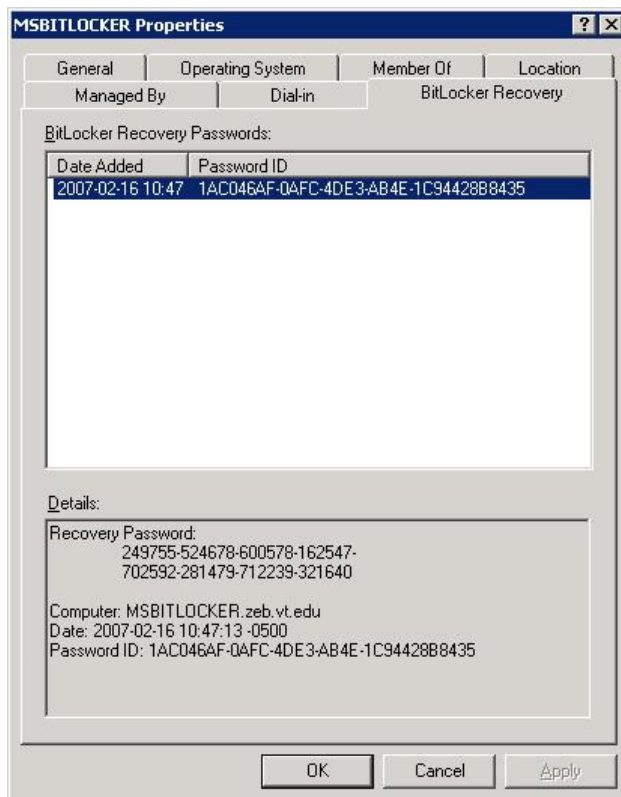


Figure 2: BitLocker Recovery Password Viewer

<sup>19</sup> <http://www.microsoft.com/downloads/details.aspx?FamilyID=3a207915-dfc3-4579-90cd-86ac666f61d4&displaylang=en>

### **Backing Up Data**

As mentioned above, recovery information can be backed up to various places: Active Directory, Digital Locker, USB devices, etc. This does not alleviate the need to have backups of the actual data that you are protecting with BitLocker. Industry best practices should still be followed to ensure that you backup important data housed on all of your machines, including ones with BitLocker enabled. Because of the level at which BitLocker operates, it should not effect or interfere with any of your backup procedures. Keep in mind however, that data stored on a BitLocker protected drive is only protected while it is stored on that drive. The backup copies of the data will be stored and transferred in clear text unless your backup client or network provides the encryption.

### **Legitimate Changes**

Situations will occur where legitimate changes are necessary that will modify the environmental conditions that the TPM verifies. For instance, a motherboard on a laptop will need to be replaced or a change in the boot manager is needed. To handle these types of situations, BitLocker needs to be disabled. After the necessary work has been performed, BitLocker can safely be re-enabled. The disabling of BitLocker does not involve actually decrypting the data, rather the data remains encrypted but the Volume Master Key (VMK) protecting it is freely available. Once BitLocker is re-enabled the volume master key is no longer freely available.

The process of making the VMK available does represent a security risk as access to that key would give the attacker the ability to access the encrypted data. Accessing the VMK is more difficult than simply reading a text file<sup>20</sup>. In fact the VMK is not actually stored in clear text on the system. Instead it is symmetrically encrypted with another key, known as a clear key. This clear key is stored in clear text, in the metadata of the unencrypted volume. This does not provide an impenetrable security boundary for the VMK, however it does provide an extra layer of protection that an attacker would need to overcome.

### **Damaged Drives**

In the event a BitLocker encrypted drive becomes damaged or other circumstances prevent BitLocker from working, Microsoft does have a tool that may help recover the data. The tool is called the BitLocker Repair Tool and it is available, along with detailed instructions here: <http://support.microsoft.com/kb/928201/en-us>. This tool does not bypass the security of BitLocker in any way; you will still need to have either the recovery password or recovery key package in order to repair the data.

### **Attacks Against BitLocker**

BitLocker, when used with a TPM, provides a hardware and software key management solution. This gives a higher level of protection than traditional software-only key

---

<sup>20</sup> <http://download.microsoft.com/download/a/f/7/af7777e5-7dcd-4800-8a0a-b18336565f5b/BitLockerFlow.doc>

management. While there still may be vulnerabilities discovered with BitLocker<sup>21</sup> or TPMs, more than likely they will be hardware based and require specialized tools and an advanced level of knowledge. These types of attacks would be atypical of the majority of the software based attacks we see today and would likely be unable to be preformed by the average laptop thief. Potentially the attacker could image the drive and store the data in hopes that an exploit or vulnerability in BitLocker will become available in the future.

Currently low level partition editing tools such as GParted<sup>22</sup> do not recognize BitLocker encrypted volumes. It is possible for tools such as these to properly make this detection<sup>23</sup>. Simply detecting BitLocker does not defeat the encryption or security that it provides.

### **BitLocker Initial Configuration Difficulties**

The initial configuration of BitLocker is a process; it is not a simple wizard or checkbox. To make this process easier, Microsoft has released a Drive Preparation Tool (<http://support.microsoft.com/kb/930063>). This tool automates the process of creating the additional volume required for BitLocker on an individual machine. Utilizing the new Windows Imaging technologies<sup>24</sup> can help to reduce the cost and time of the initial deployment by giving you the ability to have the volumes configured for BitLocker in your deployment images. As mentioned previously, the manage-bde.wsf script can be run remotely which can help speed the configuration of BitLocker once the drives have been configured.

### **BitLocker Policy Details**

Many of the policy settings that you can configure for BitLocker will not be effective immediately, they will require additional steps. For instance, if you change the encryption algorithm, the data that has already been encrypted has to be decrypted and subsequently re-encrypted with the new algorithm. This does not happen automatically; it does not become effective unless you turn off BitLocker, decrypt the drive, and then turn BitLocker back on, re-encrypting the drive with the new encryption algorithm. Along these same lines, recovery passwords are not backed up to Active Directory unless a new recovery password is created, simply configuring that policy will not initiate a backup. Other policy settings, such as requiring a TPM + PIN, merely affect the user's interface when turning BitLocker on. These settings will take effect immediately. [Appendix II](#) contains detailed descriptions of the policy settings available for configuring BitLocker and TPMs.

### **BitLocker on non-Windows volumes**

BitLocker is not supported on volumes other than the Windows volume of your system. This will be supported in Longhorn Server. It is also possible, though not officially supported by Microsoft, to configure your Vista clients to encrypt other volumes with the

---

<sup>21</sup> <http://conference.hackinthebox.org/hitbsecconf2006kl/materials/DAY 2 - Douglas MacIver - Pentesting BitLocker.pdf>

<sup>22</sup> <http://gparted.sourceforge.net/>

<sup>23</sup> [http://blogs.msdn.com/si\\_team/archive/2006/10/26/detecting-bitlocker.aspx](http://blogs.msdn.com/si_team/archive/2006/10/26/detecting-bitlocker.aspx)

<sup>24</sup> <http://technet.microsoft.com/en-us/windowsvista/aa905068.aspx>

use of the `manage-bde.wsf` script: `manage-bde.wsf -on e: -recoveryPassword -recoveryKey <USB drive letter>`. By default the other volumes will not be automatically available when the system boots so they will need to be configured to “auto unlock”:  
`manage-bde.wsf -autounlock -enable e:`.

### **Working with EFS**

While BitLocker may not be supported on other volumes in Vista, Encrypting File System (EFS) is. BitLocker compliments EFS quite well by adding protection to the EFS keys (which are stored on the Windows volume). EFS is a relatively mature technology that has been improved in Vista. While these improvements are outside of the scope of this document, it should be noted that EFS can provide data encryption for systems with additional data volumes. This is the Microsoft recommended method for providing maximum data protection<sup>25</sup>.

---

<sup>25</sup> [http://www.microsoft.com/technet/windowsvista/security/protect\\_sensitive\\_data.aspx#EGJAC](http://www.microsoft.com/technet/windowsvista/security/protect_sensitive_data.aspx#EGJAC)

## **Conclusion**

As portable computing devices continue to become smaller and more prevalent the need to secure the data on these devices will become increasingly important. The use of data encryption is an effective way to prevent unintentional disclosure of offline data.

BitLocker provides a good way to not only implement data encryption but also to ensure the integrity of the system at boot. In addition, because it is a seamless full disk encryption solution, the user is not required to make the decision of what to encrypt nor are they required to change their behavior when using their computers. The backup of recovery information and configuration options make BitLocker an attractive solution in higher education environments. This allows for flexibility while still providing a mechanism for addressing common problems encountered with a data encryption solution.

## Appendix I: Walkthrough of Enabling BitLocker

This walkthrough is provided as a guide to enable BitLocker on a “fresh” install of Vista on a system with a TPM v. 1.2.

1. Configure a group policy object with the settings you would like to use for BitLocker, see Appendix II for details on these configurations.
2. Join the machine to your domain. This needs to be done at this time in order for the policies you configured above to take effect.
3. Initialize the TPM. The process of turning on and taking ownership of the TPM is referred to as the initialization. The initialization requires that you are physically present at the machine to complete. These steps may vary depending on your BIOS.
  - a. Ensure that the TPM is not disabled or hidden in the BIOS
  - b. Activate, or turn on, the TPM in Vista by either:
    - i. The TPM Initialization Wizard: `tmp.msc` → Action → Initialize TPM
    - ii. `Manage-bde.wsf -tpm -TurnOn`
  - c. You should be prompted to shutdown the system. After your machine powers down, turn it back on and follow the instructions presented by the BIOS to complete the activation.
  - d. Take ownership of the TPM by either:
    - i. If you used the `tpm.msc` to initialize the TPM, the TPM Initialization Wizard should start automatically upon reboot. It is recommended that you select to “Automatically create the password” and that you save the password to removable media and print a hard copy.
    - ii. `Manage-bde.wsf -TakeOwnership <password>`
4. Prepare your drive. You will need to create a new NTFS primary partition to use BitLocker. This partition will be used to boot the system and will remain unencrypted. It must be 1.5GB or greater in size and set as the active partition.
  - a. Use BitLocker Drive Preparation Tool
  - b. Use the `diskpart` utility from the System Recovery command prompt after booting from a Vista DVD. These commands can be scripted and stored on a USB device.
5. Turn BitLocker on. These steps and the associated GUI display may be different depending on your BitLocker policy settings (for example: you may have disabled the ability to store recovery passwords). You will want to have at least one USB device to store the recovery key and/or password.
  - a. If using BitLocker in standard mode (uses TPM, no user interaction):
 

**Command Line Method:**

    - i. `manage-bde.wsf -on c: -recoveryPassword -recoveryKey <USB drive letter>`
    - ii. Record the recovery password displayed.
    - iii. Reboot your computer to complete the hardware test. You should run the hardware test to make sure your computer can successfully read the recovery key at start up. If you would like to avoid this reboot and the hardware test you can add an `-SkipHardwareTest` parameter to the end of the above command.

**BitLocker Control Panel Applet Method**

- i. Open the BitLocker Control Panel Applet: Start → Control Panel → Security → BitLocker Drive Encryption (supply information for UAC prompt)
- ii. Click “Turn On BitLocker”
- iii. Select “Use BitLocker without additional keys” ([Figure I-1](#))
- iv. Select “Save Password to USB drive” (select the appropriate device when prompted). Then Press Next ([Figure I-2](#))
- v. Assure that the “Run BitLocker system check” box is checked ([Figure I-3](#)) and press continue. Reboot your system, assuming your system passed the system check; BitLocker will begin to encrypt the drive.

b. If using BitLocker with a TPM and PIN

**Command Line Method:**

- i. `manage-bde.wsf -on c: -TPMandPIN <numerical PIN> -recoveryPassword -recoveryKey <USB drive letter>:\`
- ii. Record the recovery password displayed.
- iii. Reboot your computer to complete the hardware test. You should run the hardware test to make sure your computer can successfully read the recovery key at start up. If you would like to avoid this reboot and the hardware test you can add an `-SkipHardwareTest` parameter to the end of the above command.

**BitLocker Control Panel Applet Method**

- i. Open the BitLocker Control Panel Applet: Start → Control Panel → Security → BitLocker Drive Encryption (supply information for UAC prompt)
- ii. Click “Turn On BitLocker”
- iii. Select “Require PIN at every startup” ([Figure I-1](#))
- iv. Enter and confirm a PIN between 4-20 numerical characters ([Figure I-4](#))
- v. Select “Save Password to USB drive” (select the appropriate device when prompted). Then Press Next ([Figure I-2](#))
- vi. Assure that the “Run BitLocker system check” box is checked ([Figure I-3](#)) and press continue. Reboot your system, assuming your system passed the system check; BitLocker will begin to encrypt the drive.

c. If using BitLocker with TPM and a Startup Key

**Command Line Method**

- i. `manage-bde.wsf -on c: -recoveryPassword -recoveryKey <USB drive letter>:\ -TPMandStartupKey <USB drive letter>:\`
- ii. Ideally you would want to place the startup key and recovery key on different USB devices. You can do this by using two USB devices when you run this command or by moving one of the keys to a different device, the file names are listed in the output of the above command.

- iii. Record the recovery password displayed.
- iv. Reboot your computer to complete the hardware test. You should run the hardware test to make sure your computer can successfully read the startup key (and recovery key) at start up. If you would like to avoid this reboot and the hardware test you can add an – SkipHardwareTest parameter to the end of the above command.

**BitLocker Control Panel Applet Method**

- i. Open the BitLocker Control Panel Applet: Start → Control Panel → Security → BitLocker Drive Encryption (supply information for UAC prompt)
- ii. Click “Turn On BitLocker”
- iii. Select “Require Startup USB key at every startup” ([Figure I-1](#))
- iv. Select the appropriate device and press Save ([Figure I-5](#))
- v. Select “Save Password to USB drive” (select the appropriate device when prompted). Then Press Next ([Figure I-2](#))
- vi. Assure that the “Run BitLocker system check” box is checked ([Figure I-3](#)) and press continue. Reboot your system, assuming your system passed the system check; BitLocker will begin to encrypt the drive.

- d. If using BitLocker with just a Startup Key

**Command Line Method**

- i. `manage-bde.wsf -on c: -startupKey <USB drive letter>:\ - recoveryPassword -recoveryKey <USB drive letter>:\`
- ii. Ideally you would want to place the startup key and recovery key on different USB devices. You can do this by using two USB devices when you run this command or by moving one of the keys to a different device, the file names are listed in the output of the above command.
- iii. Record the recovery password displayed.
- iv. Reboot your computer to complete the hardware test. You should run the hardware test to make sure your computer can successfully read the startup key (and recovery key) at start up. If you would like to avoid this reboot and the hardware test you can add an – SkipHardwareTest parameter to the end of the above command.

**BitLocker Control Panel Applet Method**

- i. Open the BitLocker Control Panel Applet: Start → Control Panel → Security → BitLocker Drive Encryption (supply information for UAC prompt)
- ii. Click “Turn On BitLocker”
- iii. Select “Require Startup USB key at every startup” ([Figure I-6](#))
- iv. Select the appropriate device and press Save ([Figure I-5](#))
- v. Select “Save Password to USB drive” (select the appropriate device when prompted). Then Press Next ([Figure I-2](#))
- vi. Assure that the “Run BitLocker system check” box is checked ([Figure I-3](#)) and press continue. Reboot your system, assuming



your system passed the system check; BitLocker will begin to encrypt the drive.

6. BitLocker should now be in the process of encrypting the drive. You can check the status of the encryption by hovering over or clicking the BitLocker icon in the system tray ([Figure I-7](#)). During this process you should be able to use your computer as you normally would; you can even shut it down or reboot, BitLocker is able to handle that.

## Appendix II: BitLocker Group Policy Configuration

Rather than display these configuration options in the order they are listed in the group policy configuration, I have ordered them according to the functions they control.

Group policy settings for BitLocker are stored in:

Computer Configuration → Administrative Templates → Windows Components → BitLocker Drive Encryption

1. GUI changes: These settings will affect the way the BitLocker control panel applet is displayed to the user and the options that are available.
  - a. Control Panel Setup: Configure recovery folder
    - i. This setting allows you to specify the default location displayed to the user when selecting the location to store the recovery key. The user will have the option to change this location.
  - b. Control Panel Setup: Enable advanced startup options
    - i. This is where you can configure which of the advanced modes of BitLocker you would like to use. This allows you to require, disallow, or make optional the use of a startup key or PIN. It also allows you to configure BitLocker to be used without a TPM, in a startup key only mode.
2. Security changes: These settings allow you to control the level of security used by BitLocker.
  - a. Configure encryption method
    - i. Here you can configure to use AES 128 (with or without diffuser) or AES 256 (with or without diffuser). If you change this setting after BitLocker is already enabled for a drive, you will have to decrypt the drive and re-encrypt it for the change to take effect; this will not happen automatically.
  - b. Prevent memory overwrite on restart
    - i. By default, or if you configure this option to disabled, Vista will overwrite memory when you reboot the system to provide additional protection of your BitLocker keys. If you enable this option, you may see increased performance in the speed of reboots.

3. Recovery Information: These settings control where and what recovery information is stored.
  - a. Turn on BitLocker backup to Active Directory Domain Services
    - i. This setting allows you to require backup of recovery information to Active Directory and also to specify what recovery information to backup. Your options for recovery information are: only the recovery password or the recovery password and key packages. If you require the backup of recovery information then you will only be allowed to change the recovery password if the backup succeeds. If you enable this option after BitLocker has already been enabled, the recovery information will not be backed up until a new recovery password is created. This will not happen automatically.
  - b. Control Panel Setup: Configure recovery options
    - i. This setting allows you to require or disallow recovery keys and recovery passwords. By default both are required.
4. TPM validation: This setting controls how the TPM validates the environment it is in.
  - a. Configure TPM platform validation profile
    - i. This setting allows you to configure the environmental settings verified by the TPM each time the system starts (or returns from hibernation). There are twelve options, one of which is required to use BitLocker (PCR 11 – BitLocker access control). By default, seven of these registers are used.

Group policy settings for TPM configuration are stored in:  
Computer Configuration → Administrative Templates → System → Trusted Platform Module Services.

1. TPM backup information: This setting controls the backup of the TPM owner password.
  - a. Turn on TPM backup to Active Directory Domain Services
    - i. This setting allows you to disable, enable, or require the backup of the hashed TPM owner password. If this is set to required, the TPM owner password cannot be changed unless the backup is successful.
2. TPM command control: These settings control what commands the TPM will be allowed from Windows.
  - a. Configure the list of blocked TPM commands
    - i. This allows you to create a list of blocked TPM commands.
  - b. Ignore the default list of blocked TPM commands
    - i. Vista includes a list of commands that are blocked by default; this setting allows you to turn those off.
  - c. Ignore the local list of blocked TPM commands.

- i. This setting allows you to over-ride the list of locally blocked TPM commands.

### Appendix III: Screen Captures

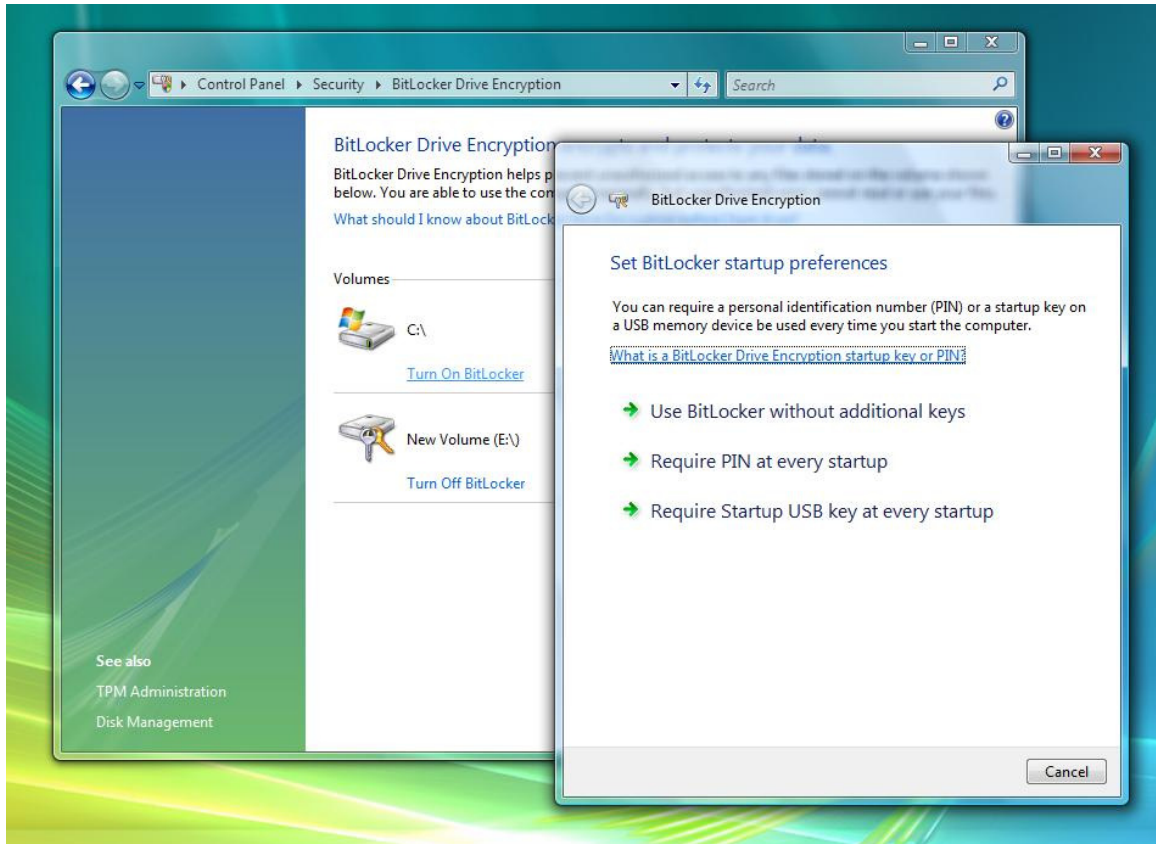


Figure I-1: Select Startup Options for BitLocker



Figure I-2: Select Location to Save Recovery Password

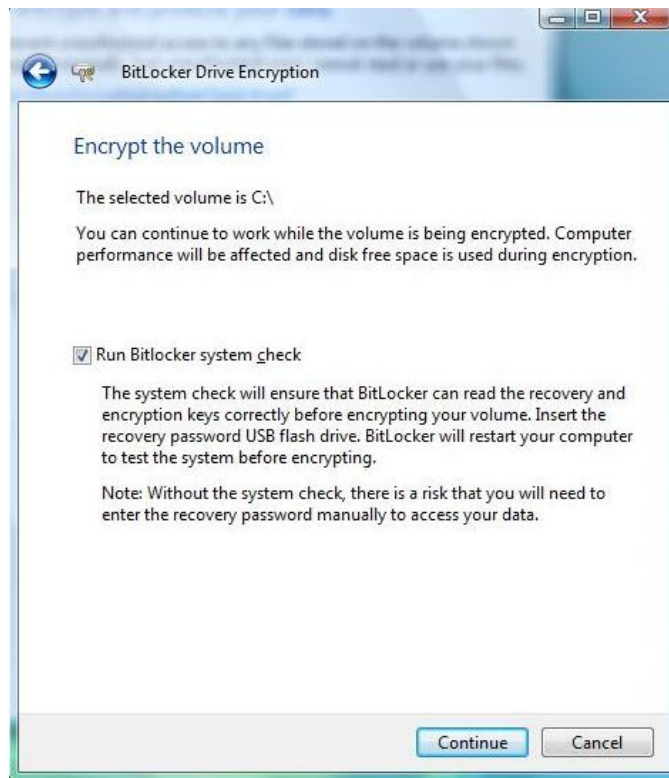


Figure I-3: BitLocker System Check

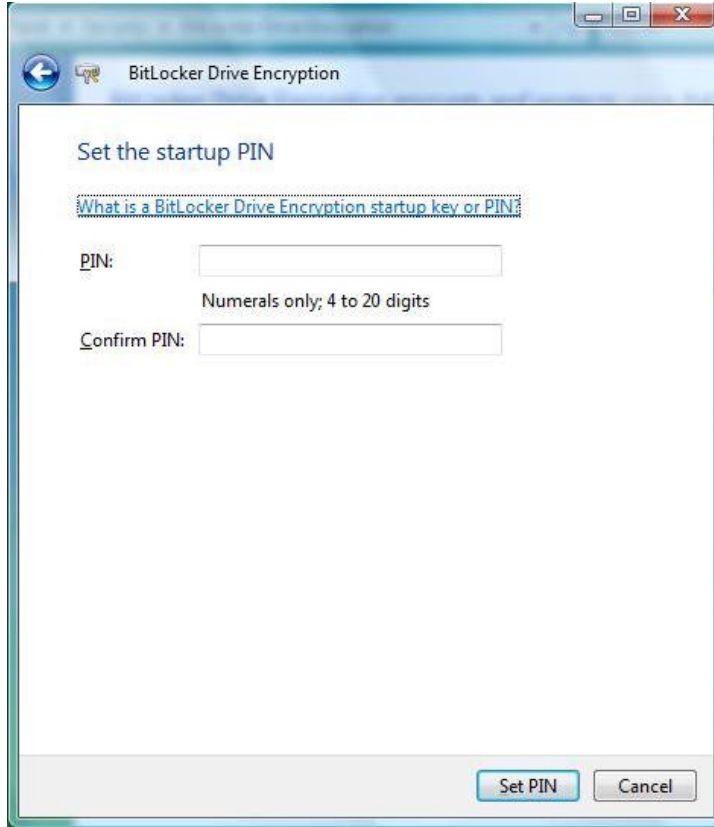


Figure I-4: Enter and Confirm PIN



Figure I-5: Select Device to Store Startup Key

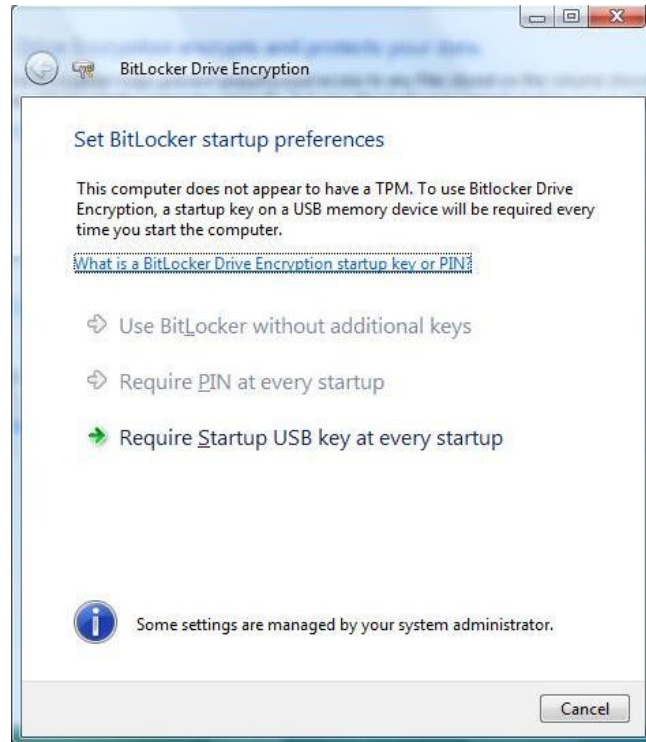


Figure I-6: No TPM, use Startup Key



Figure I-7: BitLocker Drive Encryption in Progress