Microsoft | Services

Introduction to BitLocker FVE

(Understanding the Steps Required to enable BitLocker)

Exploration of Windows 7
Advanced Forensic Topics – Day 3

Microsoft | Services

What is BitLocker?

BitLocker Drive Encryption is a full disk encryption feature included with Microsoft's Windows Vista Ultimate, Windows Vista Enterprise, Windows Server 2008, Windows 7 Ultimate, and Windows 7 Enterprise operating systems designed to protect data by providing encryption for entire volumes. By default it uses the AES encryption algorithm with a 128 bit key, combined with a diffuser for additional disk encryption specific security not provided by AES.

Why Bitlocker Exists

"Some of the largest and medium-sized U.S. airports report close to 637,000 laptops lost each year, according to the Ponemon Institute survey released Monday"
– PC World June 2008

"More than 100 USB memory sticks, some containing secret information, have been lost or stolen from the Ministry of Defense since 2004, it has emerged."
– BBC News July 2008

Microsoft | Services

BitLocker Requirements

- Windows 7 Enterprise or Ultimate
- TPM Chip version 1.2 or later (and/or) a BIOS capable of reading USB devices pre-boot

Microsoft | Services

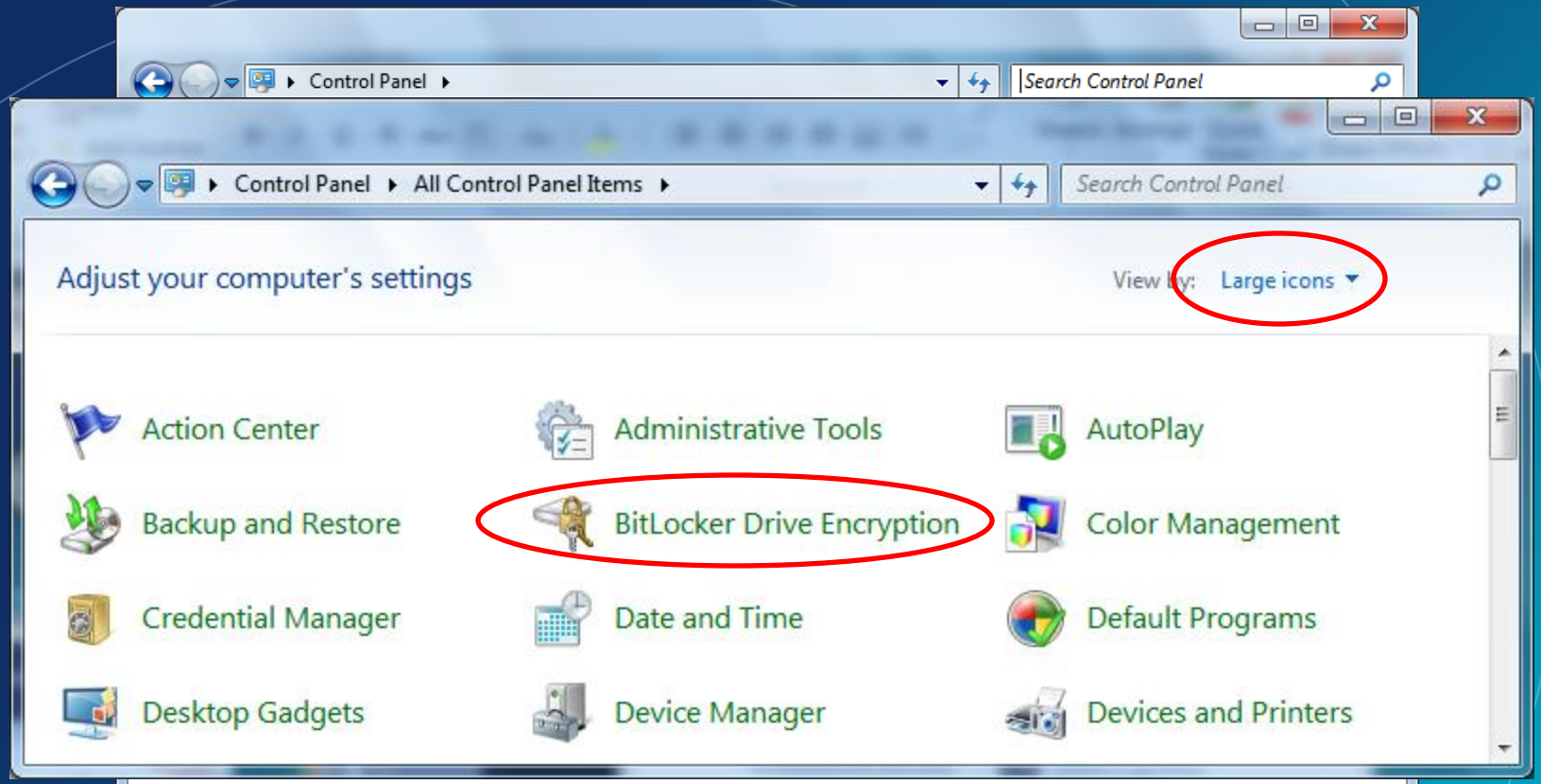
BitLocker Requirements

- BitLocker Installation
  - Operating System Installation
  - OPTIONAL: If not using TPM, edit Group Policy to allow USB key storage
  - Enabling of BitLocker and Volume Encryption

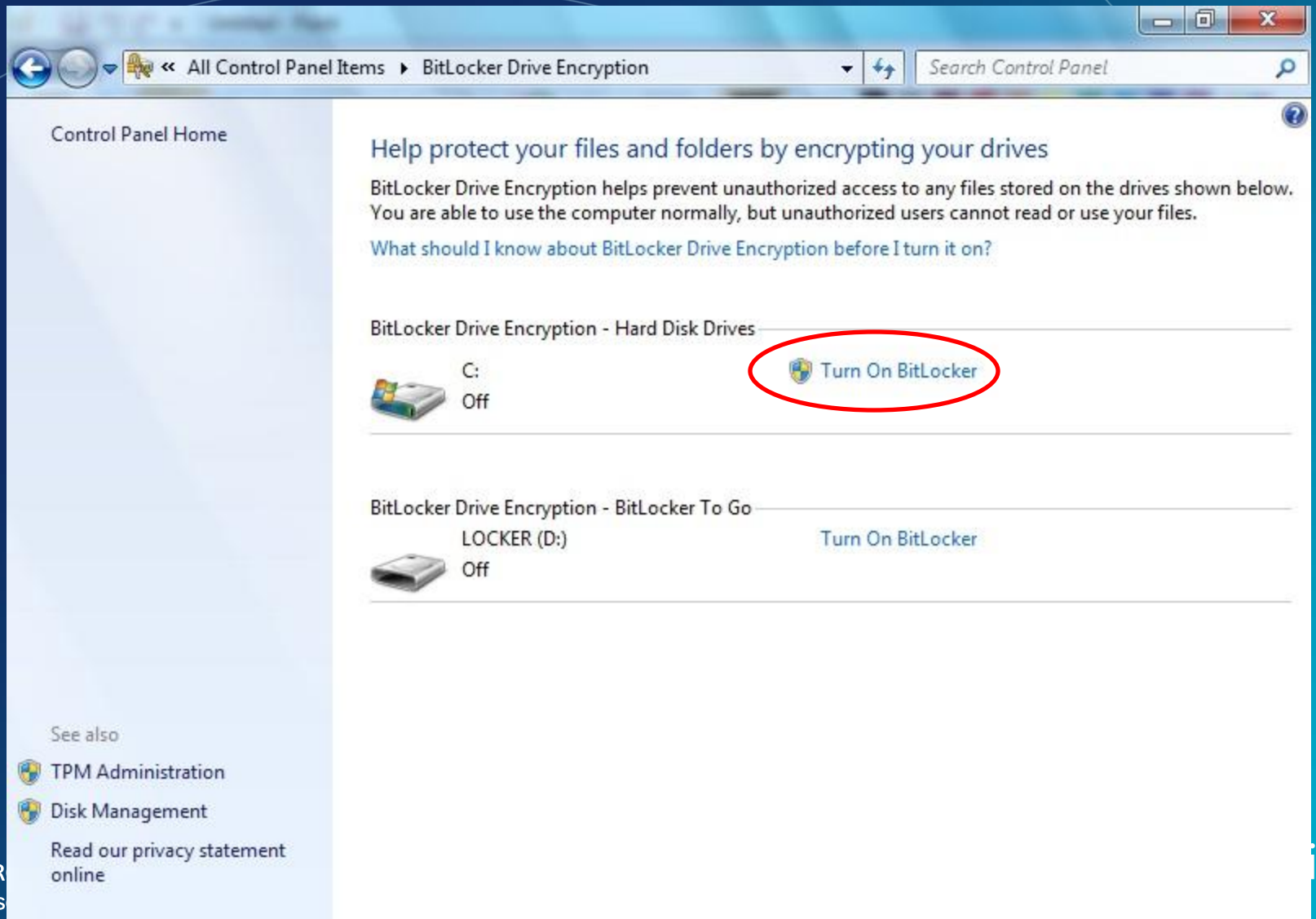
Enabling OS BitLocker via USB Key

Microsoft | Services

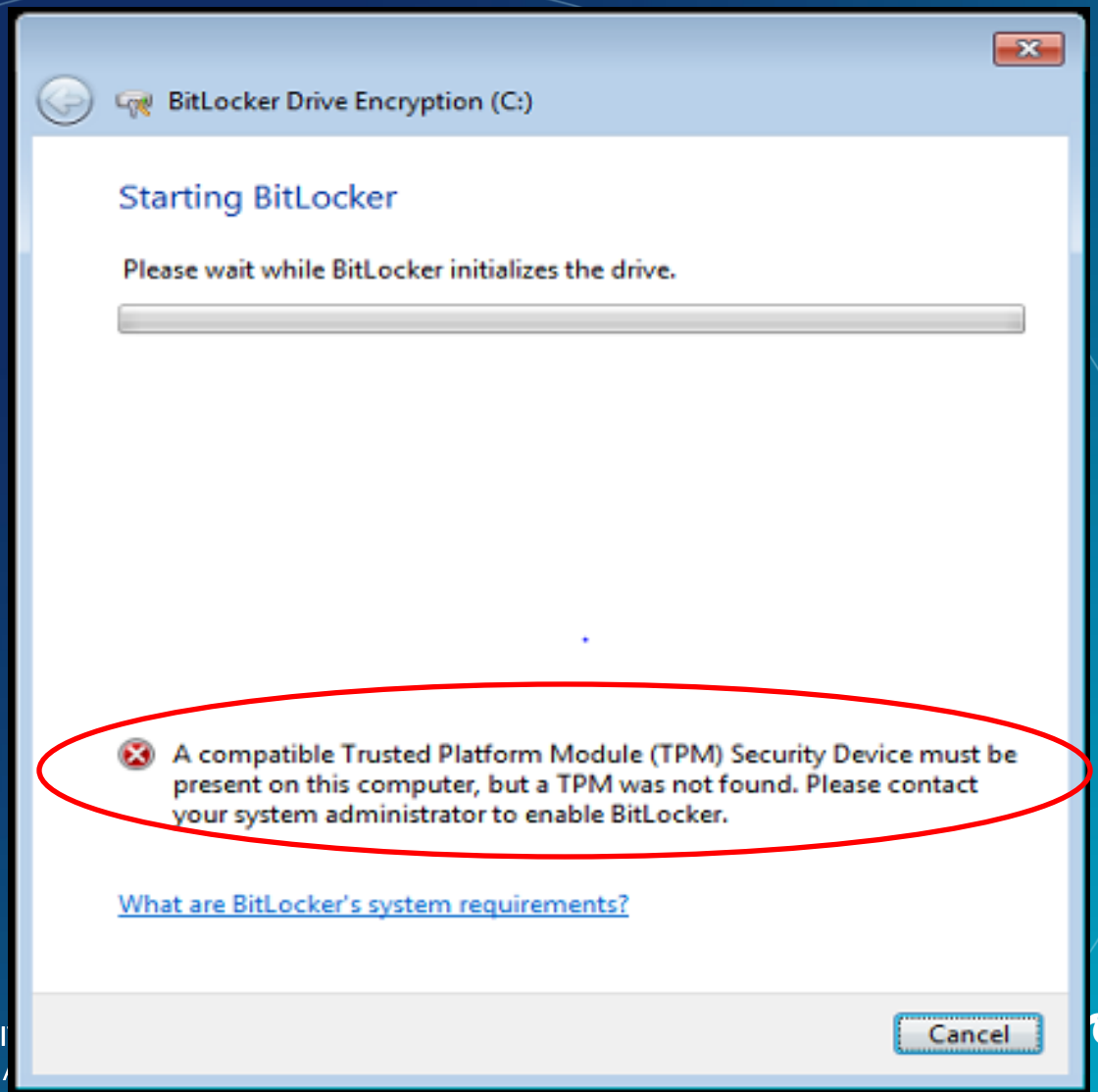
Enabling BitLocker - OS



Enabling BitLocker - OS



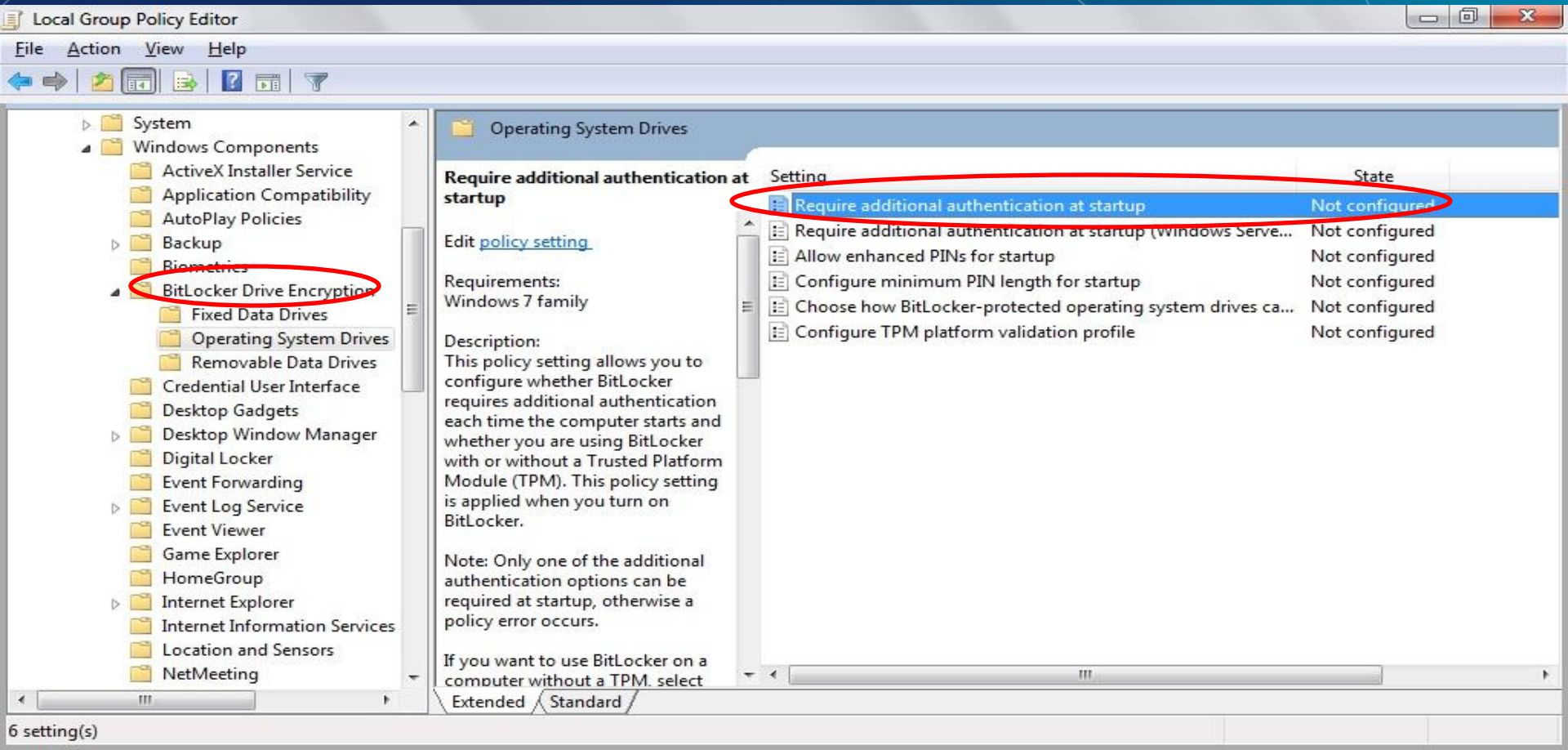
Enabling BitLocker - OS



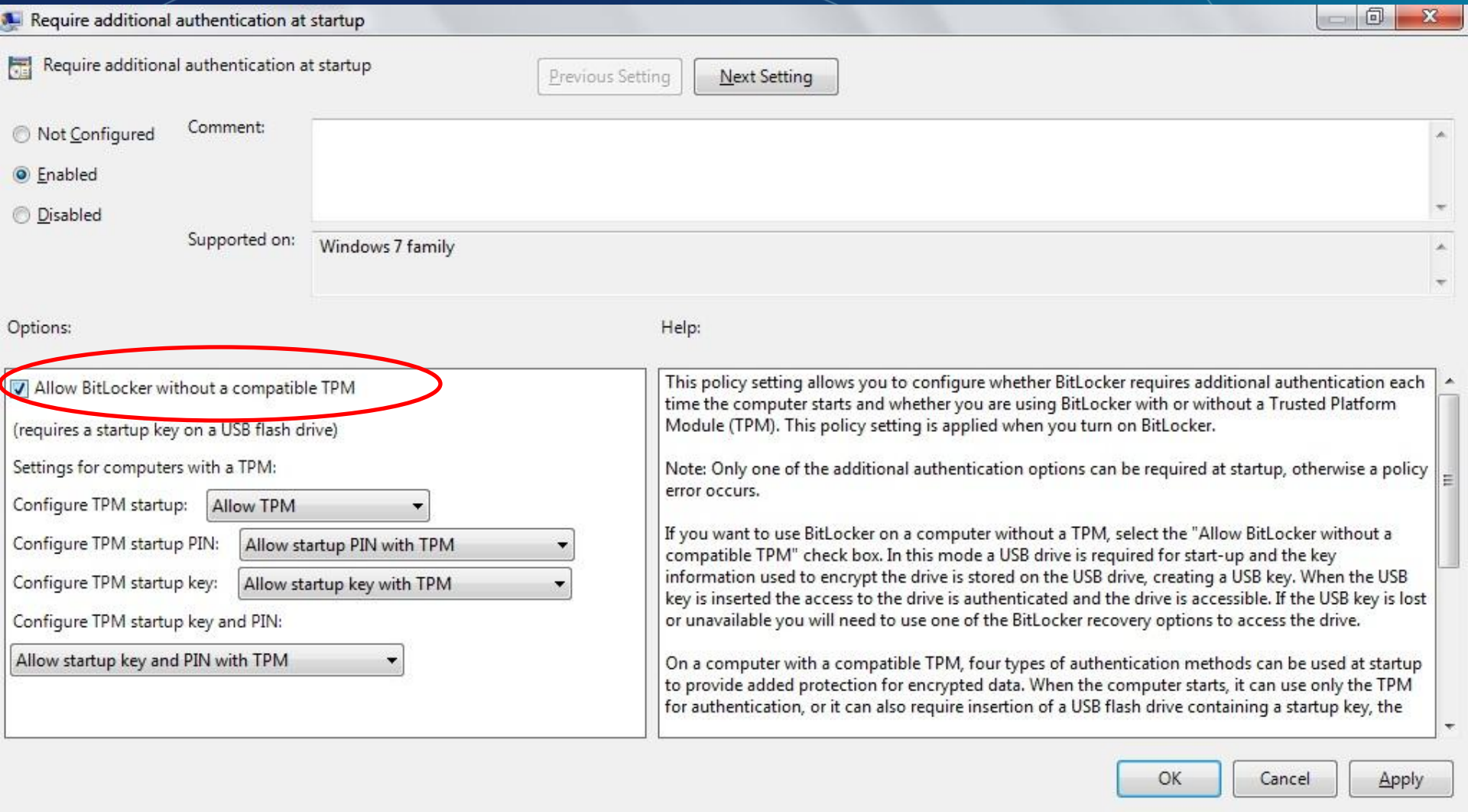
Enabling BitLocker - OS

Execute: gpedit.msc

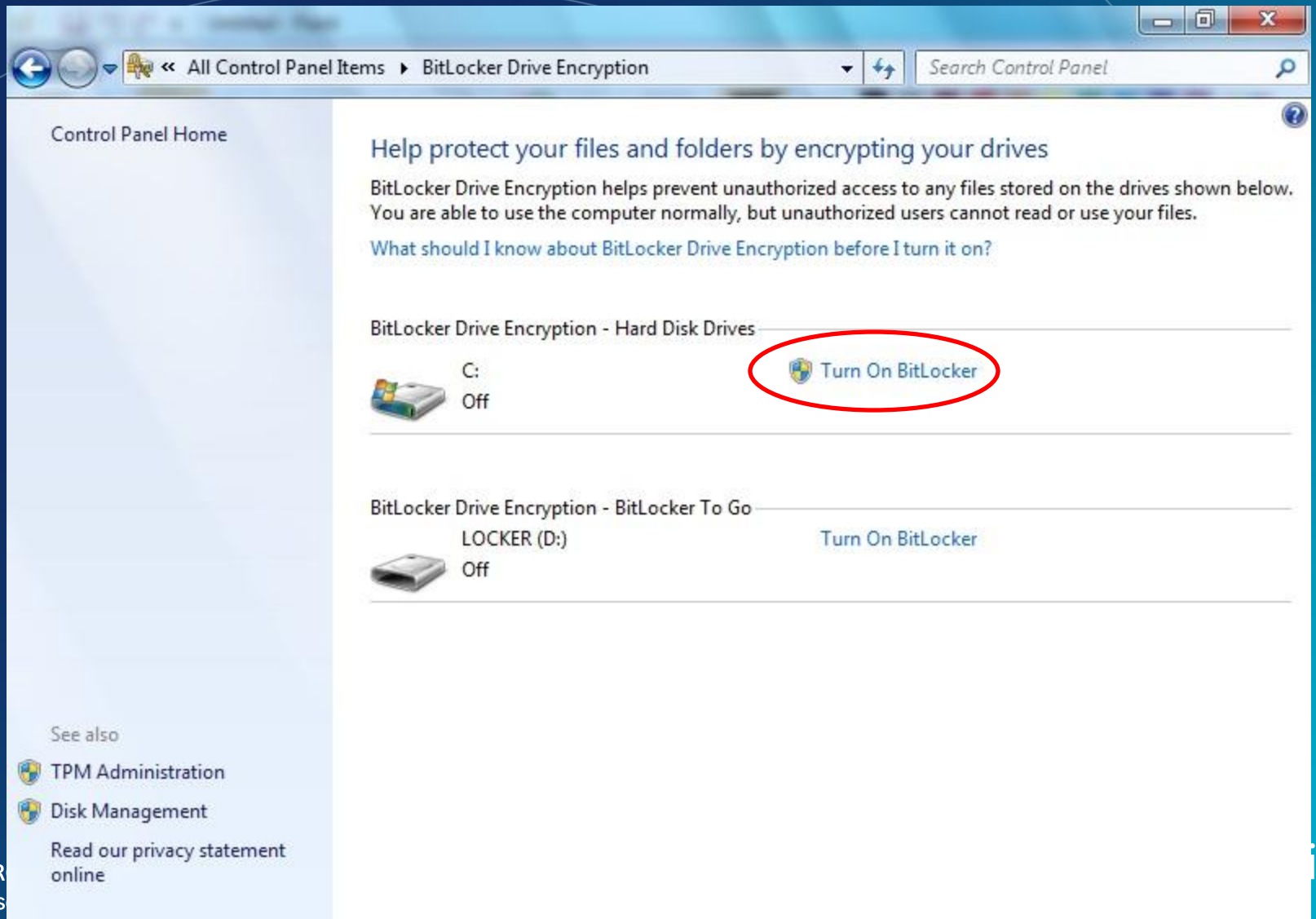
Navigate: Computer Configuration\Administrative Templates\Windows Components



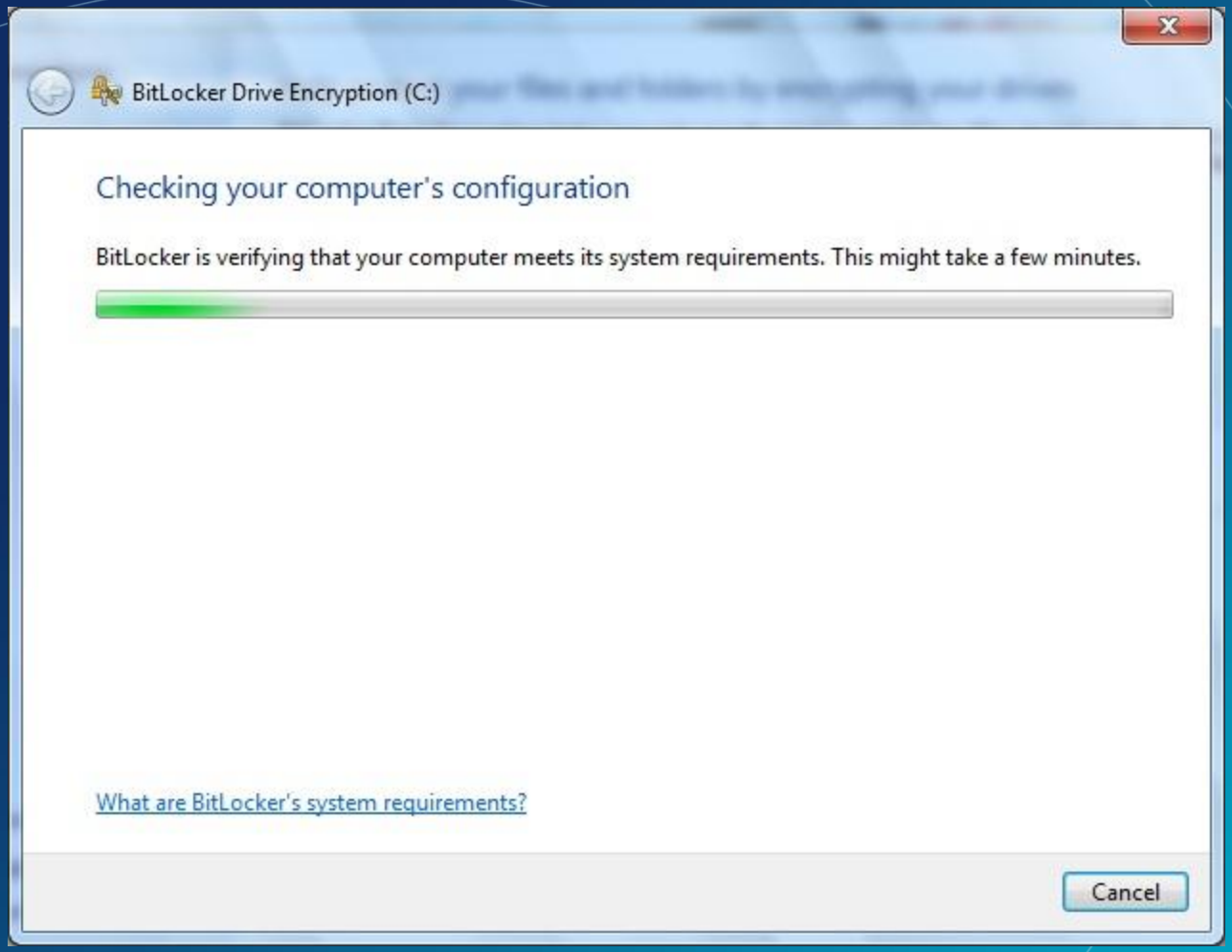
Enabling BitLocker – OS



Enabling BitLocker - OS

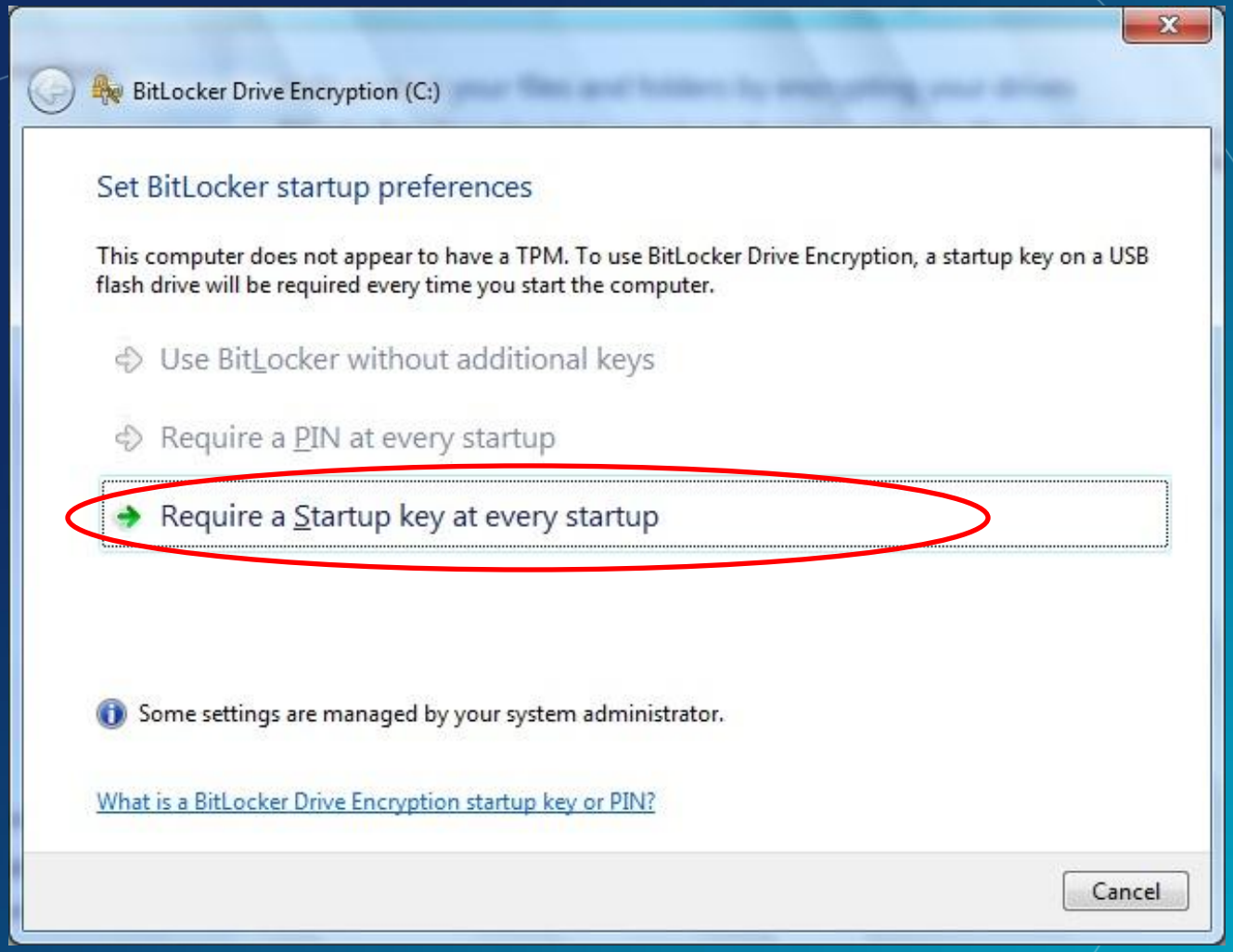


Enabling BitLocker - OS



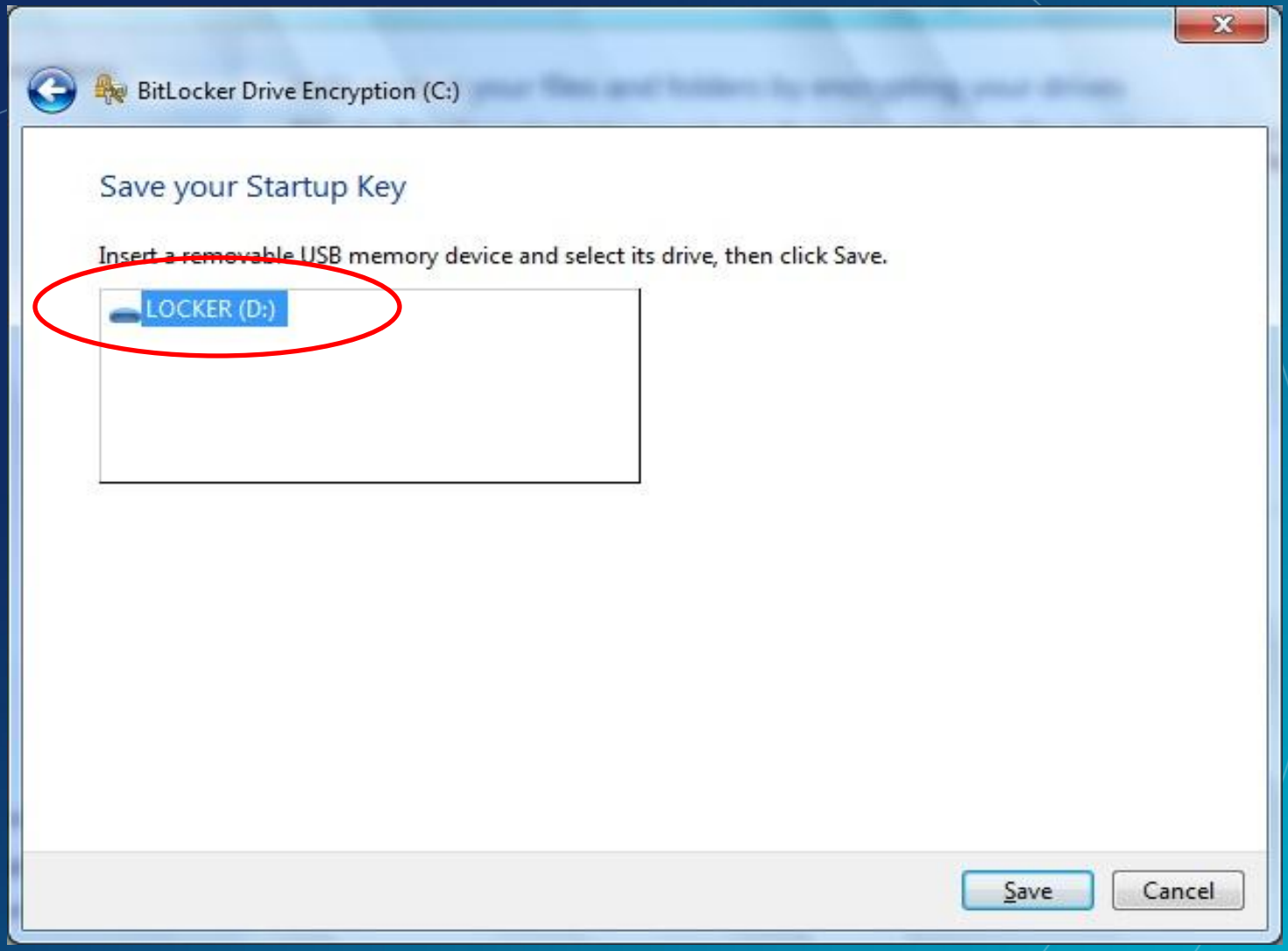
Microsoft | Services

Enabling BitLocker - OS



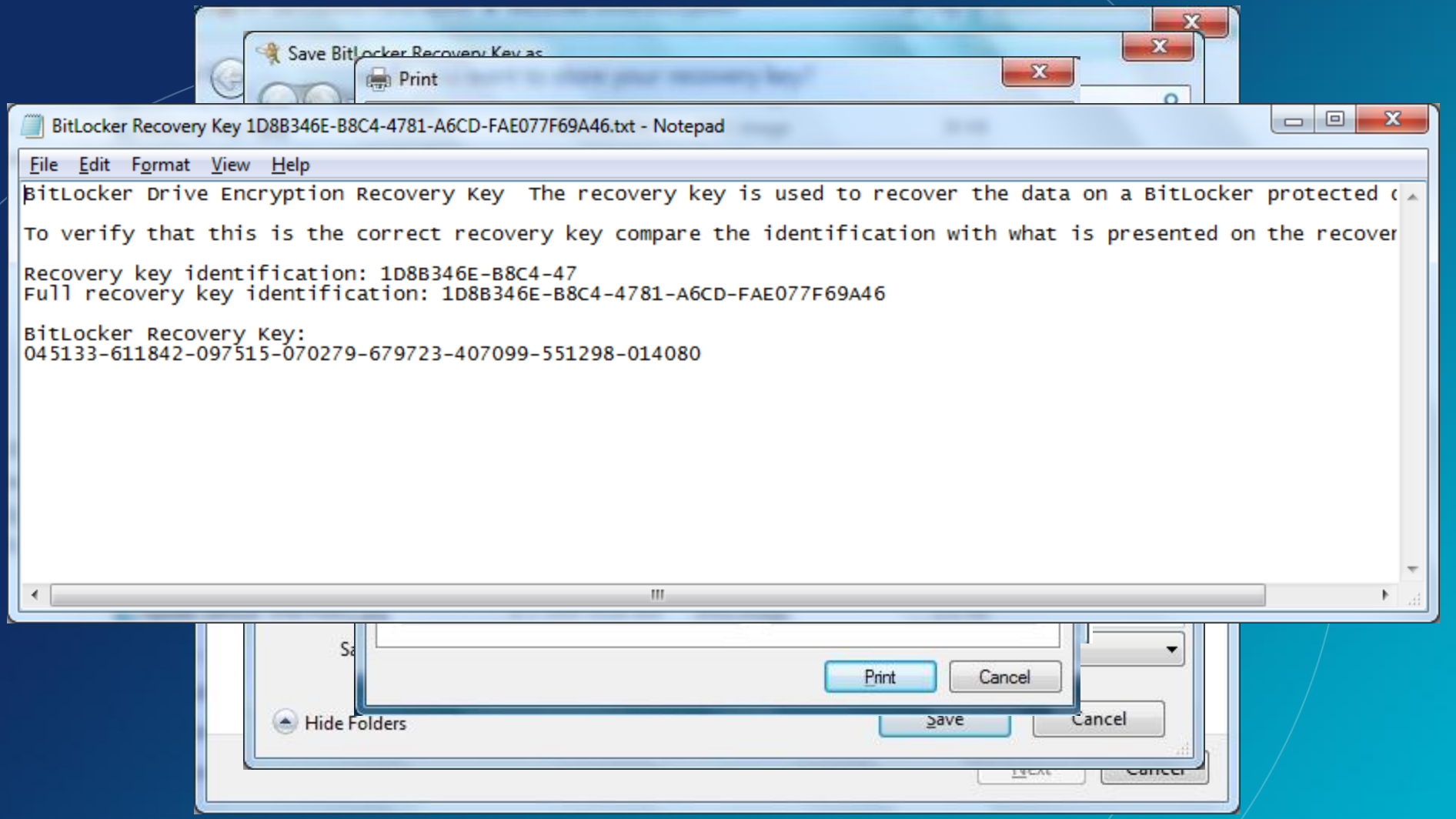
Microsoft | Services

Enabling BitLocker - OS



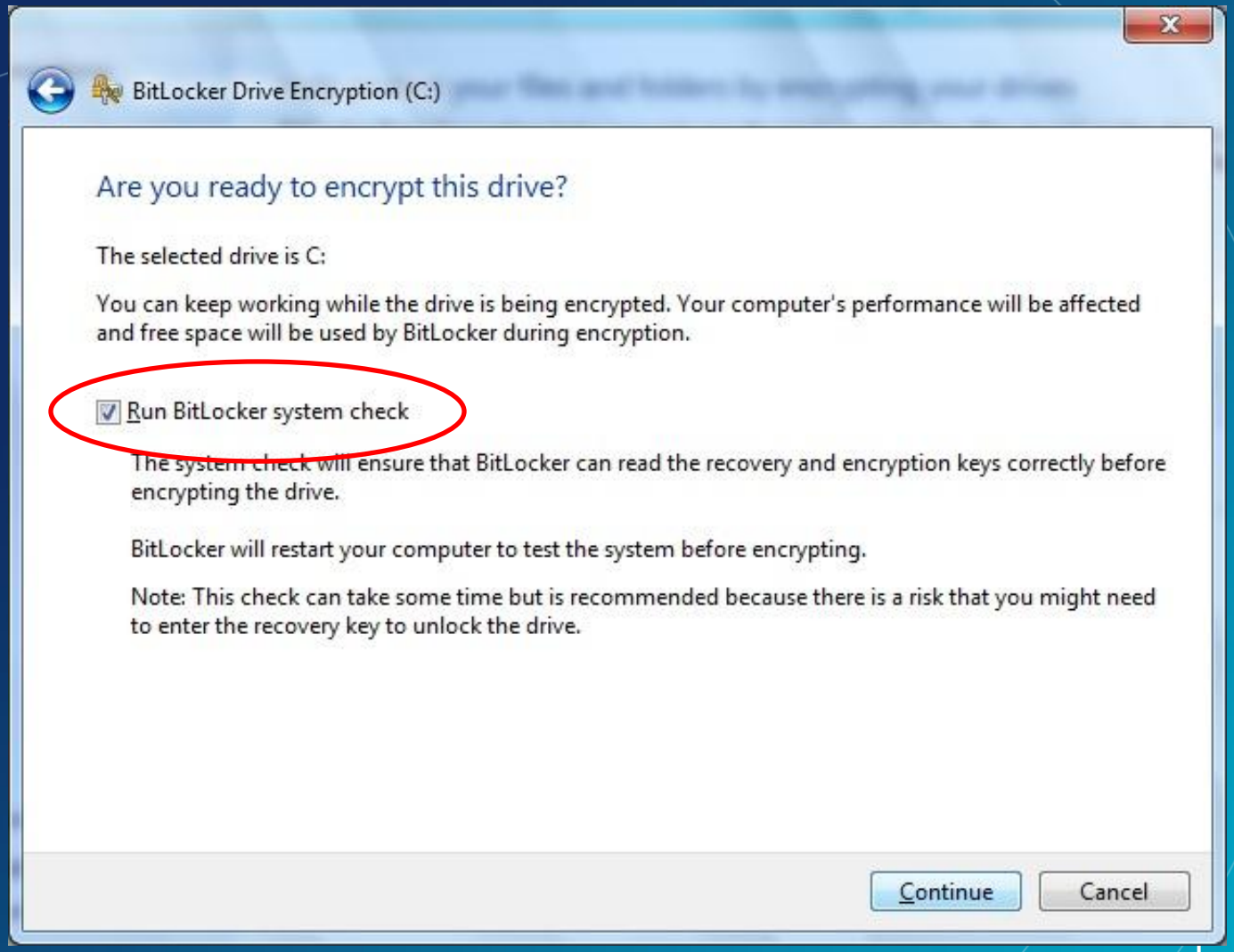
Microsoft | Services

Enabling BitLocker - OS



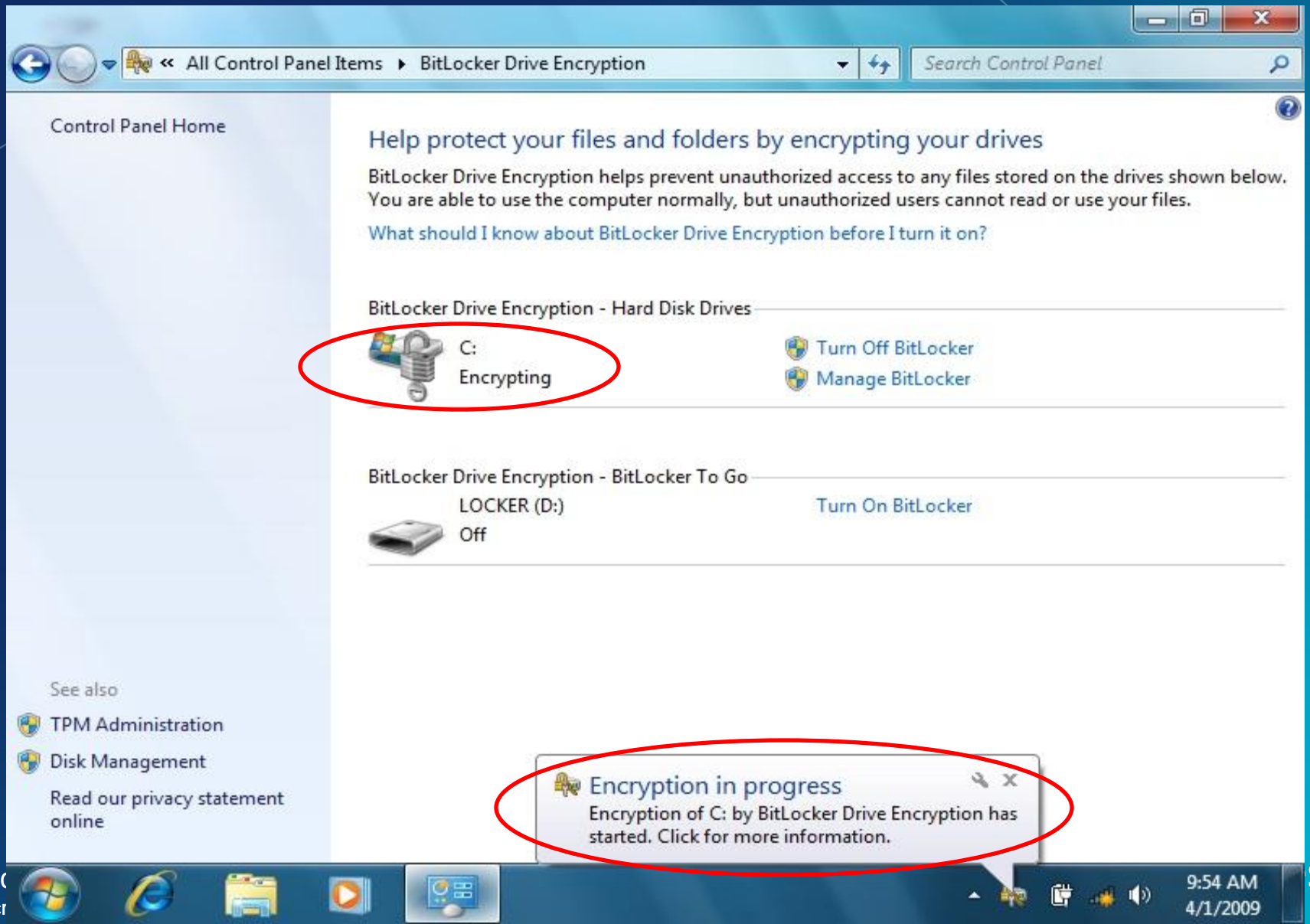
Microsoft | Services

Enabling BitLocker - OS

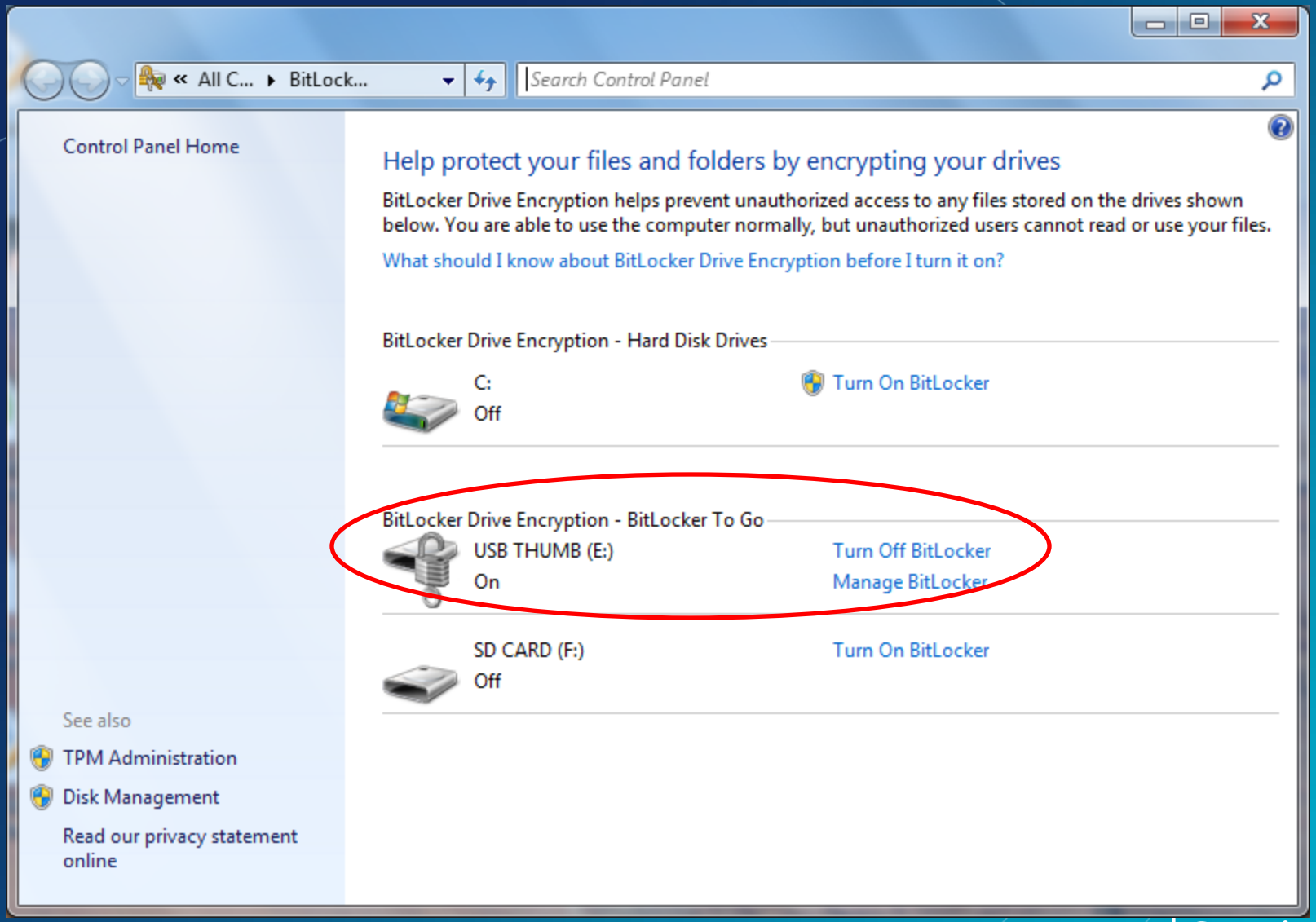


Microsoft | Services

Enabling BitLocker



Enabling BitLocker - OS



Microsoft | Services

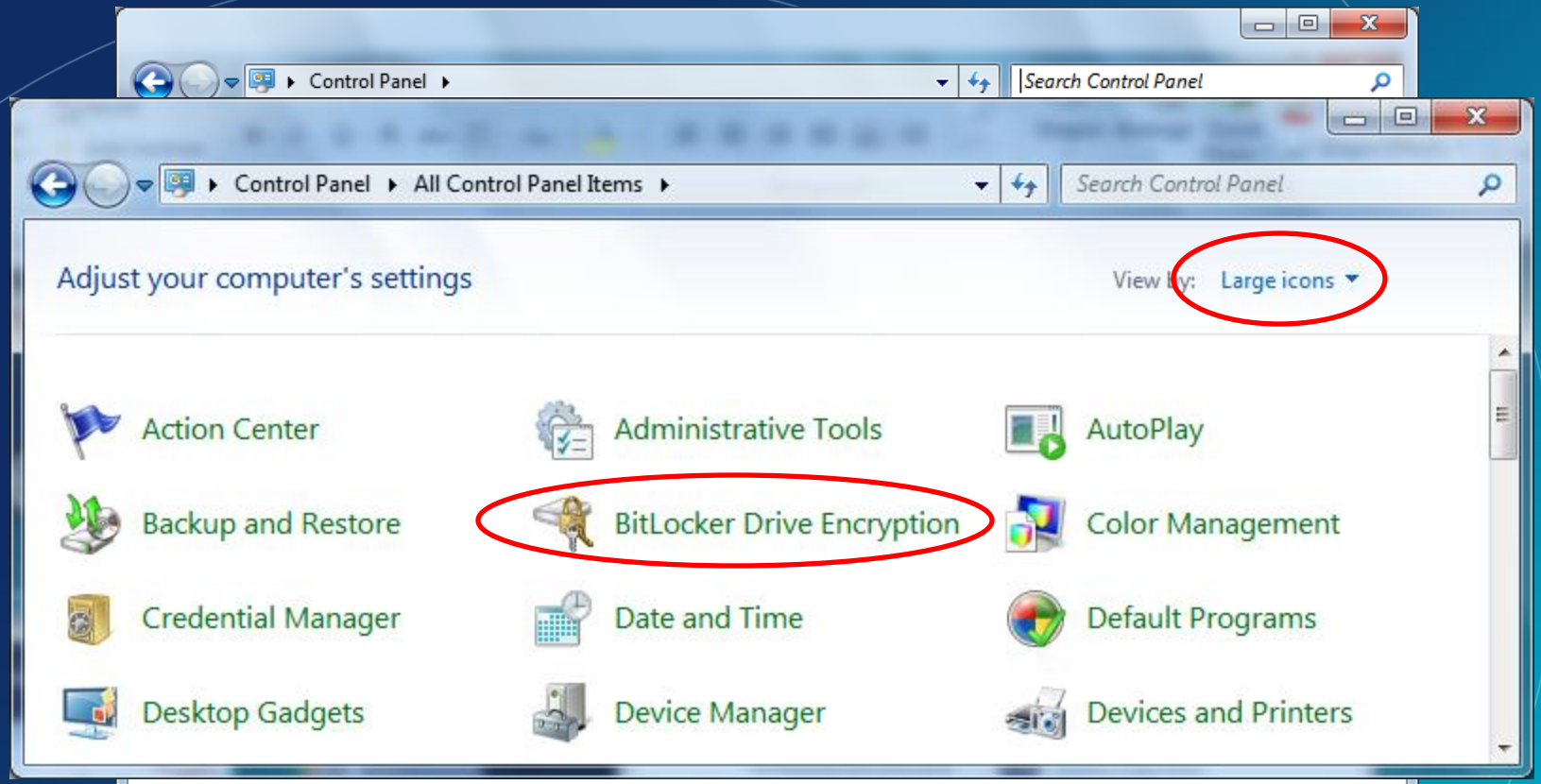
Questions?

Microsoft | Services

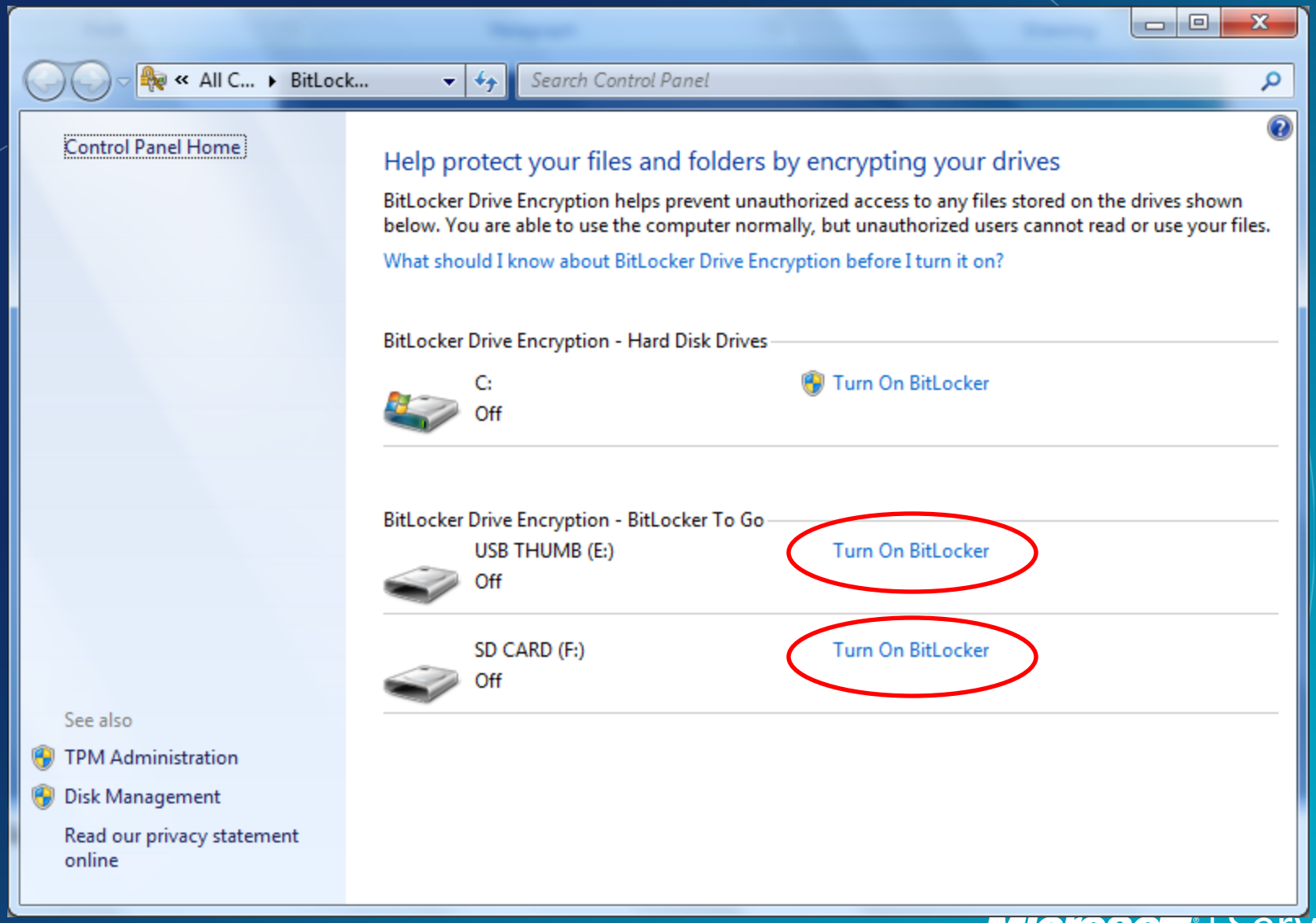
Enabling BitLocker “To Go”

Microsoft | Services

Enabling BitLocker of USB Stick

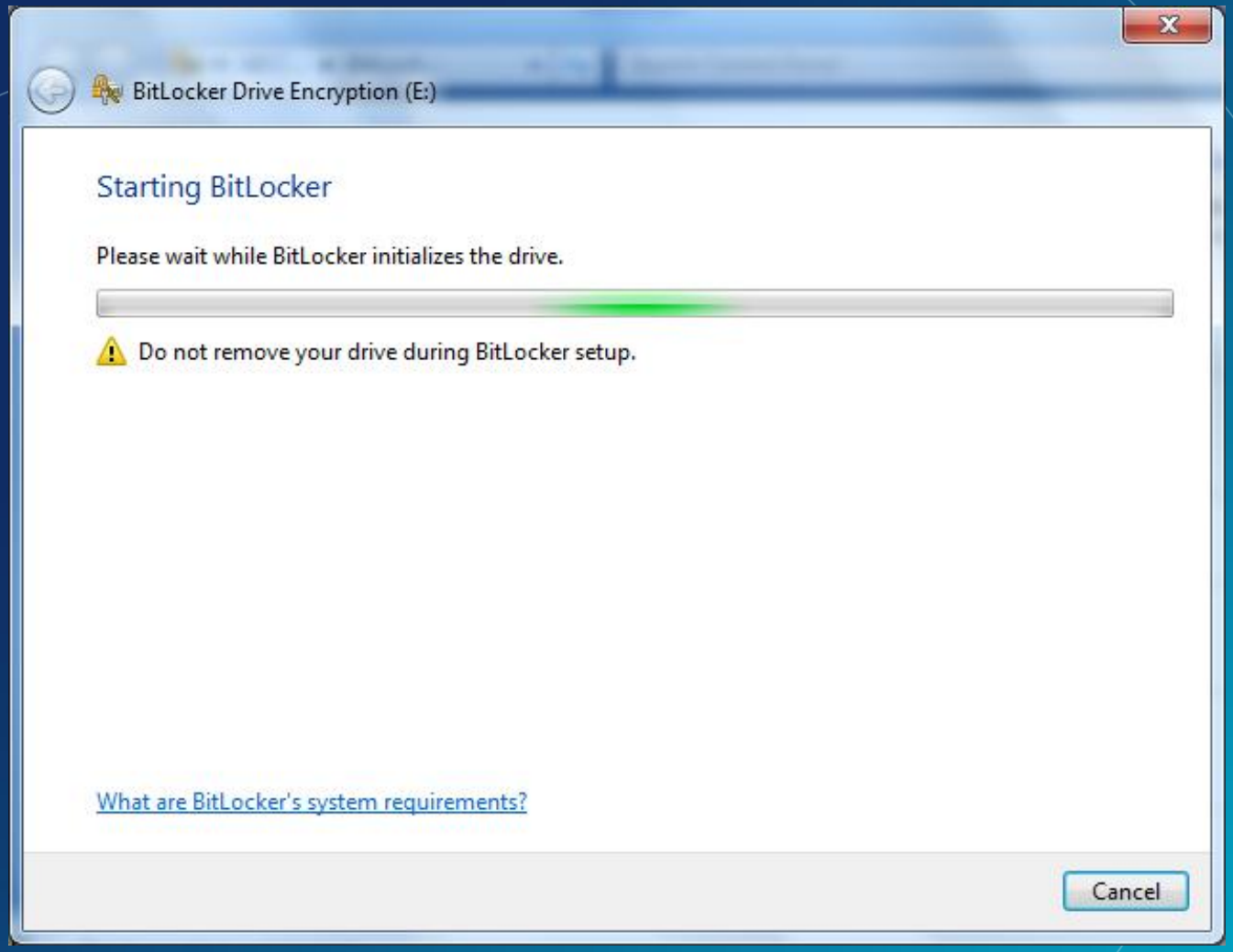


Enabling BitLocker of USB Stick



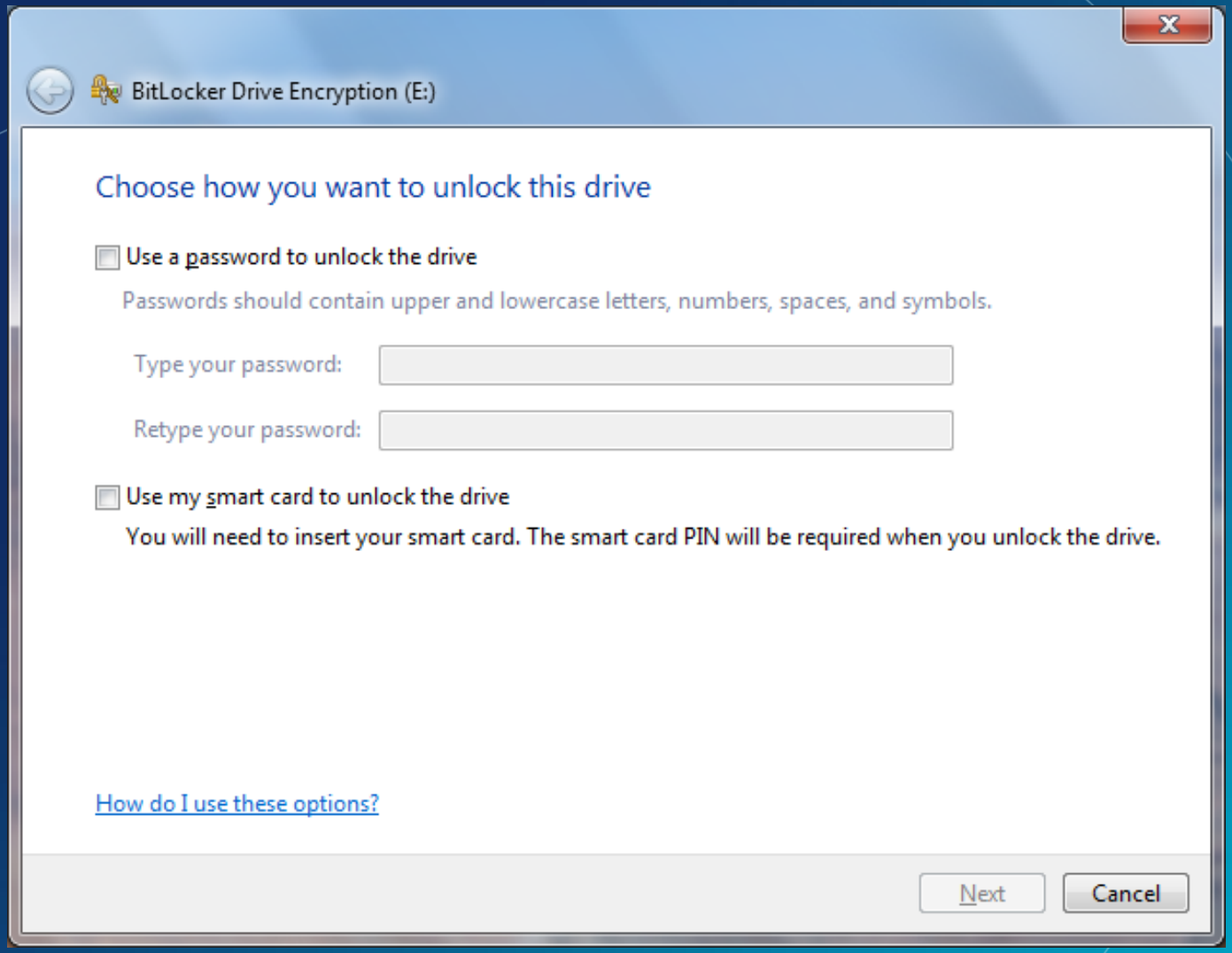
Microsoft | Services

Enabling BitLocker of USB Stick



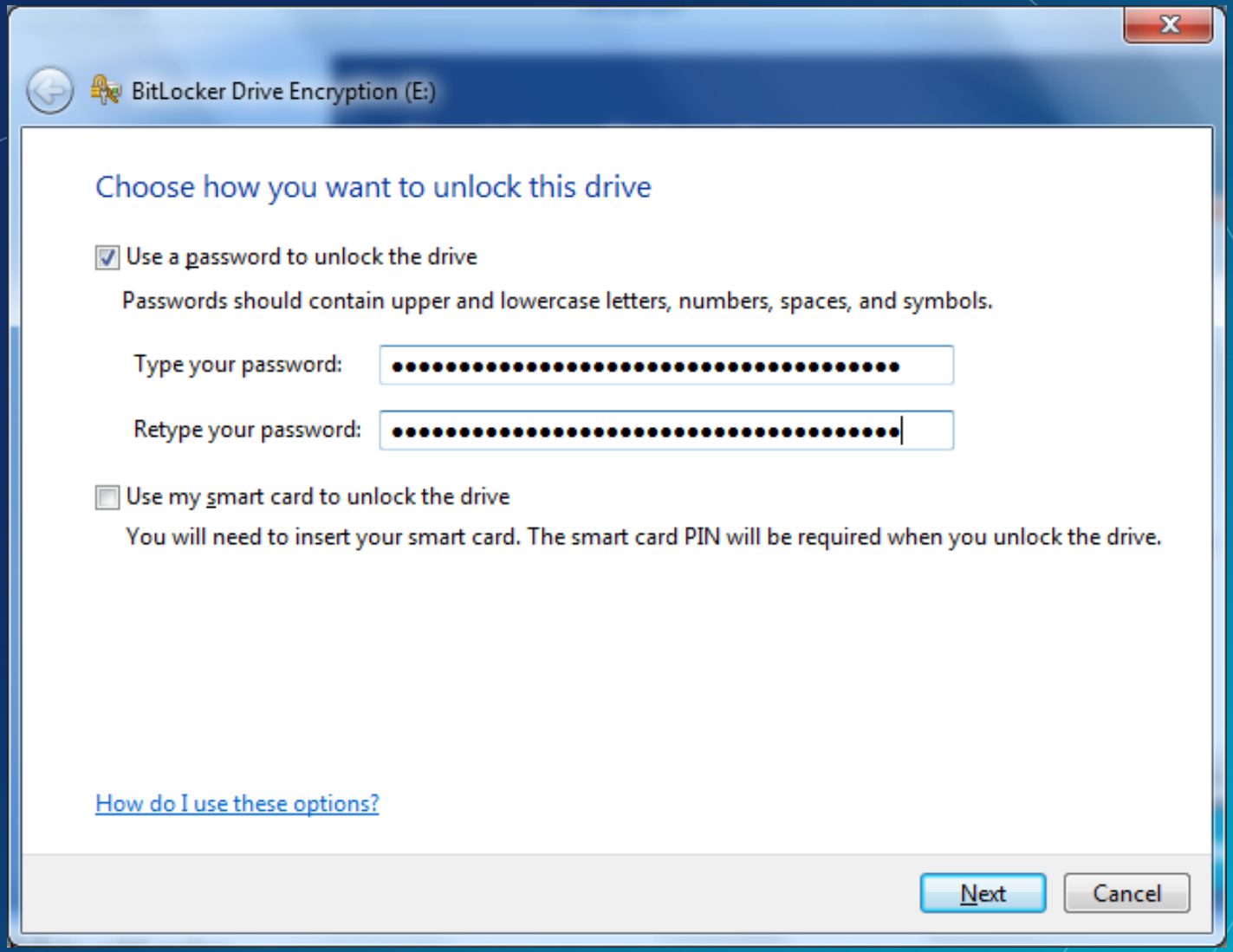
Microsoft | Services

Enabling BitLocker of USB Stick



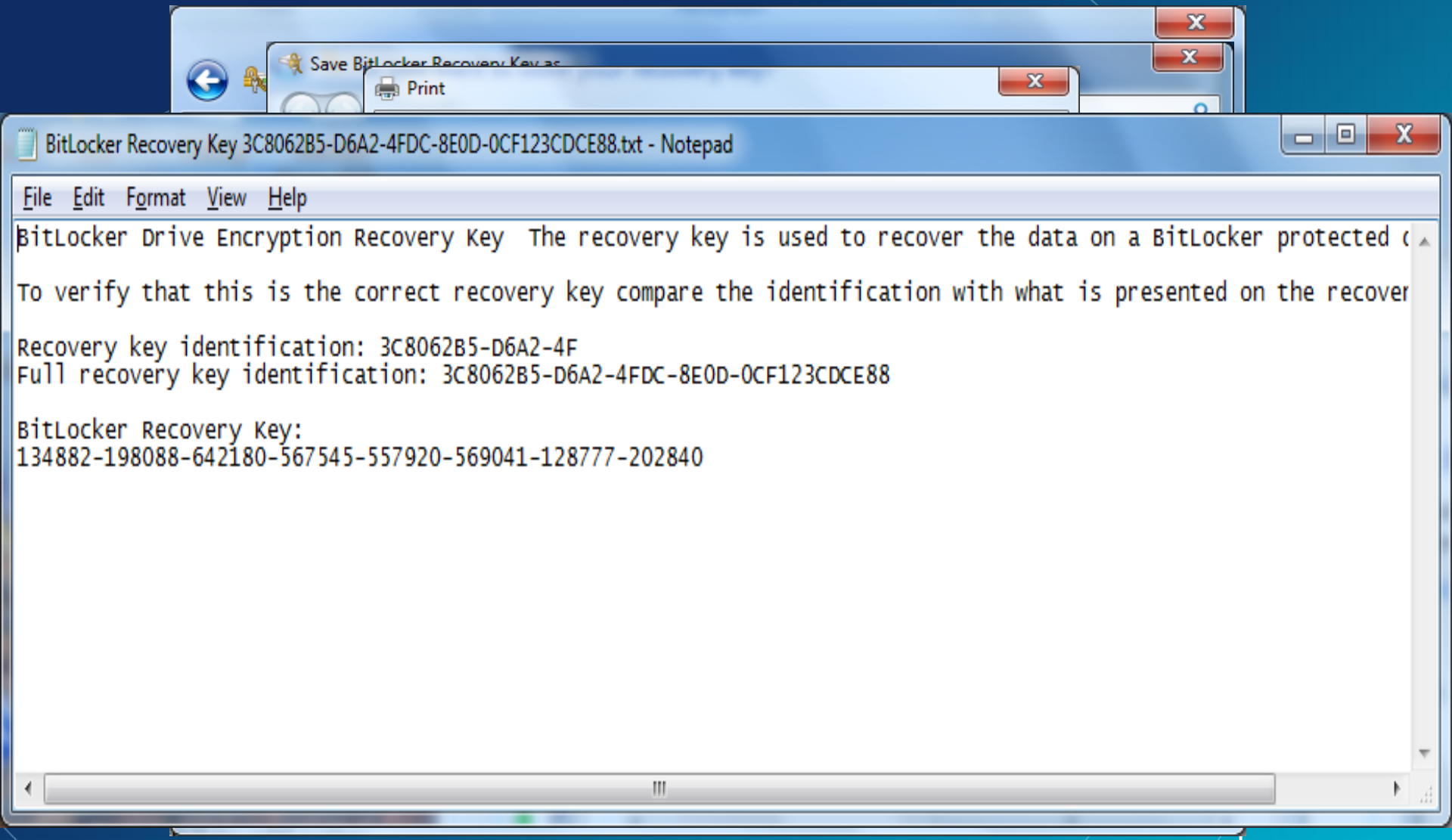
Microsoft | Services

Enabling BitLocker of USB Stick



Microsoft | Services

Enabling BitLocker of USB Stick



Microsoft | Services

Enabling BitLocker of USB Stick

Microsoft | Services

Unlocking your BitLocker enabled USB

- Insert USB device into PC and type your password when prompted

NOTE: The device can be unlocked on any Bitlocker To Go capable PC if you know the password

Microsoft | Services

Unlocking your BitLocker enabled USB

- Insert USB device into PC and type your password when prompted

NOTE: The device can be unlocked on any Bitlocker To Go capable PC if you know the password

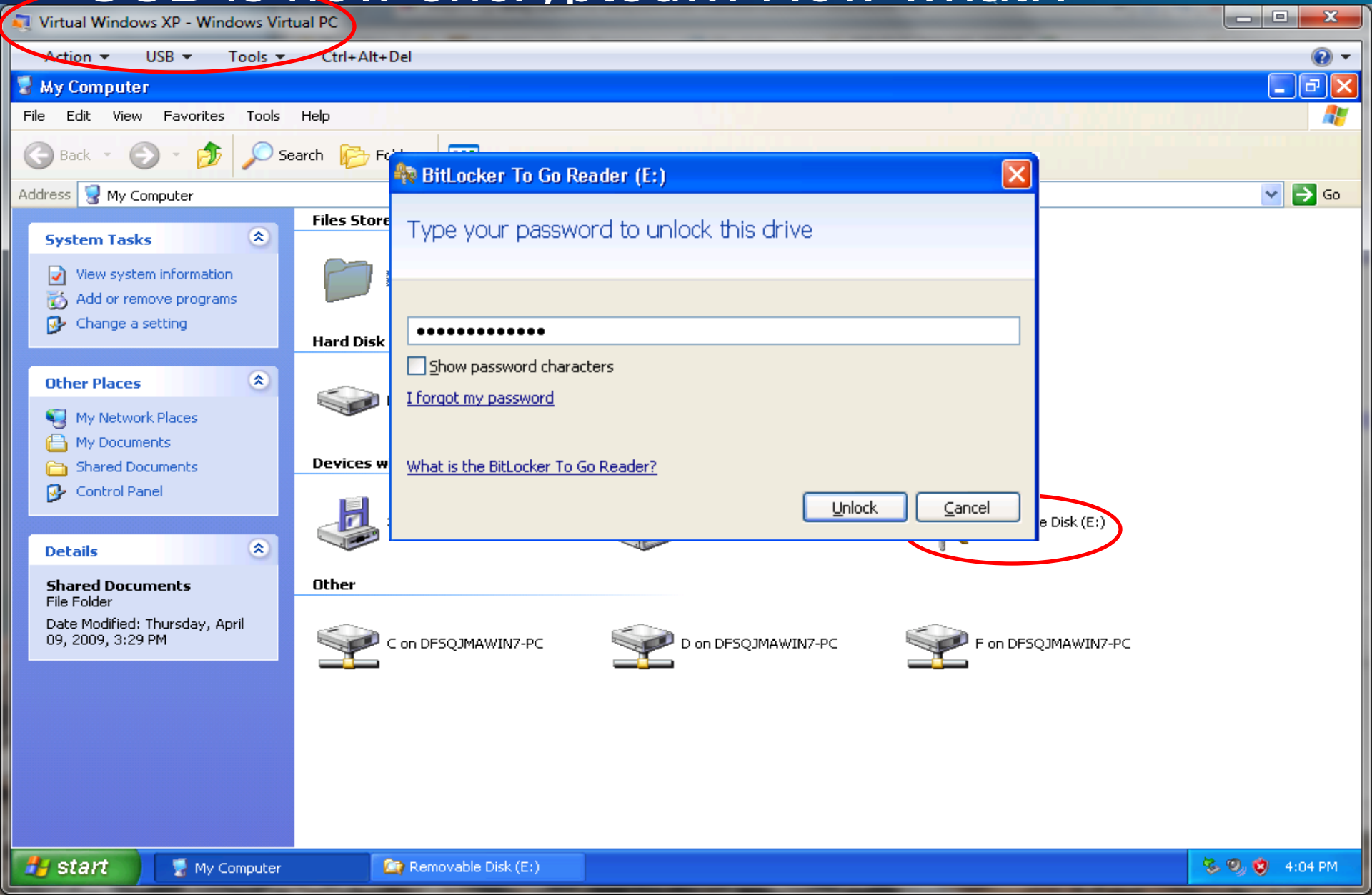
Microsoft | Services

USB is now encrypted… Now what!?

- If the encrypted USB is formatted with FAT then it can be used on down level Operating Systems
  - Win XP
  - Windows Vista
- How is this possible? These Operating Systems did not have Bitlocker to go functionality.

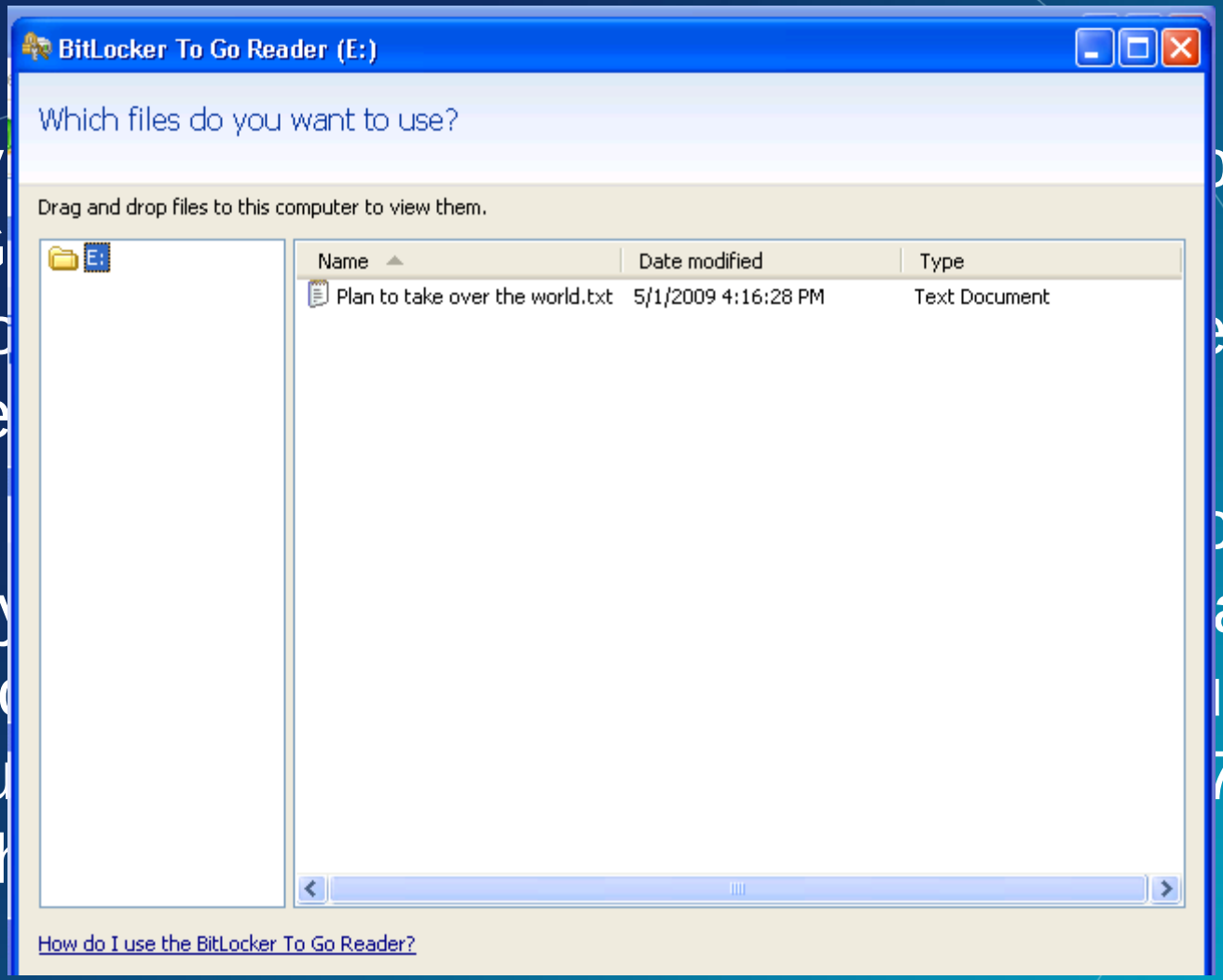
Microsoft | Services

USB is now encrypted… Now what!?



USB is now encrypted… Now what!?

- Prev ocker To G BitLo ed drive
- This ck the encry ad and ll featu 7 mach



Microsoft | Services

45

Minutes

Enabling BitLocker with a Thumb drive as a startup key

Exercise

Microsoft | Services

25

Minutes

Enabling BitLocker Encryption of a Thumb drive

Exercise

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Microsoft | Services

Microsoft | Services

BitLocker Technical Details

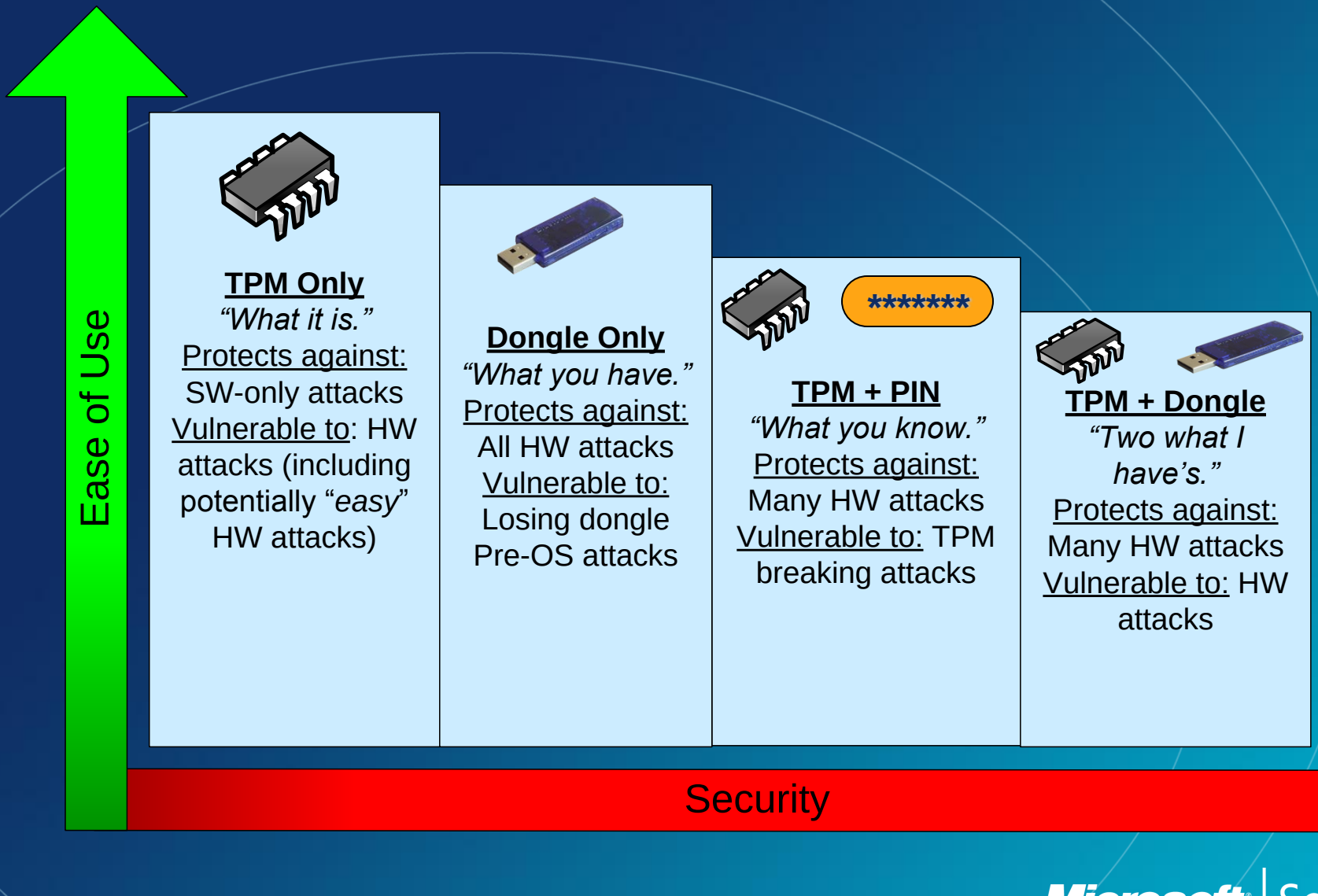
Exploration of Windows 7 Advanced Forensic Topics – Day 3

Microsoft | Services

What is BitLocker

- Review: BitLocker is a mechanism by which entire volumes of data can be secured in Windows 7:
  - Enterprise
  - Ultimate
- Why is this important?
  - This mechanism helps to protect systems from offline attacks.
  - Tell me again, how do we examine a suspect machine?

How is BitLocker Implemented



Microsoft | Services

BitLocker in Windows Vista

Drive Type	Unlock Methods	Recovery Methods	Management	Other requirements
Operating System Drives	TPM TPM+PIN TPM+Startup key TPM+PIN+ Startup Key* Startup key	Recovery password Recovery Key Active Directory backup of recovery password	Group policy controlled options presented to users	Use of the BitLocker Drive Preparation Tool to create a system partition where boot files are located. System partition size: 1.5GB System partition assigned a drive letter NTFS file system.
Fixed Data Drives*	Automatic unlocking	Same as OS drive	No policies	Operating System drive must be encrypted. NTFS file system.

*Introduced in Windows Vista SP1

Microsoft | Services

BitLocker in Windows 7
Operating system drive overview

Drive Type	Unlock Methods	Recovery Methods	Management	Other requirements
Operating System Drives	TPM TPM+PIN TPM+Startup key TPM+PIN+ Startup Key Startup key	Recovery password Recovery Key Active Directory backup of recovery password **Data Recovery Agent**	**Robust and consistent Group Policy enforcement** **Minimum Pin Length**	**Drive preparation fully integrated in BitLocker setup.** **System partition size:** **200MB without WinRE** **400MB with WinRE** **System partition letterless** NTFS file system.

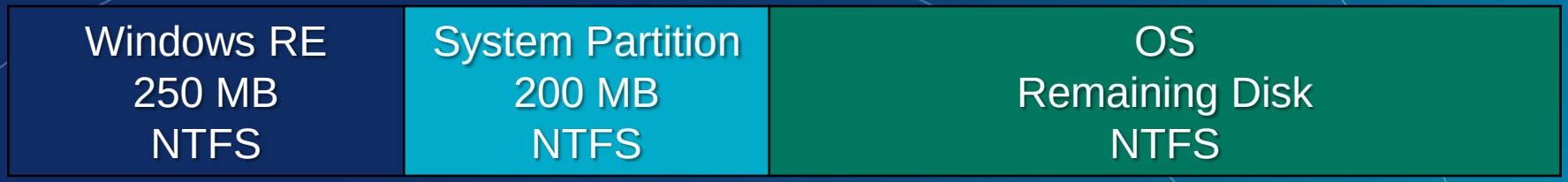
Microsoft | Services

BitLocker in Windows 7
Setup improvements

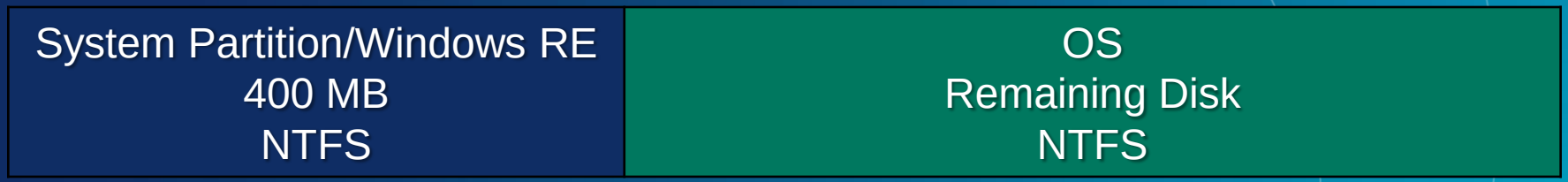
- Windows 7 is BitLocker ready
  - A separate system partition is now standard
  - System partition is now letter-less and hidden
  - BitLocker Drive Preparation Tool now integrated into the BitLocker setup experience
- Improved setup experience
  - Improved BitLocker setup wizard
  - Windows RE will be moved if installed on O/S partition

Microsoft | Services

BitLocker in Windows 7
Specifications for split-loader configuration



Note: An additional 50MB is required on the recovery partition for volume snapshots during Complete PC backups



Microsoft | Services

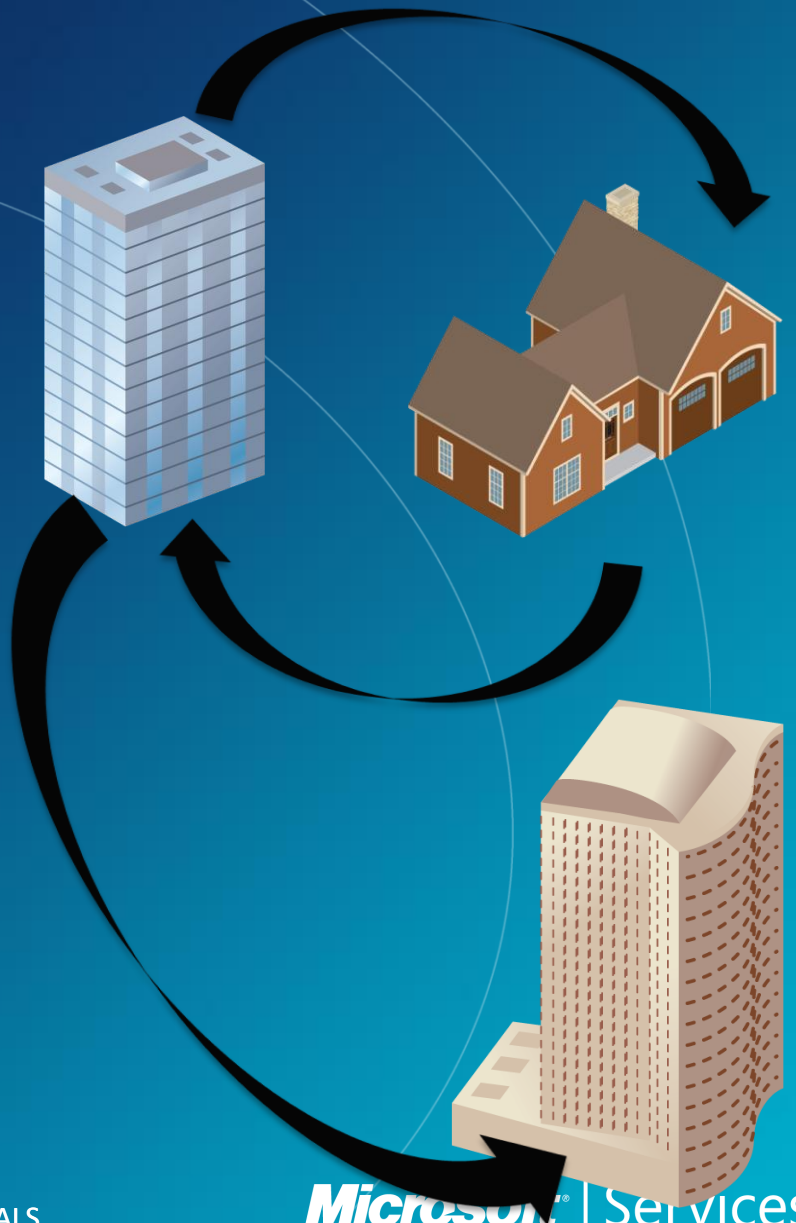
Windows 7 BitLocker To Go

Drive Type	Unlock Methods	Recovery Methods	Management	Other requirements
Removable data drives **e.g.:** **USB flash drives** **External Hard Drives**	**Passphrase** **Smart card** **Automatic Unlocking**	Recovery password Recovery Key Active Directory backup of recovery password **Data Recovery Agent**	**Robust and consistent group policy controls** **Ability to mandate encryption prior to granting write access**	File systems: NTFS **FAT** **FAT32** **ExFAT**

Microsoft | Services

Windows 7 BitLocker To Go
New unlock methods

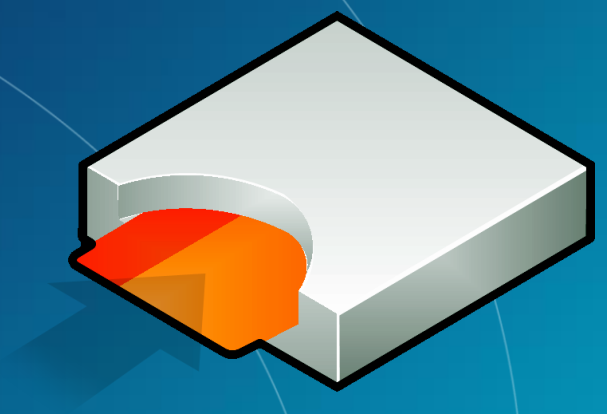
- Roaming using a Passphrase
  - No specific hardware requirement
  - Easily roam inside and outside domains/organizations
  - Complexity and length requirements managed by Group Policy



Microsoft | Services

Windows 7 BitLocker To Go
New unlock methods

- Roaming using Smart Cards
  - Leverages existing PKI infrastructure
  - Requires specific hardware
  - Can roam to any computer running Windows 7 or Server 2008 R2
  - Uses much stronger keys than passphrase Roaming using a Passphrase



Microsoft | Services

Windows 7 BitLocker To Go
New recovery mechanism

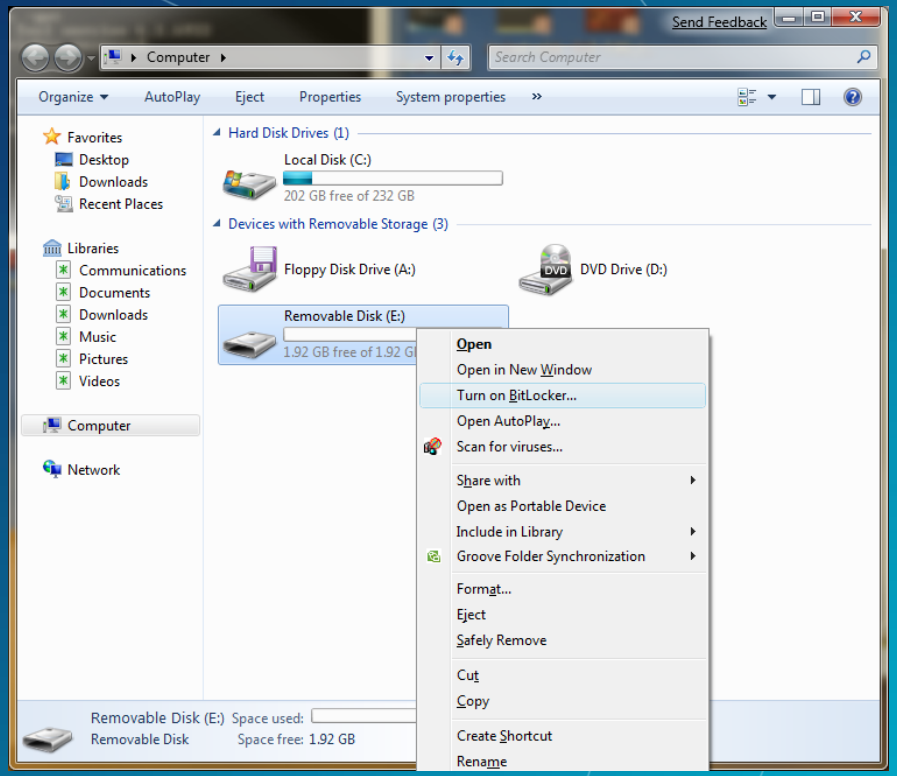
- Data Recovery Agents (DRA)
  - Certificate-based key protector
    - >A certificate containing a public key is distributed through Group Policy and is applied to any drive that mounts
    - >The corresponding private key is held by a DRA in corpsec
  - Allows IT department to have a way to unlock all protected drives in an enterprise
  - Leverage existing PKI infrastructure
  - Saves space in AD – same Key Protector on all drives
  - Also applies to O/S and fixed drives

Microsoft | Services

Windows 7 BitLocker To Go

Managing BitLocker

- BitLocker from Windows Explorer
- Right click drives in Windows Explorer to:
  - Turn on BitLocker
  - Unlock a drive
  - Manage BitLocker

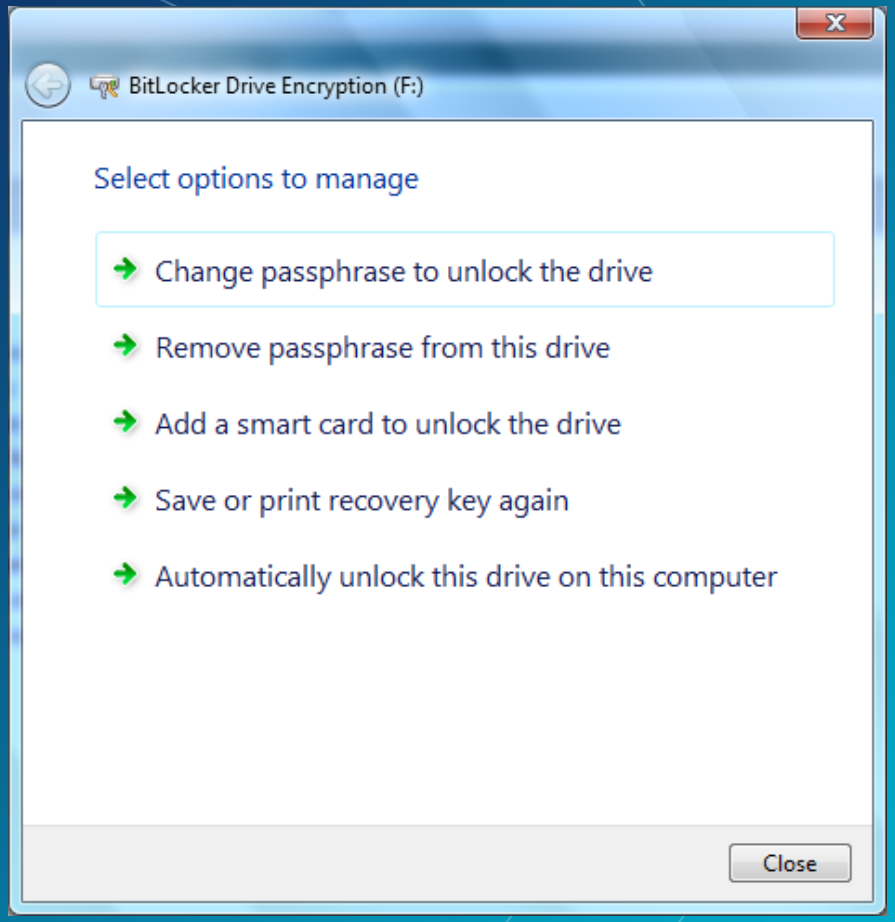


Microsoft | Services

Windows 7 BitLocker To Go

Managing BitLocker removable drives

- Data Drives
  - Add, remove, or change their passphrase
  - Add or remove a smart card
  - Add or remove automatic unlocking
  - Duplicate their recovery key/password



Microsoft | Services

Windows 7 BitLocker To Go - Enterprise
Mandating BitLocker on removable drives

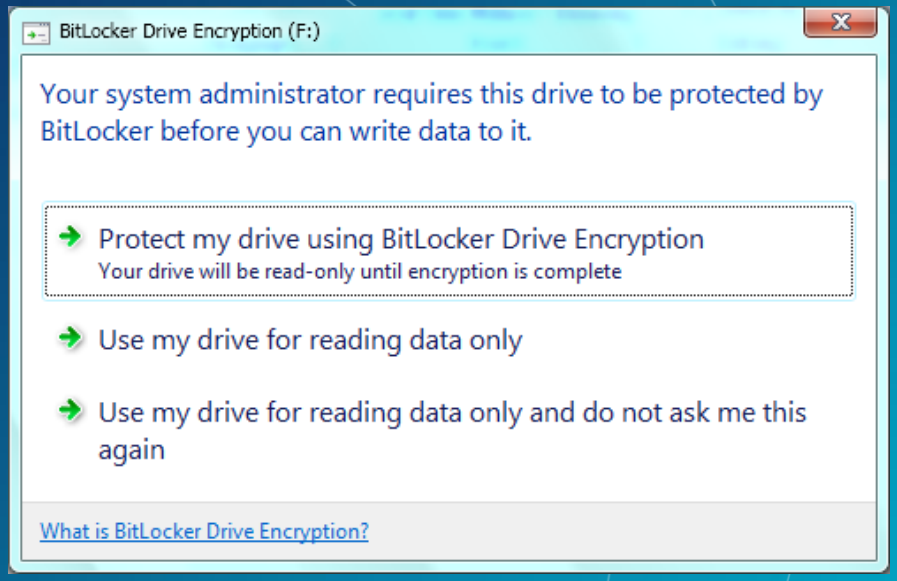
- Requiring BitLocker for removable data drives
  - When this policy is enforced, all removable drives will require BitLocker protection in order to have write access
  - As soon as a drive is plugged into a machine, a dialog is displayed to the user to either enable BitLocker on the device or only have read-only access

Microsoft | Services

Windows 7 BitLocker To Go

Mandating BitLocker on removable drives

- The user gets full RW access only after encryption is completed
- Users can alternatively enable BitLocker at a later time



Microsoft | Services

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Microsoft | Services

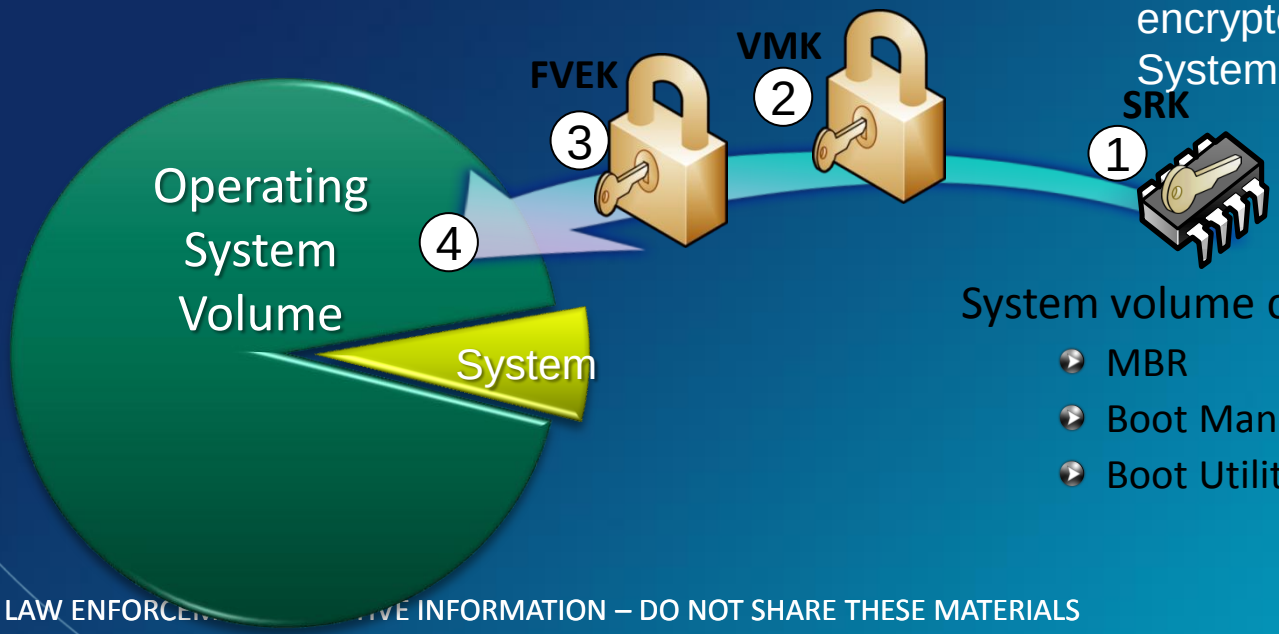
Disk Layout and Key Storage

Operating system volume contains:

- encrypted OS
- encrypted page file
- encrypted temp files
- encrypted data
- encrypted hibernation file

Where's the encryption key?

- SRK (Storage Root Key) contained in TPM
- SRK encrypts the VMK (Volume Master Key).
- VMK encrypts FVEK (Full Volume Encryption Key) – used for the actual data encryption.
- FVEK and VMK are stored encrypted on the Operating System Volume.



System volume contains:

- MBR
- Boot Manager
- Boot Utilities

Microsoft | Services

BitLocker Explained

- BitLocker can be implemented in a number of ways and can be thought of as a 2 phase approach to securing a machine
  - Phase 1: Pre-OS Validation
  - Phase 2: Full Volume Encryption

  Note: Both phases may not be implemented depending on hardware and software versions

Drive Encryption Specifics

- Some of the tenants of BitLocker
  - Once enabled the data on the drive is always encrypted unless the volume is decrypted
  - FVEVOL.SYS sits underneath the file system driver and performs all encryption / decryption
  - The drive is encrypted a sector at a time and supports sector sized from 512 – 8192 bytes

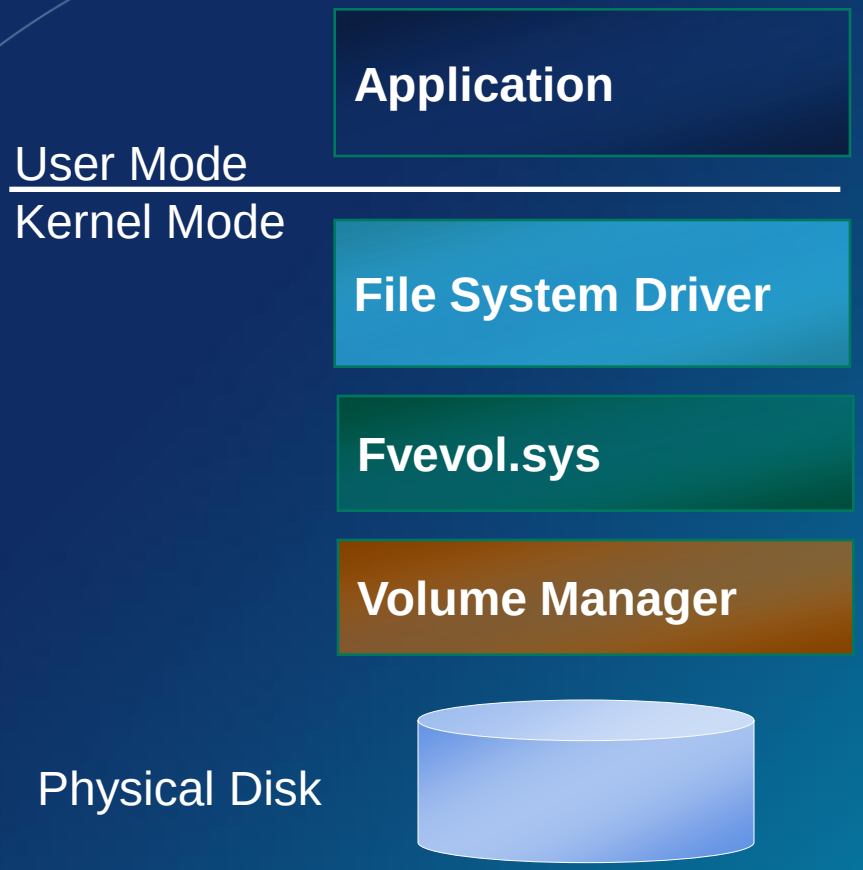
Drive Encryption Specifics

Once enabled the data on the drive is always encrypted unless the volume is decrypted

- The initial process of enabling BitLocker takes a while as all of the data on the disk is encrypted.
- There are 2 options once a drive is encrypted:
  - Disabled: Volume is still encrypted but the VMK is stored in the clear (used for updates)
  - Decrypt: Decrypting the drive completely

Drive Encryption Specifics

FVEVOL.SYS sits underneath the file system driver and performs all encryption / decryption



- Once booted, Vista (and the user) sees no difference in experience
- The encryption / decryption happens at a lower level

Microsoft | Services

Drive Encryption Specifics

The drive is encrypted a sector at a time and supports sector sized from 512 – 8192 bytes

- It would be impractical to encrypt the entire drive as one blob not to mention unmanageable given the number of reads and writes
- BitLocker encrypts the drive a sector at a time so that only the sectors that are being read or written have to be manipulated.

Microsoft | Services

BitLocker Forensic View (Details and Artifacts in BitLocker Data)

Exploration of Windows Vista Advanced Forensic Topics – Day 3

Microsoft | Services

Examination of Physical Image

- Despite the fact that BitLocker implements full volume encryption, there are a number of locations that contain clear text data
- The BIOS Parameter Block (BPB) is the first 54 bytes in the first sector of a volume and has volume “signature” data

Examination of Physical Image

Offset (h)	Offset (d)	Size	Field	Required Value for BitLocker
0x003	3	8	Signature	‘-‘,’F’,’V’,’E’,’-‘,’F’,’S’,’-‘
0x00B	11	2	BytesPerSector	
0x00D	13	1	SectorsPerCluster	One of 0x01, 0x02, 0x04, 0x08, 0x10, 0x20, 0x40 or 0x80
0x00E	14	2	ReservedClusters	0x0000
0x010	16	1	FatCount	0x00
0x011	17	2	RootEntries	0x0000
0x013	19	2	Sectors	0x0000
0x016	22	2	SectorsPerFat	0x0000
0x020	32	4	LargeSectors	0x00000000
0x038	56	8	MetadataLcn	

Microsoft | Services

Examination of Physical Image

- In addition to the data in the volume signature field, BitLocker stores copies of the metadata in other locations.
- First location is calculated with the following data from the signature field:

  MetadataLCN * SectorsPerCluster * BytesPerSector

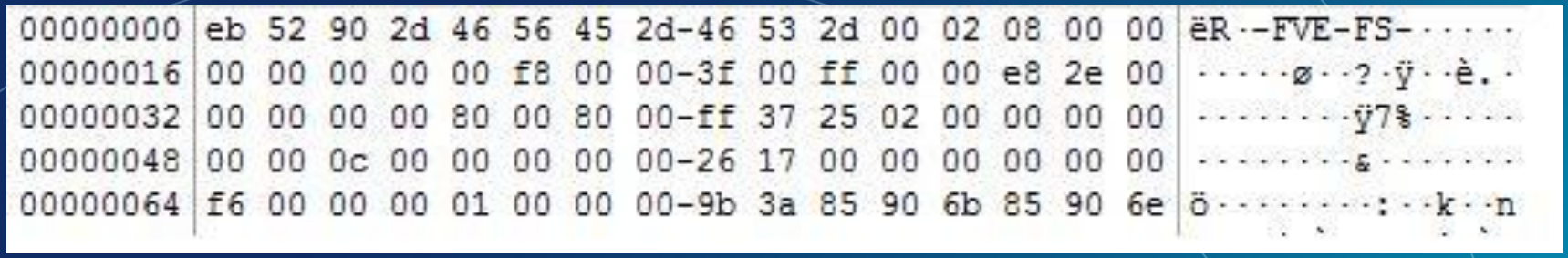
Microsoft | Services

Examination of Physical Image

Offset (h)	Offset (d)	Size	Field	Content
0x000	0	8	Signature	‘-‘,’F’,’V’,’E’,’-‘,’F’,’S’,’-‘
0x008	8	2	Size	Size of structure. Validation data follows this structure.
0x002	2	10	Version	0x0001 for current version.
0x004	4	12		Version specific content.

- Additionally a text string search for –FVE-FS- to find this location and verify the calculation

Examination of Physical Image - VISTA

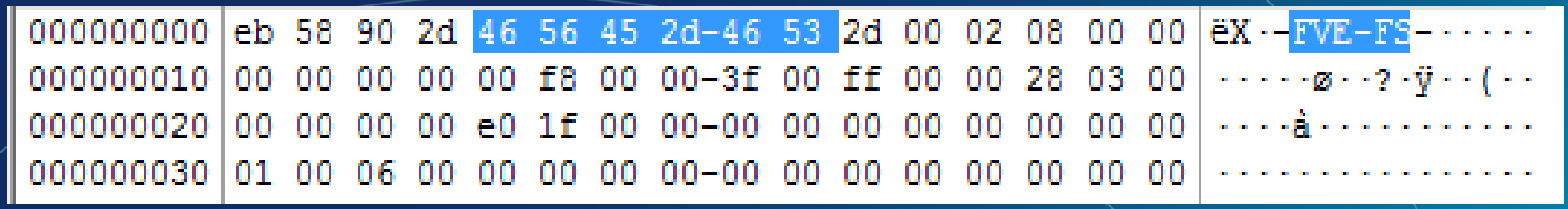


```
00000000 eb 52 90 2d 46 56 45 2d-46 53 2d 00 02 08 00 00 ëR·-FVE-FS-·····
00000016 00 00 00 00 00 f8 00 00-3f 00 ff 00 00 e8 2e 00 ·····ø··?·ÿ··è.·
00000032 00 00 00 00 80 00 80 00-ff 37 25 02 00 00 00 00 ·····ÿ7%·····
00000048 00 00 0c 00 00 00 00 00-26 17 00 00 00 00 00 00 ·····&·····
00000064 f6 00 00 00 01 00 00 00-9b 3a 85 90 6b 85 90 6e ö·····:··k··n
```

- Viewing the volume signature in your favorite forensic tool makes the issue very clear
- Notice the signature “-FVE-FS-”

Microsoft | Services

Examination of Physical Image – Win 7



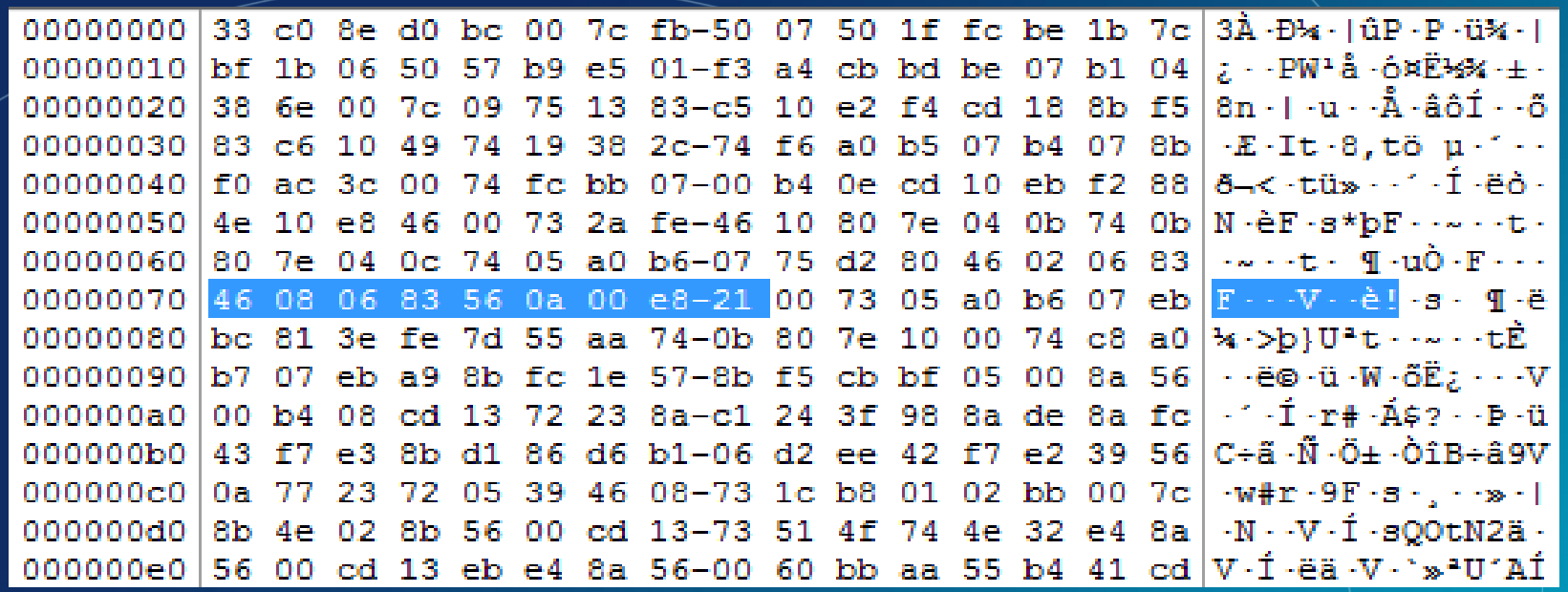
000000000	eb	58	90	2d	46	56	45	2d	46	53	2d	00	02	08	00	00
000000010	00	00	00	00	00	f8	00	00	3f	00	ff	00	00	28	03	00
000000020	00	00	00	00	e0	1f	00	00	00	00	00	00	00	00	00	00
000000030	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00

000000000	ë	X	·	·	-	F	V	E	-	F	S	-	·	·	·	·
000000010	·	·	·	·	·	ø	·	·	?	·	ÿ	·	·	(	·	·
000000020	·	·	·	·	à	·	·	·	·	·	·	·	·	·	·	·
000000030	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·

- Viewing the volume signature in your favorite forensic tool makes the issue very clear
- Notice the signature “-FVE-FS-”

Microsoft | Services

Examination of Physical Image – BL To Go DOS – IS THIS RIGHT?



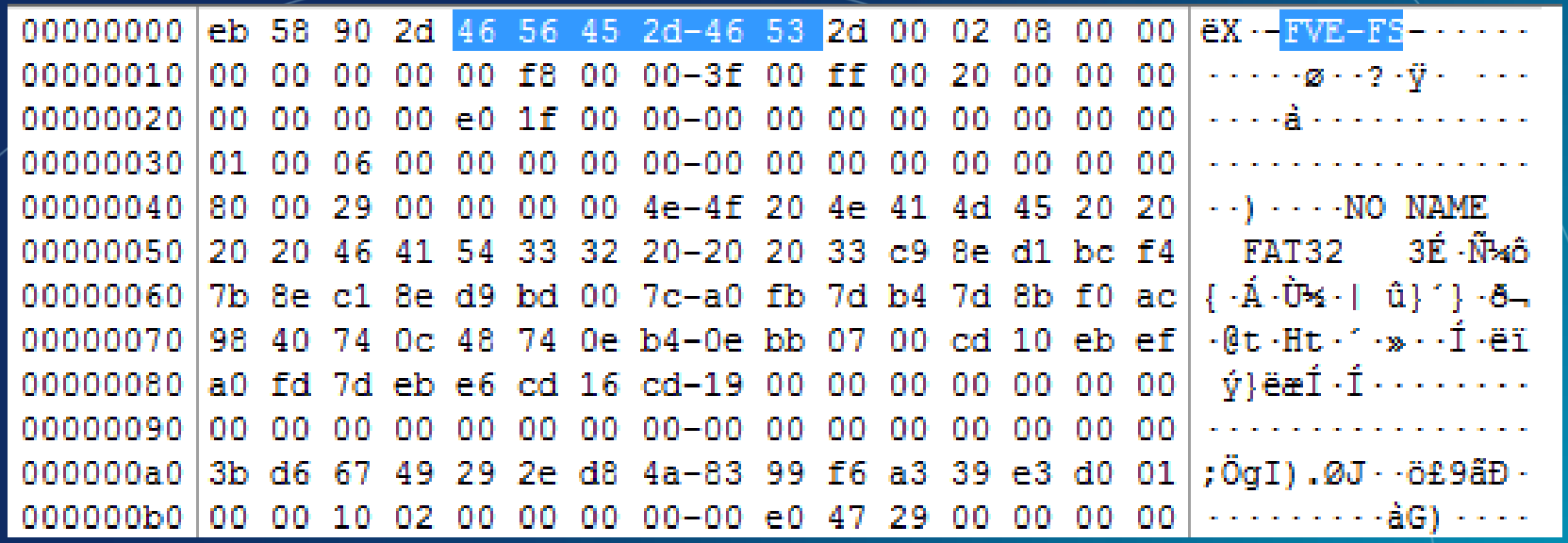
00000000	33	c0	8e	d0	bc	00	7c	fb	50	07	50	1f	fc	be	1b	7c
00000010	bf	1b	06	50	57	b9	e5	01	f3	a4	cb	bd	be	07	b1	04
00000020	38	6e	00	7c	09	75	13	83	c5	10	e2	f4	cd	18	8b	f5
00000030	83	c6	10	49	74	19	38	2c	74	f6	a0	b5	07	b4	07	8b
00000040	f0	ac	3c	00	74	fc	bb	07	00	b4	0e	cd	10	eb	f2	88
00000050	4e	10	e8	46	00	73	2a	fe	46	10	80	7e	04	0b	74	0b
00000060	80	7e	04	0c	74	05	a0	b6	07	75	d2	80	46	02	06	83
00000070	46	08	06	83	56	0a	00	e8	21	00	73	05	a0	b6	07	eb
00000080	bc	81	3e	fe	7d	55	aa	74	0b	80	7e	10	00	74	c8	a0
00000090	b7	07	eb	a9	8b	fc	1e	57	8b	f5	cb	bf	05	00	8a	56
000000a0	00	b4	08	cd	13	72	23	8a	c1	24	3f	98	8a	de	8a	fc
000000b0	43	f7	e3	8b	d1	86	d6	b1	06	d2	ee	42	f7	e2	39	56
000000c0	0a	77	23	72	05	39	46	08	73	1c	b8	01	02	bb	00	7c
000000d0	8b	4e	02	8b	56	00	cd	13	73	51	4f	74	4e	32	e4	8a
000000e0	56	00	cd	13	eb	e4	8a	56	00	60	bb	aa	55	b4	41	cd

00000000	3	À	·	Ð	¾	·	|	û	P	·	P	·	ü	¾	·	|
00000010	¿	·	·	P	W	¹	å	·	ó	¤	Ë	¾	¾	·	±	·
00000020	8	n	·	|	·	u	·	·	Å	·	â	ô	Í	·	·	õ
00000030	·	Æ	·	I	t	·	8	,	t	ö		µ	·	´	·	·
00000040	ð	¬	<	·	t	ü	»	·	·	´	·	Í	·	ë	ò	·
00000050	N	·	è	F	·	s	*	þ	F	·	·	~	·	·	t	·
00000060	·	~	·	·	t	·		¶	·	u	Ò	·	F	·	·	·
00000070	F	·	·	·	V	·	·	è	!	·	s	·		¶	·	ë
00000080	¾	·	>	þ	}	U	ª	t	·	·	~	·	·	t	È	
00000090	·	·	ë	©	·	ü	·	W	·	õ	Ë	¿	·	·	·	V
000000a0	·	´	·	Í	·	r	#	·	Á	$	?	·	·	Þ	·	ü
000000b0	C	÷	ã	·	Ñ	·	Ö	±	·	Ò	î	B	÷	â	9	V
000000c0	·	w	#	r	·	9	F	·	s	·	¸	·	·	»	·	|
000000d0	·	N	·	·	V	·	Í	·	s	Q	O	t	N	2	ä	·
000000e0	V	·	Í	·	ë	ä	·	V	·	`	»	ª	U	´	A	Í

- Viewing the volume signature in your favorite forensic tool makes the issue very clear
- Notice the signature “FVE!”

Microsoft | Services

Examination of Physical Image – BL To Go NTFS



```
00000000  eb 58 90 2d 46 56 45 2d-46 53 2d 00 02 08 00 00  ëX·-FVE-FS-·····
00000010  00 00 00 00 00 f8 00 00-3f 00 ff 00 20 00 00 00  ·····ø··?·ÿ· ···
00000020  00 00 00 00 e0 1f 00 00-00 00 00 00 00 00 00 00  ····à···········
00000030  01 00 06 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00000040  80 00 29 00 00 00 00 4e-4f 20 4e 41 4d 45 20 20  ··)····NO NAME
00000050  20 20 46 41 54 33 32 20-20 20 33 c9 8e d1 bc f4    FAT32   3É·Ñ¼ô
00000060  7b 8e c1 8e d9 bd 00 7c-a0 fb 7d b4 7d 8b f0 ac  {·Á·Ù½·| û}´}·ð¬
00000070  98 40 74 0c 48 74 0e b4-0e bb 07 00 cd 10 eb ef  ·@t·Ht·´·»··Í·ëï
00000080  a0 fd 7d eb e6 cd 16 cd-19 00 00 00 00 00 00 00   ý}ëæÍ·Í·······
00000090  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
000000a0  3b d6 67 49 29 2e d8 4a-83 99 f6 a3 39 e3 d0 01  ;ÖgI).ØJ·ö£9ãÐ·
000000b0  00 00 10 02 00 00 00 00-00 e0 47 29 00 00 00 00  ·········àG)····
```

- Viewing the volume signature in your favorite forensic tool makes the issue very clear
- Notice the signature “-FVE-FS-”

Microsoft | Services

Examination of the BEK File

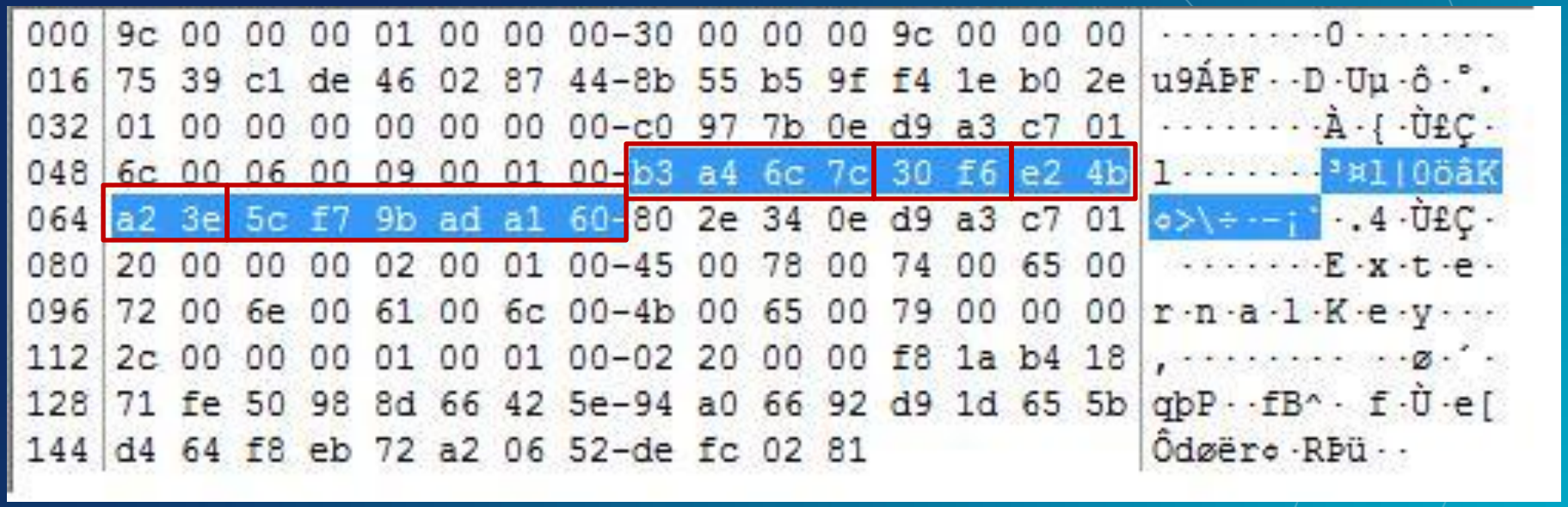
- We can also see the Recovery Key ID number (i.e. the GUID like name of the BEK file)

  Offset 56(d), Length 4 bytes (Reversed)
  Offset 60(d), Length 2 bytes (Reversed)
  Offset 62(d), Length 2 bytes (Reversed)
  Offset 64(d), Length 2 bytes (Forward)
  Offset 66(d), Length 6 bytes (Forward)

Microsoft | Services

Examination of the BEK File

Recovery Key:
ID: {7C6CA4B3-F630-4BE2-A23E-5CF79BADA160}
External Key File Name:
7C6CA4B3-F630-4BE2-A23E-5CF79BADA160.BEK



000	9c	00	00	00	01	00	00	00	30	00	00	00	9c	00	00	00
016	75	39	c1	de	46	02	87	44	8b	55	b5	9f	f4	1e	b0	2e
032	01	00	00	00	00	00	00	00	c0	97	7b	0e	d9	a3	c7	01
048	6c	00	06	00	09	00	01	00	b3	a4	6c	7c	30	f6	e2	4b
064	a2	3e	5c	f7	9b	ad	a1	60	80	2e	34	0e	d9	a3	c7	01
080	20	00	00	00	02	00	01	00	45	00	78	00	74	00	65	00
096	72	00	6e	00	61	00	6c	00	4b	00	65	00	79	00	00	00
112	2c	00	00	00	01	00	01	00	02	20	00	00	f8	1a	b4	18
128	71	fe	50	98	8d	66	42	5e	94	a0	66	92	d9	1d	65	5b
144	d4	64	f8	eb	72	a2	06	52	de	fc	02	81				

Microsoft | Services

Examination of the BEK File

- When implementing BitLocker with a Startup Key (USB drive or encrypting a data volume) we can get additional information from the file itself.
  - Date of key generation
  - Time of key generation

  Offset 72(d), Length 8 bytes (Little endian)

BitLocker Investigative Impact

- What do investigators have on our side?
  - BitLocker is only available in Windows Enterprise and Ultimate SKUs
  - BitLocker has a number of “Recovery” scenarios that we can exploit
  - Encryption is “scary” to users (even criminals)
  - BitLocker, at its core, is a password technology, we simply have to get the password from our suspect or surroundings

Microsoft | Services

BitLocker Investigative Impact

- What do investigators have on our side?
  - We are investigators, and should be aware if our suspect is using encryption technology prior to entry
  - BitLocker in the Enterprise should have a high likelihood of recovery information availability
  - BitLocker protected drives can be mounted and examined forensically if we can get in
  - We are the good guys!

Microsoft | Services

BitLocker Investigative Impact

- What do investigators have working against us?
  - BitLocker has very low user interaction after the initial setup
  - BitLocker has <5% overhead on performance
  - If used in the TPM + PIN scenario, we need the user to provide the PIN or recovery info
  - If used in the TPM + USB scenario, we need the USB drive or user supplied recovery info

Microsoft | Services

BitLocker Investigative Impact

- What do investigators have working against us?
  - BitLocker uses US Government grade encryption in 128 bit or 256 bit AES keying
  - BitLocker operates at a lower level of the OS so security technologies can be layered (EFS)

Microsoft | Services

BitLocker Investigative Impact

- Introduction of this security technology in Windows Vista and Windows 7 does not amount to an overwhelming blow to the efforts of law enforcement
- As has been true throughout history the dumb criminals will be easy to catch and the smart ones harder…

Questions?

Microsoft | Services

30

Minutes

Enabling BitLocker on Data volumes

Exercise 6

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Microsoft | Services

Microsoft | Services

Mounting BitLocker Protected Volumes

Exploration of Windows 7 Advanced Forensic Topics – Day 3

Microsoft | Services

Requirements – NEED TO TEST Versions

- Examiner System must be running either Windows Win 7 Enterprise or Ultimate
- BitLocker does NOT have to be enabled on the Examiner system
- All obvious write protection mechanisms should be in place – Forensics 101

Mounting a BitLocker Drive

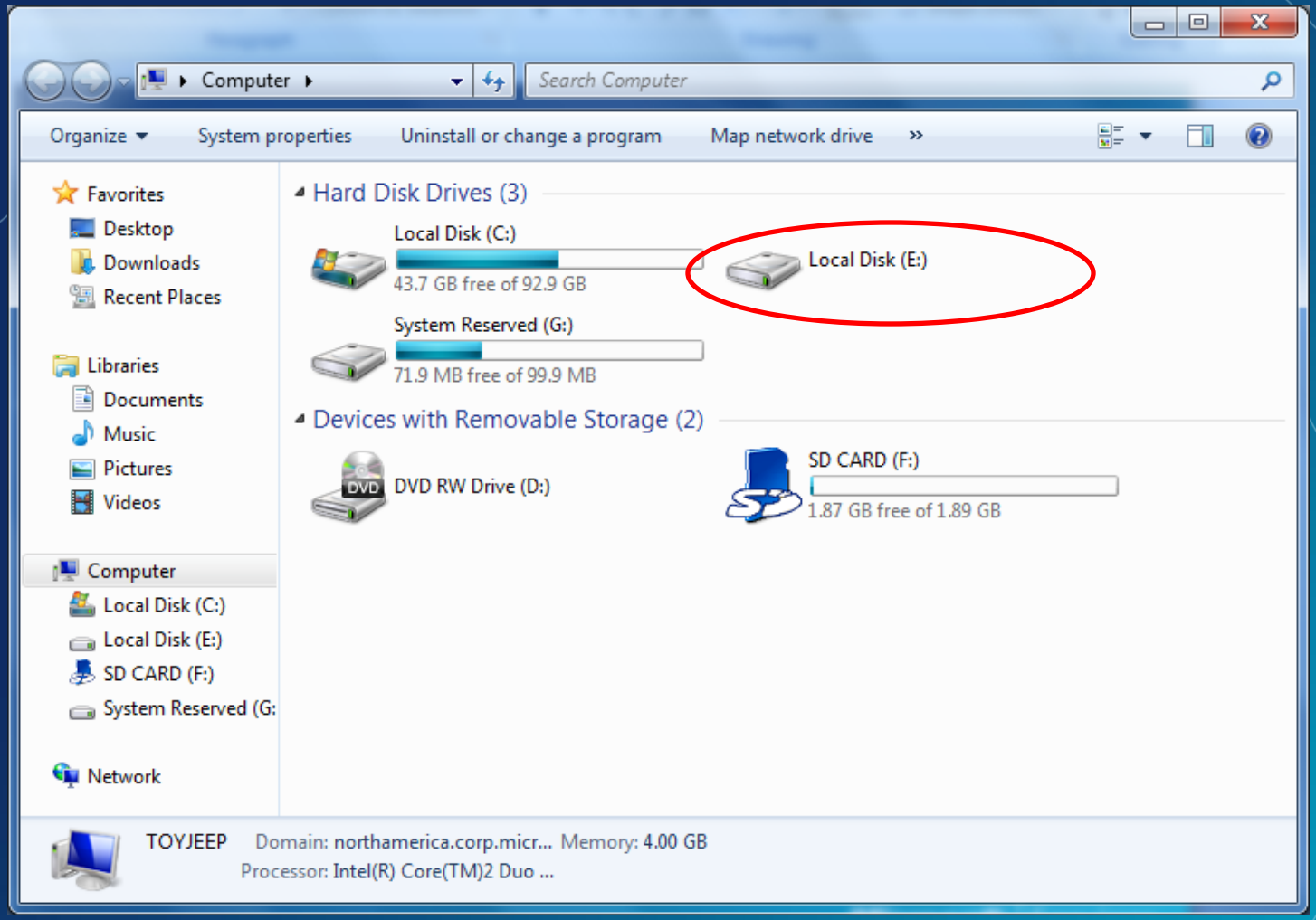
- Investigators can use the recovery mechanisms built into the BitLocker mechanism to access the protected drive
- Just like EFS
- **WE STILL NEED THE PASSWORD!!!**

Microsoft | Services

Mounting a BitLocker Drive

- Physical Mount
  - Install the “suspect” drive as a secondary drive through a write blocker
  - Boot to a BitLocker capable version of Win 7
  - Access the BitLocker MMC
  - You should see the “suspect” drive
  - Use the BitLocker recovery process to temporarily access the data

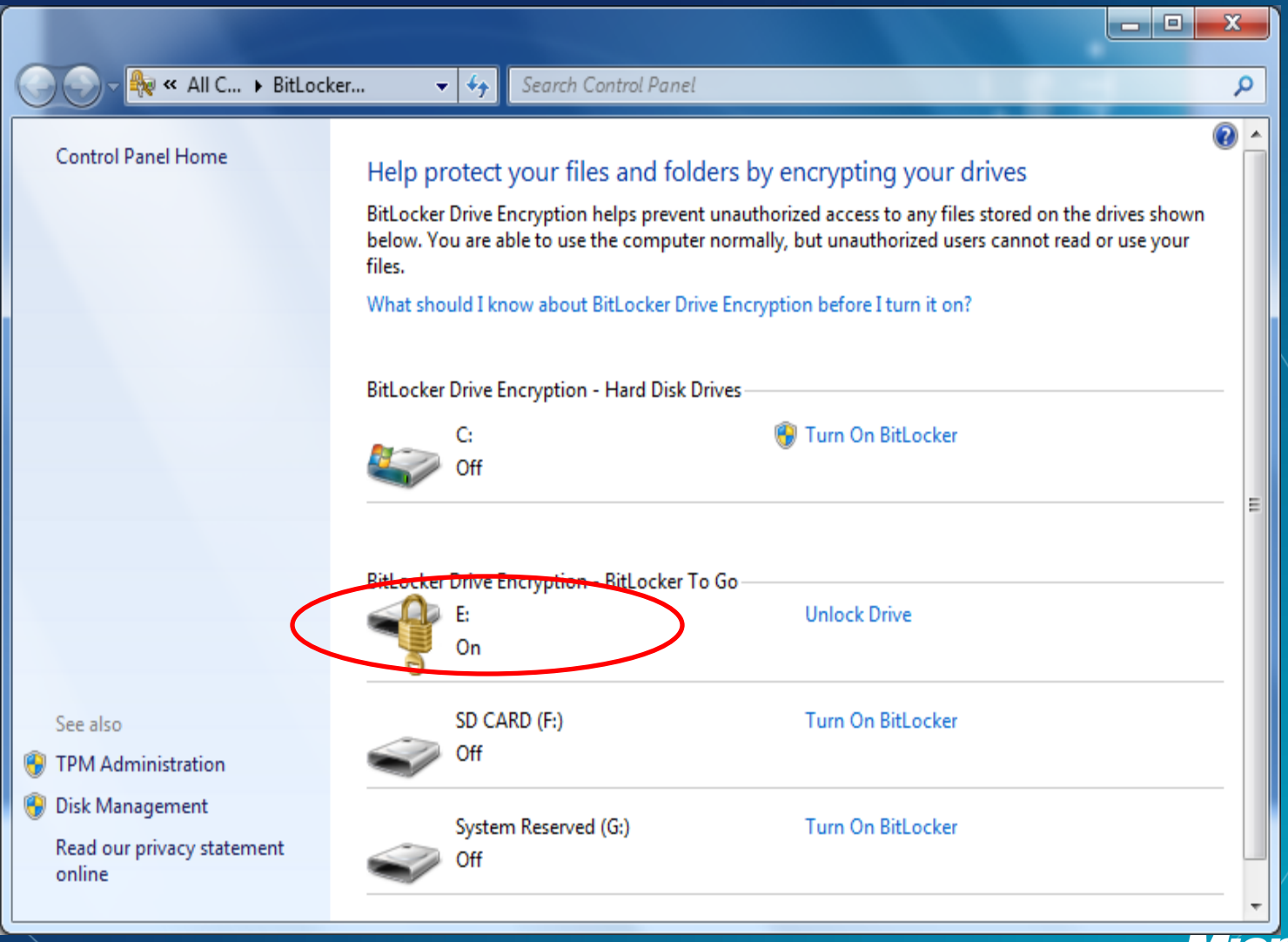
Mounting a BitLocker Drive



- The drive is recognized but it can not be read
- Details are unavailable

Microsoft | Services

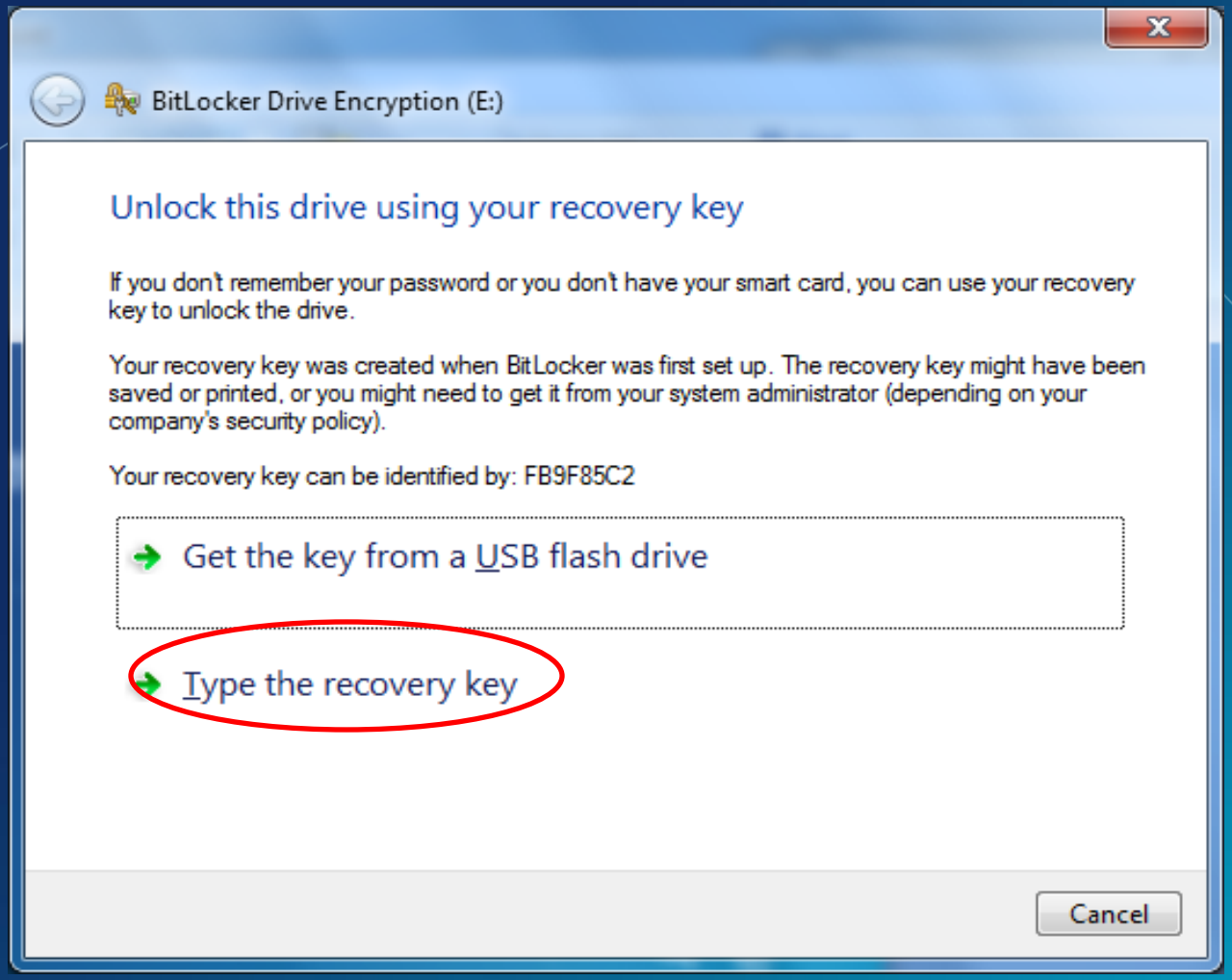
Mounting a BitLocker Drive



- The BitLocker MMC is sees the drive as protected – "Unlock"

Microsoft | Services

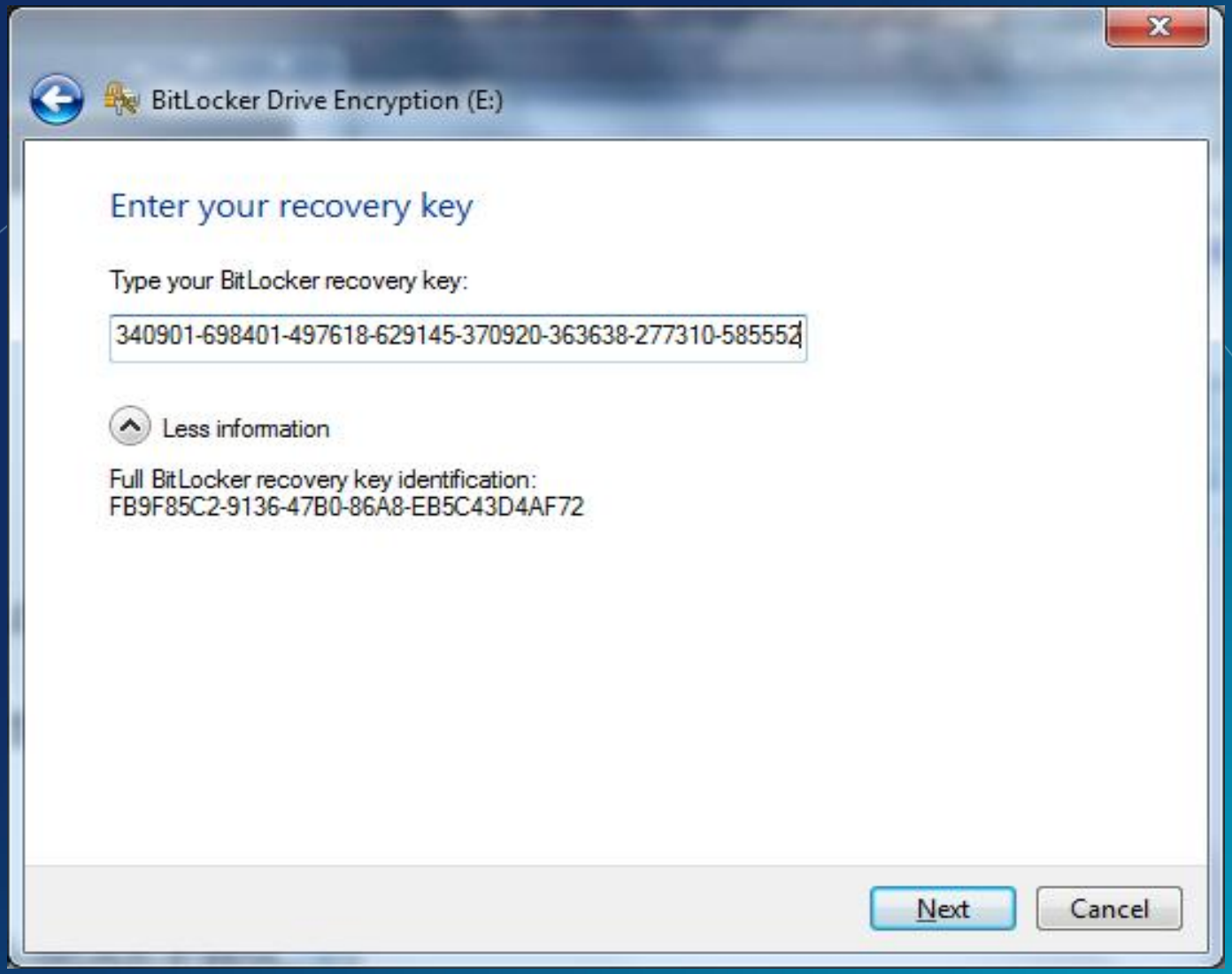
Mounting a BitLocker Drive



- Choose password format – "USB Key" or "Manually"

Microsoft | Services

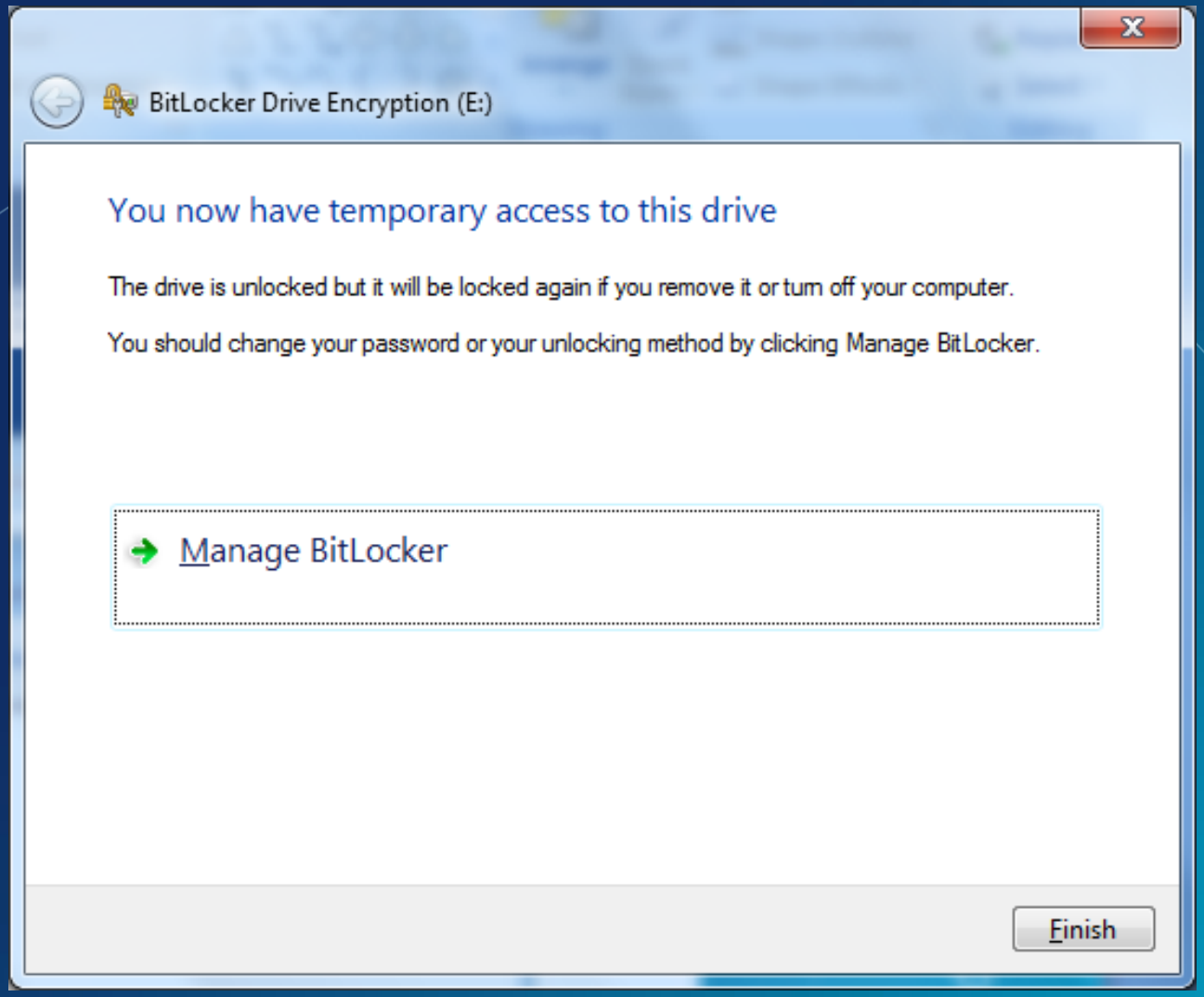
Mounting a BitLocker Drive



- We have the Recovery Key
Password so we type it in

Microsoft | Services

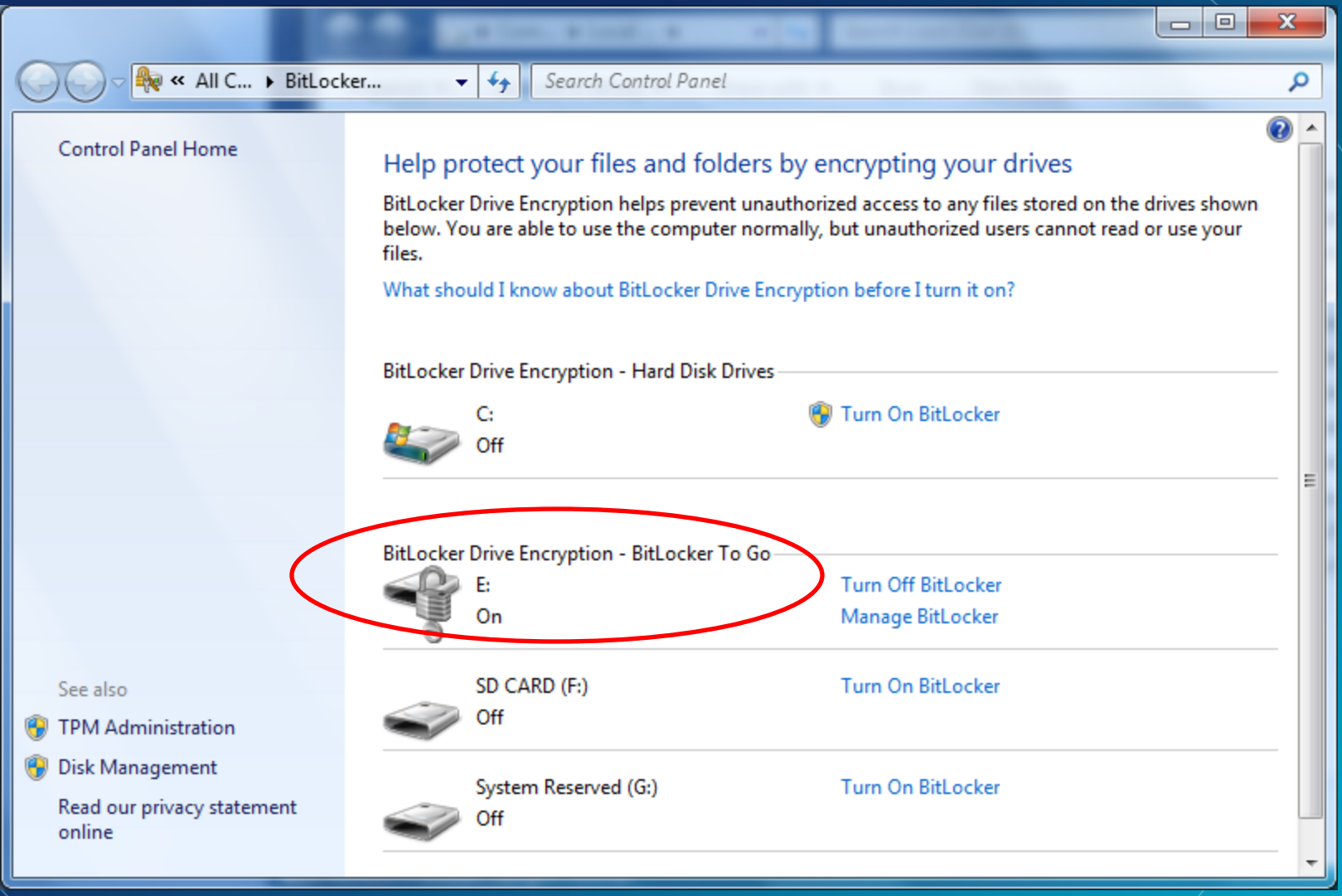
Mounting a BitLocker Drive



- "You can now temporarily access this drive"

Microsoft | Services

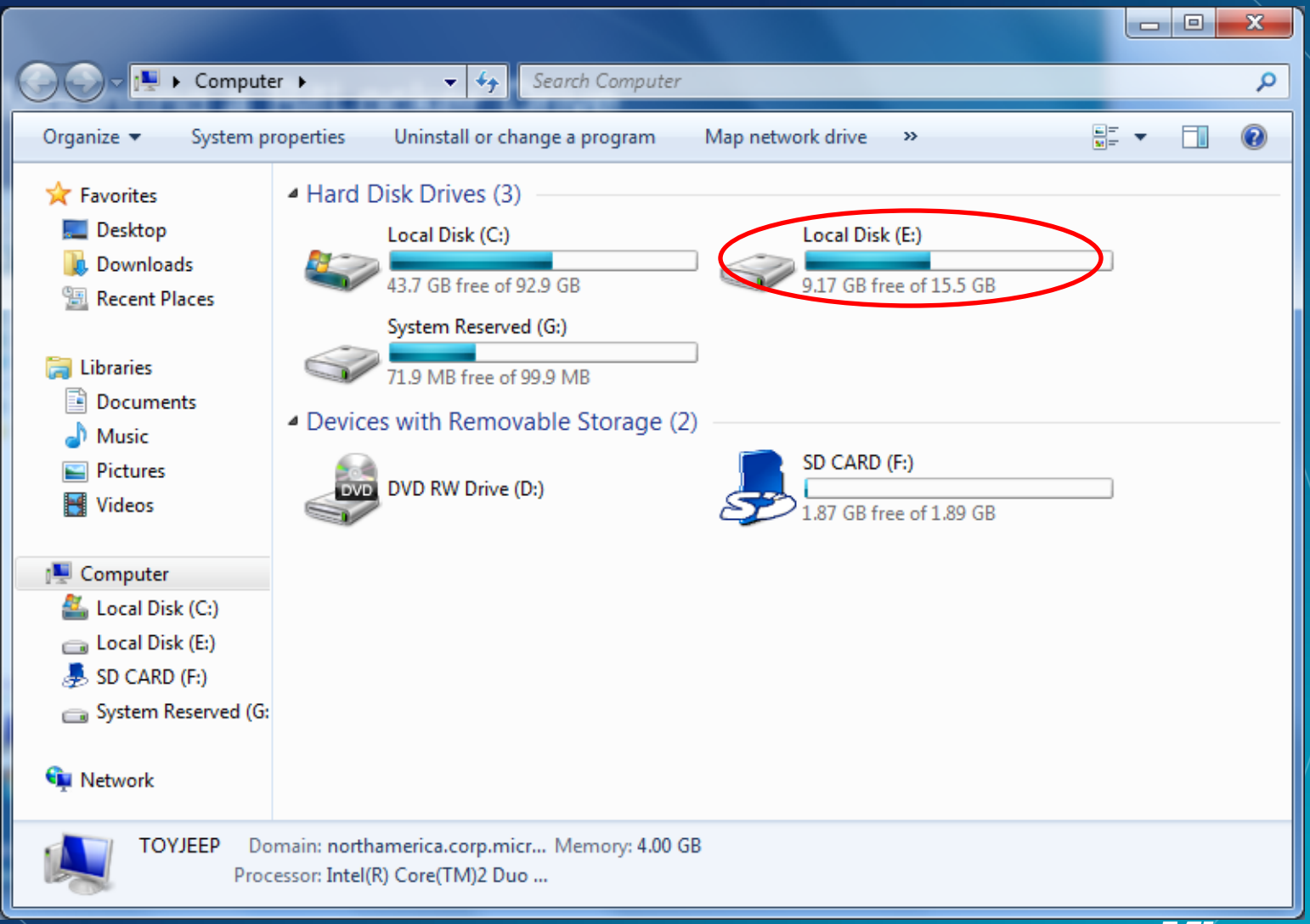
Mounting a BitLocker Drive



- Granted access to a BitLocker protected drive!

Microsoft | Services

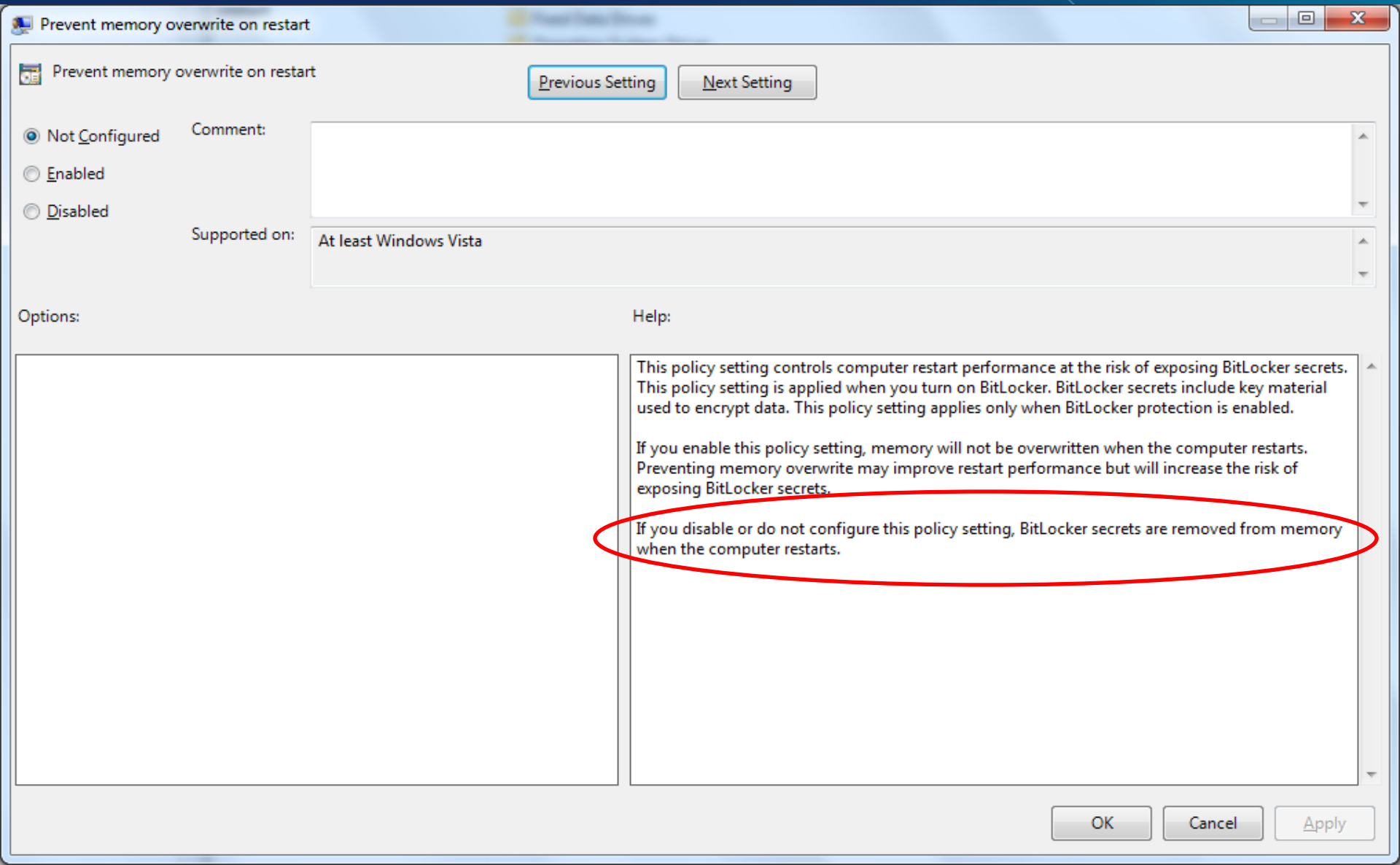
Mounting a BitLocker Drive



- Drive details are now available and we can process the drive

Microsoft | Services

Bitlocker “Cold Boot” attack?



Questions?

Microsoft | Services

Microsoft | Services

Tools for Dealing with BitLocker Evidence

Exploration of Windows 7 Advanced Forensic Topics – Day 3

Microsoft | Services

BitLocker Aware Forensic Tools

- Some tools already handle disk images of encrypted drives provided the investigator has recovery or startup key material

Microsoft | Services

Alternatives

- If the tool used does not support BitLocker, an investigator should obtain 2 images of the suspect system
  - Physical – To allow for booting and testing
  - Logical – To allow for examination in the tool

Alternatives

- The increase in use of encryption and the number of most technically savvy criminal necessitates the move from traditional offline only forensic to a hybrid online / offline approach where two sets of data are collected and examined.

Microsoft | Services

Microsoft | Services

Dealing with BitLocker on a Live System

Exploration of Windows Vista Advanced Forensic Topics – Day 3

Microsoft | Services

Manage-BDE

- In Vista this tool was a script. Manage-BDE.WSF
- In Win7 it was converted to an EXE.
- C:\Windows\System32\Manage-BDE.exe
- Manage-BDE and Repair tool are now part of Windows PE, Windows RE and Windows 7

Manage-BDE

- This tool can manage every aspect of BitLocker on a system
  - Encrypt drives
  - Lock and Unlock drives
  - Decrypt drives
  - Manage BitLocker Keys
  - View Recovery Key information

Manage-BDE

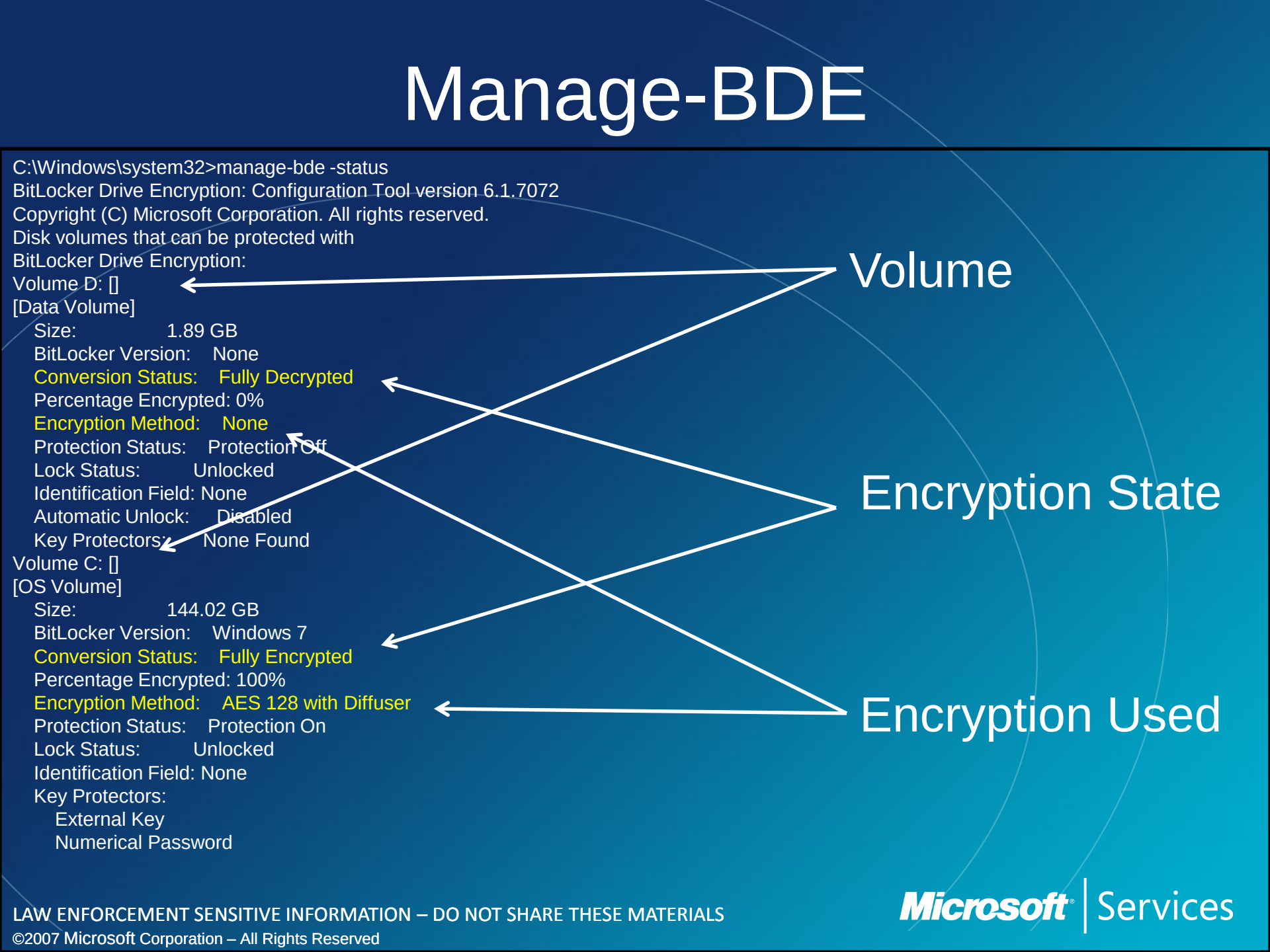
- Viewing if BitLocker is enabled on any drive on a live system:

  Note: You must run as Administrator

  manage-bde -status

Manage-BDE

```
C:\Windows\system32>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 6.1.7072
Copyright (C) Microsoft Corporation. All rights reserved.
Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume D: []
[Data Volume]
    Size:                 1.89 GB
    BitLocker Version:    None
    Conversion Status:    Fully Decrypted
    Percentage Encrypted: 0%
    Encryption Method:    None
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: None
    Automatic Unlock:     Disabled
    Key Protectors:       None Found
Volume C: []
[OS Volume]
    Size:                 144.02 GB
    BitLocker Version:    Windows 7
    Conversion Status:    Fully Encrypted
    Percentage Encrypted: 100%
    Encryption Method:    AES 128 with Diffuser
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: None
    Key Protectors:
        External Key
        Numerical Password
```



Microsoft | Services

Manage-BDE

- What about recovery information?

manage-bde –protectors –get c:

Note: You will need to run this for all drives attached to the system. i.e.

manage-bde –protectors –get d:

manage-bde –protectors –get e:

Manage-BD

```
C:\Windows\system32>manage-bde -protectors -get c:
BitLocker Drive Encryption: Configuration Tool version 6.1.7072
Copyright (C) Microsoft Corporation. All rights reserved.
Volume C: []
All Key Protectors
    External Key:
      ID: {B2EDF460-234E-40D4-8F2D-14DC4D29722C}
      External Key File Name:
        B2EDF460-234E-40D4-8F2D-14DC4D29722C.BEK
    Numerical Password:
      ID: {738C71C6-8CEA-4273-81EC-8A2F23A7DF21}
      Password:
        290103-627220-601392-709918-475816-546480-189739-185042
```


Microsoft | Services

Manage-BDE

- We can even unlock the drive with the manage-bde tool.
- Remember unlocking the drive leaves the data encrypted but simply stores the Volume Master Key (VMK) in the clear so the system can boot without a startup key

manage-bde –unlock c:
manage-bde –autounlock –enable c:

Microsoft | Services

Forensic First Responders

- Inclusion of this tool in any first responder toolkit is a must.
- A script can be leveraged to detect BitLocker on a live system and automatically obtain Recovery Key data and/or unlock the drive

Microsoft | Services

Questions?

Microsoft | Services

30

Minutes

Mounting BitLocker Protected Volumes for Preview

Exercise

Microsoft | Services

30

Minutes

Imaging Implications for BitLocker Protected Drives

Exercise

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Microsoft | Services

30

Minutes

Examining File system Signatures of BitLocker Protected Volumes

Exercise

Microsoft | Services

BitLocker in Win7 at a Glance

Drive Type	Unlock Methods	Recovery Methods	Management	Other requirements
Operating System Drives	TPM TPM+PIN TPM+Startup key TPM+PIN+ Startup Key Startup key	Recovery password Recovery Key Active Directory backup of recovery password Domain Recovery Agent	Robust and consistent Group Policy enforcement Minimum Pin Length	Drive preparation fully integrated in BitLocker setup. System partition size: 200MB without WinRE 400MB with WinRE System partition letterless NTFS file system.
Data Drives *Includes fixed and removable*	Passphrase Smart Card Automatic Unlocking	Same as OS drives	Robust and consistent group policy controls Ability to mandate encryption prior to granting write access	File systems: NTFS FAT FAT32 ExFAT