



Windows Vista™

Windows BitLocker™ Drive Encryption Design Guide

Microsoft Corporation

Published: August 2007

Abstract

This document describes the various aspects of planning for deploying Windows BitLocker Drive Encryption™ for Windows Vista® Enterprise and Windows Vista® Ultimate computers in an enterprise environment. To plan your enterprise deployment of BitLocker, you must first understand your current policies and procedures. This guide provides a systematic approach to help you frame your decision making process before deploying BitLocker and establish BitLocker design strategy.

This guide is intended for use by an infrastructure specialist or system architect. It assumes that you have a good understanding of how BitLocker and TPM work on a functional level.

Microsoft

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.

© 2007 Microsoft Corporation. All rights reserved.

Microsoft, ActiveX, BitLocker, ImageX, Visual Studio, Windows Deployment Services, Windows Vista, and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Windows BitLocker Drive Encryption Design Guide.....	5
Designing a BitLocker Strategy.....	6
Audit your environment.....	6
Evaluate BitLocker authentication methods.....	9
Create a BitLocker support matrix.....	13
Define hardware implementation standards.....	14
Define disk configuration.....	19
Define Active Directory Domain Services configuration.....	20
Define BitLocker and Windows Vista Group Policy settings.....	21
Define password and key management policies.....	24
Define support processes.....	25
Define inventory and tracking processes.....	26
Determine when to configure computers for BitLocker.....	26
Checklist: Designing a BitLocker strategy.....	29
Document your BitLocker design.....	31
Case study: Contoso Pharmaceuticals strategy design.....	35
Appendix: Reviewing BitLocker Requirements.....	48

Windows BitLocker Drive Encryption Design Guide

This document describes the various aspects of planning for deploying Windows BitLocker™ Drive Encryption for Windows Vista® Enterprise and Windows Vista® Ultimate computers in an enterprise environment. To plan your enterprise deployment of BitLocker, you must first understand your current policies and procedures. This guide provides a systematic approach to help you frame your decision making process before deploying BitLocker and establish a BitLocker design strategy.

This guide is intended for use by an infrastructure specialist or system architect. It assumes that you have a good understanding of how BitLocker and TPM work on a functional level.

After you read this guide and finish gathering and documenting your organization's requirements, you will have the information necessary to begin deploying BitLocker using the guidance in the Windows BitLocker Drive Encryption Deployment Guide (<http://go.microsoft.com/fwlink/?LinkId=96685>).

Overview of BitLocker

BitLocker is a data protection feature available in Windows Vista Enterprise and Windows Vista Ultimate for client computers, and in Windows Server® 2008. BitLocker addresses the threats of data theft and of exposure from lost, stolen, or inappropriately decommissioned personal computers by providing a closely integrated solution in Windows Vista.

Data on a lost or stolen computer is vulnerable to unauthorized access, either by running a software attack tool against it or by transferring the computer's hard disk to a different computer. BitLocker helps mitigate unauthorized data access by enhancing Windows Vista file and system protections. BitLocker also helps render data inaccessible when BitLocker-protected computers are decommissioned or recycled.

For more information about the TPM and BitLocker, see the following resources.

- Windows BitLocker Drive Encryption Technical Overview (<http://go.microsoft.com/fwlink/?LinkId=77977>).
- Windows BitLocker Drive Encryption Frequently Asked Questions (<http://go.microsoft.com/fwlink/?LinkId=77976>).
- Trusted Computing Group: Trusted Platform Module (TPM) Specifications (<http://go.microsoft.com/fwlink/?LinkID=69584>).

Designing a BitLocker Strategy

This section describes the critical planning steps that are necessary to deploy BitLocker Drive Encryption. Review and complete these planning tasks before you begin deployment. The following sections will help you collect information that you can use to frame your decision-making process about deploying and managing BitLocker systems. When you design your BitLocker deployment strategy, define the appropriate policies and configuration requirements based on the business requirements of your organization.

Topics in this section

- [Audit your environment](#)
- [Evaluate BitLocker authentication methods](#)
- [Create a BitLocker support matrix](#)
- [Define hardware implementation standards](#)
- [Define disk configuration](#)
- [Define Active Directory Domain Services configuration](#)
- [Define BitLocker and Windows Vista Group Policy settings](#)
- [Define password and key management policies](#)
- [Define support processes](#)
- [Define inventory and tracking processes](#)
- [Determine when to configure computers for BitLocker](#)
- [Checklist: Designing a BitLocker strategy](#)
- [Document your BitLocker design](#)
- [Case study: Contoso Pharmaceuticals strategy design](#)

Audit your environment

To plan your enterprise deployment of BitLocker, you must first understand your current environment. Conduct an informal audit to define your current policies, procedures, and hardware environment. Focus in the following areas that BitLocker might affect:

- [Security policies](#)
- [IT department structure](#)
- [Build process](#)
- [Current and future hardware platform considerations](#)
- [Impact on current systems management tools](#)



Note

Refer to the "Audit Your Environment" section in [Case study: Contoso Pharmaceuticals strategy design](#) to understand how Contoso audited and documented its environment.

Document current security policies

Begin by reviewing your existing corporate security policies as they relate to disk encryption software. If your organization is not currently using disk encryption software, none of these policies will exist. If you are using disk encryption software, then you might need to modify your organization's policies to address the capabilities of BitLocker.

Use the following questions to help you document your organization's current disk encryption security policies:

1. Are there policies to address which computers will use BitLocker and which computers will not use BitLocker?
2. What policies exist to control recovery password and recovery key storage?
3. What are the policies for validating the identity of users that need to perform BitLocker recovery?
4. What policies exist to control who in the organization has access to recovery data?
5. What policies exist to control computer decommissioning or retirement?

Document current IT department structure

Before you can understand how BitLocker affects deployment of new computers and retirement of outdated computers, you should fully understand how your IT department currently handles desktop and server management.

Use the following questions to help you document your current IT department structure:

1. What part of your organization sets the standards for purchasing new computers?
2. Who in your organization builds and configures desktop and laptop computers?
3. Who in your organization builds and configures server systems?
4. Who is responsible for Active Directory Domain Services (AD DS) management?
5. Who is responsible for retiring outdated computers?

Document current build process

Windows Vista offers new deployment tools and technology to streamline deployment. There are also specific deployment and configuration requirements for BitLocker.

Use the questions below to document your current processes before you plan your deployment:

1. Has your organization documented its system build process? If not, ensure that you document your organization's current system build processes.

2. Are computers shipped to you preconfigured from the OEM with a corporate build?
3. Are new computer operating system installations performed on site or are they performed remotely?
4. Do you use one standard corporate image, or do you use many?
5. What tools and methods do you currently use for deployment?
6. Which departments are involved in deployment?
7. Is there any user interaction during deployment?
8. If you use sector-based or image-based deployment, what is included in these images?
9. How are these images serviced over time?
10. What infrastructure dependencies does your build process have (such as SQL Server or Web servers)?

Document current and future hardware platform considerations

Documenting the existing hardware platforms that are deployed in your environment helps you discover how your current environment will support BitLocker.

Use the following questions to document your current and future hardware platform considerations:

1. What laptop hardware platforms are in use?
2. What desktop hardware platforms are in use?
3. Do any of the current hardware platforms have a TPM version 1.2?
4. What is the hardware lifecycle and refresh policy?
5. Are the computers with a TPM version 1.2 Windows Vista® Enterprise or Windows Vista® Ultimate certified?
6. For computers without a TPM version 1.2, does the current BIOS support reading USB devices in the pre-operating system environment?
7. For computers without a TPM version 1.2, is a BIOS update available to add support for reading USB devices in the pre-operating system environment?

Recommendation

Test your individual hardware platforms with the BitLocker system check option while you are enabling BitLocker. After you install Windows Vista, use the BitLocker Control Panel item to start a BitLocker system check on the computer. The system check will ensure that BitLocker can read the recovery information from a USB device and encryption keys correctly before it encrypts the volume. CD and DVD drives cannot act as a block storage device and cannot be used to store the BitLocker recovery material.

▶ To test for system compatibility on a Windows Vista computer

1. Click the Start button, click **Control Panel**, and then click **Security**.
2. Under **BitLocker Drive Encryption**, click **Protect your computer by encrypting data on your disk**.
3. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
4. Click **Turn On BitLocker**.
5. In the **BitLocker Drive Encryption** dialog box, select an authentication method and save the BitLocker recovery material in whatever manner you prefer.
6. On the **Encrypt the volume** page, select the **Run BitLocker system check** check box, and then click **Next**.
7. Restart and log on to the computer, and then check the notification area for any BitLocker notifications.

Assess impact on current systems management tools

Use the following questions to assess what impact BitLocker will have on your existing software distribution tools and methods:

- Do you distribute software or system updates remotely?
- Do you perform overnight distribution?
- Do you reboot users' computers without the users being present?

Depending on the types of authentication methods that you have specified for particular classifications of computers, BitLocker could impact your distribution methods.

For example, if a computer uses the TPM + PIN or TPM + startup key authentication method, and at 2:00 AM you deploy software updates to the computer that requires a reboot, the computer will not continue with the boot process unless the PIN is entered or the startup key is inserted. From a user's perspective, the computer was running when he or she left the day before but has been rebooted overnight. If you currently use wake-on-LAN or a BIOS auto-power-on feature to boot computers for maintenance purposes, these computers will also be affected by the use of the TPM + PIN or TPM + startup key authentication method.

Evaluate BitLocker authentication methods

BitLocker helps prevent unauthorized access to data on lost or stolen computers by:

- Encrypting the entire Windows operating system volume on the hard disk.
- Verifying the boot process integrity.

The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer running Windows Vista has not been tampered with while the system was offline.

In addition, BitLocker offers the option to lock the normal startup process until the user supplies a personal identification number (PIN) or inserts a removable USB device, such as a flash drive, that contains a startup key. These additional security measures provide multifactor authentication and assurance that the computer will not start or resume from hibernation until the correct PIN or startup key is presented.

On computers that do not have a TPM version 1.2, you can still use BitLocker to encrypt the Windows operating system volume. However, this implementation will require the user to insert a USB startup key to start the computer or resume from hibernation, and does not provide the pre-startup system integrity verification offered by BitLocker working with a TPM.

BitLocker key protectors

Key protector	Description
TPM	A hardware device used to help establish a secure root-of-trust. BitLocker only supports TPM version 1.2 and above.
PIN	A user-entered numeric key protector that can only be used in addition to the TPM.
Startup key	An encrypted file that can be stored on most removable media. This key protector can be used alone on non-TPM computers, or in conjunction with a TPM for added security.
Recovery password	A 48-digit number used to unlock a volume when it is in recovery mode. The user must enter this password at boot time by using the function keys (F1-F10).
Recovery key	An encrypted file used for recovering data encrypted on a BitLocker volume.

BitLocker in Windows Vista supports four different authentication modes, depending on the computer's hardware capabilities and the desired level of security.

BitLocker authentication methods

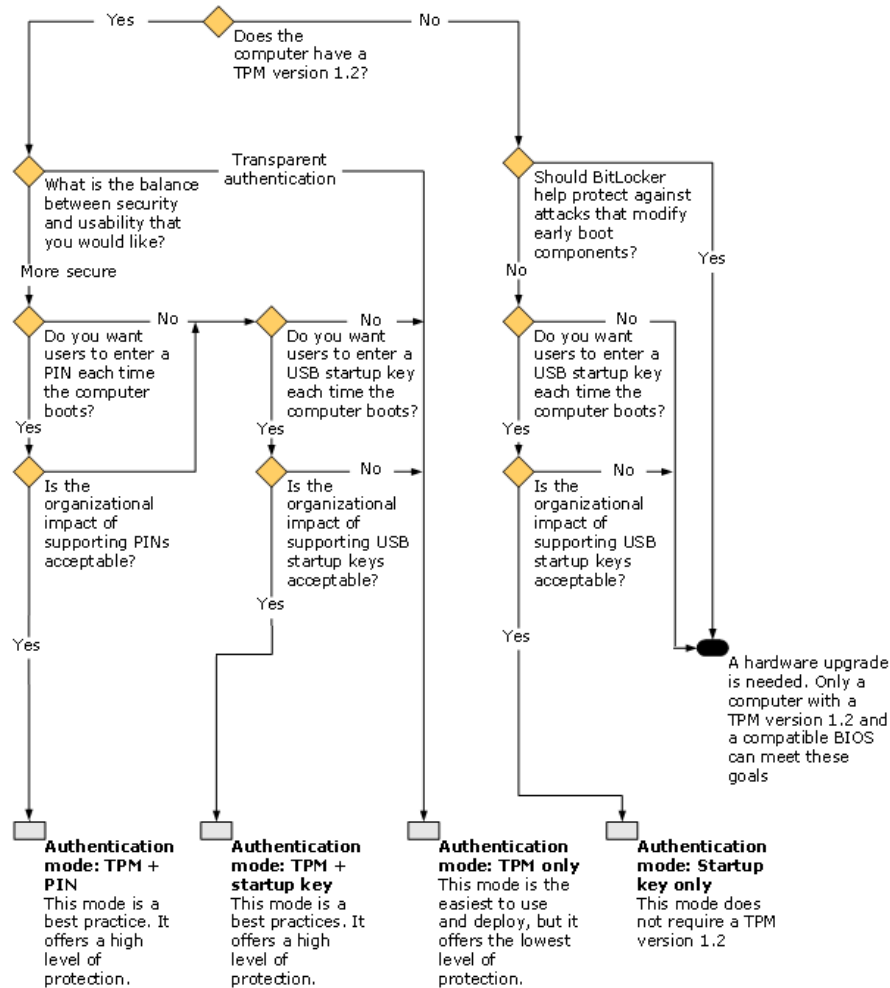
Authentication method	Requires user interaction	Description
TPM only	No	TPM validates early boot

Authentication method	Requires user interaction	Description
		components.
TPM + PIN	Yes	TPM validates early boot components. The user must enter the correct PIN before the start-up process can continue, and before the drive can be unlocked. A Trusted Computing Group (TCG) compliant TPM version 1.2 helps to protect the PIN from brute force attacks.
TPM + startup key	Yes	The TPM successfully validates early boot components, and a USB flash drive containing the startup key has been inserted.
Startup key only	Yes	The user is prompted to insert the USB flash drive that holds the recovery key and/or startup key and reboot the computer.

BitLocker authentication methods differ in the level of protection offered, cost of deployment, and ease of use.

Review the questions and decision-making flowchart below when evaluating authentication modes to help deploy a solution that best meets your security needs.

Decision-making flowchart



Will you support computers without TPM version 1.2?

Determine whether you will support computers that do not have a TPM version 1.2 in your environment. If you choose to support BitLocker on this type of computer, a user must use a USB startup key to boot the system. This requires additional support processes similar to multifactor authentication.

What areas of your organization need a baseline level of data protection?

The TPM-only authentication method will provide the most transparent user experience for organizations that need a baseline level of data protection to meet security policies. It has the lowest total cost of ownership. TPM-only might also be more appropriate for computers that are unattended or that must reboot unattended.

However, TPM-only authentication method offers the lowest level of data protection. This authentication method protects against attacks that modify early boot components, but the level

of protection can be affected by potential weaknesses in hardware or in the early boot components. BitLocker's multifactor authentication methods significantly increase the overall level of data protection.

What areas of your organization need a more secure level of data protection?

If there are areas of your organization where data residing on user computers is considered highly-sensitive, consider the best practice of deploying BitLocker with multifactor authentication on those systems. Requiring the user to input a PIN or USB startup key significantly increases the level of protection for the system.

What multifactor authentication method does your organization prefer?

The protection differences between having a PIN and having a USB startup key cannot be easily quantified, especially because users might leave USB devices in their computers or use the devices for other tasks. Consider each authentication method's impact on Helpdesk support, user education, user productivity, and automated systems management processes. The cost of distributing USB startup keys might make PIN the multifactor method of choice. Users forgetting the PIN or losing the USB startup key will lead to additional requests for recovery. Minimize the Helpdesk impact by considering the guidance you give to users during provisioning (for example, have users specify a 4-digit PIN instead of a 10-digit PIN).



Note

Refer to the "Evaluate BitLocker authentication methods" section in [Case study: Contoso Pharmaceuticals strategy design](#) to understand how Contoso documented its current environment.

Create a BitLocker support matrix

Most enterprise organizations have a mixture of laptop and desktop computers. Even though not all of these computers will contain sensitive data, BitLocker can be deployed across the enterprise.

You can group your enterprise's computers into a mixture of computer-based and role-based groupings:

- Computer-based groupings
 - Desktop computers
 - Laptop computers
 - High-security computers
 - Low-security computers
- Role-based groupings
 - Accounting organization computers
 - Software development computers

- Executive computers
- Tele-working computers
- Remote location computers

Based on the BitLocker key protectors that you have decided to use, and how you have grouped your various computers, document the BitLocker authentication modes in your environment. You can use the sample support matrix table in [Document your BitLocker design](#) in the "Create a BitLocker support matrix" section.

Define hardware implementation standards

Topics in this section

- [TPM hardware configurations](#)
- [Non-TPM hardware configurations](#)
- [OEM-specific requirements](#)

As part of your deployment, refer to the hardware platform information in the Current and future hardware platform section in [Audit your environment](#) to help you decide what hardware platforms will have BitLocker support.

Consider what hardware you will be using for computers that are running BitLocker. You might choose to support BitLocker only on new systems that have a TPM version 1.2, or you might choose to support existing computers that do not have a TPM version 1.2. These computers can use BitLocker in a non-TPM configuration.

TPM hardware configurations

In your deployment plan, identify what TPM-based hardware platforms will be supported. Document the hardware models from an OEM of your choice, so that their configurations can be tested and supported. TPM hardware requires special consideration during all aspects of planning and deployment.

Physical presence interface

The Trusted Computing Group (TCG) TPM specification requires physical presence to perform some TPM administration functions, such as turning on and turning off the TPM. Physical presence means a person must physically interact with the system and the TPM interface in order to confirm or reject changes to TPM status. This typically cannot be automated with scripts or other automation tools unless the individual OEM supplies them. The following are examples of TPM administrative tasks that require physical presence:

- Activating the TPM
- Clearing the existing owner information from the TPM without owner password
- Deactivating the TPM

- Temporarily disabling the TPM without the owner password

TPM states of existence

For each of the TPM states of existence, the TPM can transition into another state (for example, moving from disabled to enabled). The states are not exclusive.

State	Description
Enabled	Most features of the TPM are available. The TPM may be enabled and disabled multiple times within a boot period, if ownership is taken.
Disabled	The TPM restricts most operations. Exceptions include the ability to report TPM capabilities, extend and reset Platform Configuration Register (PCR) functions, and to perform hashing and basic initialization. The TPM may be enabled and disabled multiple times within a boot period.
Activated	Most features of the TPM are available. The TPM may be activated and deactivated only through physical presence which requires a reboot.
Deactivated	Similar to disabled, with the exception that ownership can be taken while deactivated and enabled. The TPM may be activated and deactivated only through physical presence which requires a reboot.
Owned	Most features of the TPM are available. The TPM has an endorsement key and storage root key, and the owner knows information about owner authorization data.
Un-owned	The TPM does not have a storage root key and may or may not have an endorsement key.

Important

BitLocker cannot use the TPM until it is in the following state: enabled, activated, and owned. When the TPM is in this state and only when it is in this state, all operations are available.

The state of the TPM exists independent of the computer's operating system. Once the TPM is enabled, activated, and owned, the state of the TPM is preserved if the operating system is reinstalled.

Endorsement keys

For a TPM to be usable by BitLocker, it must contain an endorsement key, which is an RSA key pair. The private half of the key pair is held inside the TPM and is never revealed or accessible outside the TPM. If the TPM does not contain an endorsement key, BitLocker will force the TPM to generate one automatically as part of BitLocker setup.

An endorsement key can be created at various points in the TPM's lifecycle, but needs to be created only once for the lifetime of the TPM. If an endorsement key does not exist for the TPM, it must be created before TPM ownership can be taken.

You can create the endorsement key with any one of the following:

- BitLocker user interface when you take TPM ownership. For guidance about how to take ownership of the TPM, see the Windows Trusted Platform Module Step-by-Step Guide (<http://go.microsoft.com/fwlink/?LinkID=82830>).
- TPM WMI providers (<http://go.microsoft.com/fwlink/?LinkId=93478>)
 - For a sample WMI script, download the Microsoft BitLocker Deployment Code Samples (<http://go.microsoft.com/fwlink/?LinkID=96685>).

For more information about the TPM and the TCG, see the Trusted Computing Group: Trusted Platform Module (TPM) Specifications (<http://go.microsoft.com/fwlink/?LinkID=69584>).

Non-TPM hardware configurations

Your existing non-TPM hardware might be able to run BitLocker with additional support.

Use the following questions to identify issues that might affect your deployment in a non-TPM configuration:

- Does the current hardware meet the minimum specifications to support Windows Vista? If it is not capable of supporting Windows Vista, is the hardware upgradeable, or is it a better choice to replace it?
- Do you have budget for USB flash drives for each of these computers?
- What is the expected service life of these USB devices?
- Do your existing non-TPM devices support USB devices at boot time?

Recommendation

Test your individual hardware platforms with the BitLocker system check option while you are enabling BitLocker. After you install Windows Vista, use the BitLocker Control Panel item to start a BitLocker system check on the computer. The system check will ensure that BitLocker can read the recovery information from a USB device and encryption keys correctly before it encrypts the volume. CD and DVD drives cannot act as a block storage device and cannot be used to store the BitLocker recovery material.

To test for system compatibility on a Windows Vista computer

1. Click the Start button, click **Control Panel**, and then click **Security**.
2. Under **BitLocker Drive Encryption**, click **Protect your computer by encrypting data on your disk**.
3. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
4. Click **Turn On BitLocker**.
5. In the **BitLocker Drive Encryption** dialog box, select an authentication method and save the BitLocker recovery material in whatever manner you prefer.
6. On the **Encrypt the volume** page, select the **Run BitLocker system check** check box, and then click **Next**.
7. Restart and log on to the computer, and then check the notification area for any BitLocker notifications.

OEM-specific requirements

Choose computers that have a TPM version 1.2 that is certified for Windows Vista. For TPM-compliant computers, each manufacturer will likely have a different default shipping configuration. Use the following questions to help plan for automated deployment:

- **What tools does the OEM provide to automate TPM management?**

Investigate what management tools your OEM provides for managing the BIOS configuration of your computers. These tools should be comprehensive enough to manage the state of the TPM and the BIOS administrator password if required. Without these tools, several manual steps could be interjected into your automated build process.
- **When in the computer's lifecycle is the endorsement key for the TPM generated?**

Before you can use a TPM, it must have an endorsement key applied to it. The endorsement key is valid only for the TPM with which it is associated, and it must be tracked for the entire life of the computer. There are various times when this endorsement key can be applied to the platform. The manufacturer can do this during the build process, or a value-added reseller or the computer owner (consumer) can do it. It is important to know where or when the

endorsement key is applied because this information must be kept secure and tracked for the entire life of the computer.

You can automate creation of the endorsement key during your build process, or you can rely on the manufacturer or OEM to apply the endorsement key. If you choose to create the endorsement key during your build process, and if an endorsement key does not exist, see the sample WMI script, `enablebitlocker.vbs`, which is available as part of the Microsoft BitLocker Deployment Code Samples (<http://go.microsoft.com/fwlink/?LinkID=96685>). The sample script automatically creates an endorsement key when taking ownership of the TPM. If you use the BitLocker user interface to enable BitLocker, an endorsement key will be created automatically when taking ownership of the TPM.

- **How is the TPM configured in the BIOS when it is shipped to your organization?**

From a deployment perspective it is important to have computers shipped to you in a state that is secure and that allows you to streamline your deployment process. Computers that are equipped with a TPM and shipped to your organization in a disabled state will require physical presence at some point during your build process to enable it. This physical presence requirement will inject a manual step into your deployment. Some OEMs might provide automation tools to override this manual step, but this depends on each OEM's implementation of the TPM technology.

The TPM can also be shipped in an enabled state. This allows you to automate the activation and ownership process within Windows Vista, using the BitLocker WMI providers.

- **Does the OEM require a BIOS administrator password to use the TPM?**

As a part of the physical presence specification, the OEM might require that a BIOS administrator password be set to enable and activate the TPM. This requirement might also inject a manual step into your deployment process. Again, OEMs might provide automation tools to specify the password. You might consider having the OEM ship the computer not only with the TPM enabled, but also with a default BIOS administrator password for your organization. You can then change the BIOS password during the build process if the OEM provides the appropriate automation tools.

- **How is the boot order on the BitLocker computers configured?**

The boot order on a computer can affect your build process, if you choose to build your computers using a bootable DVD. If the CD or DVD drive is first in the boot order, or before the hard disk that will boot Windows Vista, then it would be included in the measurement of the boot process that BitLocker performs. However, this would be blocked when you try to enable BitLocker, forcing you to eject the CD or DVD and restart the computer.

If the boot order is configured with the hard disk that will boot Windows Vista before the CD or DVD drive, then the CD or DVD is not measured during the system boot process. In this configuration, you still need to remove any CD or DVD bootable media before enabling BitLocker, but you do not have to restart the computer. However, you can programmatically eject any CD or DVD media and then continue enabling BitLocker.

If you are planning to automate your build process completely, ensure that the boot order of your target computers is configured in a way to support this type of automation.



Note

Refer to the OEM-specific configuration section in [Case study: Contoso Pharmaceuticals strategy design](#) to understand how Contoso has planned to support BitLocker systems.

Define disk configuration

To function correctly, BitLocker requires a specific disk configuration. Configuring the disk drives of your computer is the most critical step when preparing a computer to use BitLocker encryption.

BitLocker requires two NTFS partitions: one for the operating system, and one for the system. The system partition should be at least 1.5 GB for BitLocker, Windows Vista recovery, and Windows Vista servicing. The operating system partition must meet the Windows Vista installation requirements.

Windows Recovery Environment (Windows RE) is an extensible recovery platform that is based on Windows Pre-installation Environment (Windows PE). When the computer fails to start, Windows automatically transitions into this environment, and the Startup Repair tool in Windows RE automates the diagnosis and repair of an unbootable Windows Vista installation. Windows RE also contains the drivers and tools that are needed to unlock a volume protected by BitLocker by providing a recovery key or recovery password. To use Windows RE in conjunction with BitLocker, the Windows RE boot image must reside on a volume that is not protected by BitLocker. To use Windows RE in conjunction with BitLocker, follow the partitioning guidelines in the table below.

BitLocker partitioning guidelines

Disk configuration	Partition 1	Partition 2	Partition 3
Windows RE and BitLocker on separate partitions	System Type 0x7 1.5GB (Active)	Windows RE Type 0x27 1GB	Windows Vista Type 0x7
Windows RE and BitLocker on same partition	Windows RE Type 0x7 1.5GB (Active)	System Windows Vista Type 0x7	Not needed



Caution

If you place Windows RE and BitLocker on the same (active) partition, you cannot perform a restore from a Complete PC backup without using a Windows RE CD. This is because Complete PC must always restore the active partition, but fails do so when the

files that Windows RE uses to start from are also on the active partition. To ensure that you can perform a complete PC backup without requiring a Windows RE CD, install Windows RE and BitLocker on separate partitions.

Windows RE can also be used from boot media other than the local hard disk. If you choose not to install Windows RE on the local hard disk of BitLocker-enabled computers, you can use alternate boot methods, such as Windows Deployment Services, CD-ROM, or USB flash drive, for recovery.

Recommendation

Install the Windows RE tools on all of the computers on which you plan to use BitLocker, or give support personnel an alternate Windows RE boot method, such as Windows Deployment Services or removable media. Windows RE enables support personnel to use recovery keys and passwords to unlock BitLocker-protected volumes.

Define Active Directory Domain Services configuration

BitLocker integrates with Active Directory Domain Services (AD DS) to provide centralized key management. By default, no recovery information is backed up to Active Directory. Administrators can configure Group Policy settings to enable backup of BitLocker or TPM recovery information. Before configuring these settings, a domain administrator must ensure that the AD DS schema has been extended with the necessary storage locations and that access permissions have been granted to perform the backup. The following recovery data can be saved for each computer object:

- **Recovery password**

A 48-digit recovery password used to recover a BitLocker-protected volume. Users enter this password to unlock a volume when BitLocker enters recovery mode.

- **Key package data**

With this key package and the recovery password, you will be able decrypt portions of a BitLocker-protected volume if the disk is severely damaged. Each key package will only work with the volume it was created on, which can be identified by the corresponding volume ID.

- **TPM owner password hash**

When ownership of the TPM is taken a hash of the ownership password can be taken and stored in AD DS. This information can then be used to reset ownership of the TPM.

To take advantage of this integration, you must extend the Active Directory schema and configure BitLocker-specific Group Policy objects. Your environment must meet the following minimum requirements to enable schema extension:

- All domain controllers in the domain must be at least Windows Server 2003 SP1.
- The account that you use to update the Active Directory schema must be a member of the Schema Admins group.



Note

If you have a Windows Server® 2008 Beta 3 domain controller in your environment, the schema extensions are already in place and do not need to be updated.

By default, domain administrators are the only users that will have access to BitLocker recovery information. When you plan your support process, define what parts of your organization need access to BitLocker recovery information. Use this information to define how the appropriate rights will be delegated in your AD DS environment.

Recommendation

We recommend that you extend your Active Directory schema to support storing BitLocker recovery material in AD DS. If you have more than one AD DS forest in your environment, you must extend the schema in each forest that contains BitLocker computers.

For more information about Active Directory configuration and BitLocker recovery, see the following resources:

- Configuring Active Directory to Back up Windows BitLocker Drive Encryption and Trusted Platform Module Recovery Information (<http://go.microsoft.com/fwlink/?LinkId=82827>).
- Retrieving a Recovery Password (<http://go.microsoft.com/fwlink/?LinkId=93476>).
- BitLocker Repair Tool (<http://go.microsoft.com/fwlink/?LinkId=91736>).

Define BitLocker and Windows Vista Group Policy settings

To control the user experience in the BitLocker Control Panel item and to modify other configuration options, you can use Group Policy or local computer policy settings. How you choose to configure these policy settings depends on how you implement BitLocker and what level of user interaction will be allowed.

BitLocker Group Policy settings

BitLocker Group Policy settings are found in Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\

- Turn on BitLocker backup to Active Directory Domain Services
- Control Panel Setup: Configure recovery folder
- Control Panel Setup: Configure recovery options
- Control Panel Setup: Enable advanced startup options
- Configure encryption method
- Prevent memory overwrite on startup
- Configure TPM platform validation profile

TPM Services Group Policy settings

TPM Services Group Policy settings are found in Computer Configuration\Administrative Templates\System\Trusted Platform Module Services\

- Turn on TPM backup to Active Directory Domain Services
- Configure the list of blocked TPM commands
- Ignore the default list of blocked TPM commands
- Ignore the local list of blocked TPM commands

Administrative templates to configure these Group Policy settings are pre-installed by Windows and made available through gpedit.msc. For Windows Vista, these templates are located in %windir%\PolicyDefinitions and named **tpm.admx** and **VolumeEncryption.admx**.

Recommendation

It is best practice always to require backup of recovery information for both the TPM and BitLocker to AD DS. Configure the Group Policy settings below for your BitLocker-protected computers.

BitLocker Group Policy setting	Configuration
BitLocker Drive Encryption: Turn on BitLocker backup to Active Directory Domain Services	Require BitLocker backup to AD DS (Passwords and key packages)
Trusted Platform Module Services: Turn on TPM backup to Active Directory Domain Services	Require TPM backup to AD DS

Refer to the "Define BitLocker and Windows Vista Group Policy settings" section in [Case study: Contoso Pharmaceuticals strategy design](#) to understand how Contoso intends to support BitLocker systems.

FIPS settings

You can configure the Federal Information Processing Standard (FIPS) settings in Windows Vista for FIPS compliance. As an effect of FIPS compliance, users cannot create or save a BitLocker recovery password. You can optionally create a recovery key, however. When FIPS is disabled, based on the existing Group Policy, users must create and save a recovery key or recovery password while enabling BitLocker using the user interface.

Important

If you enable this setting, users will be unable to save a recovery password to any location. This includes AD DS and network folders. In addition, you cannot use WMI or the BitLocker Drive Encryption wizard to create a recovery password.

You can save the optional recovery key to a USB flash drive. Because recovery passwords cannot be saved to AD DS when FIPS is enabled, Windows Vista will display an error if AD DS backup is required by Group Policy.

You can edit the FIPS setting by using the Security Policy Editor (Secpol.msc) or by editing the Windows registry. You must be an administrator to perform either of these procedures.

The FIPS setting is located in the Security Policy Editor at Local Policies\Security Options\System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.

▶ To edit the FIPS setting using the Security Policy Editor

1. Click the Start button, type **secpol.msc** into the **Start Search** box, and then click **secpol.msc**.
2. `uac_appears`
3. In the console tree, expand Local Policies, and then click Security Options.
4. In the details pane, right-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**, and then click **Properties**.
5. Enable or disable the setting, and then click **OK**.

▶ To edit the FIPS setting using the Windows registry

1. Click the Start button, type **regedit** into the **Start Search** box, and then click **regedit**.
2. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
3. In Registry Editor, expand **HKEY_LOCAL_MACHINE**, expand **SYSTEM**, expand **CurrentControlSet**, expand **Control**, expand **LSA**, and then click **FipsAlgorithmPolicy**.
4. To enable the setting, double-click **Enabled**, and change the value data to 1.

Other Group Policy settings

Windows Vista computers will Sleep frequently to conserve power when idle and help extend system battery life. When a computer transitions to Sleep, open programs and documents are persisted in memory. When resuming from Sleep, users are not required to re-authenticate with a PIN or USB startup key to access encrypted data. This might lead to conditions where data security is compromised. In unusual circumstances, where increased data protection is required, organizations using BitLocker may wish to use Hibernate instead of Sleep. This setting does not have an impact on TPM-only mode, because it provides transparent user experience at startup and resuming from Sleep/Hibernate states.

You can use the following Group Policy settings to disable all available sleep states:

Power management Group Policy settings

Setting	Configuration
Allow Standby States (S1-S3) When Sleeping (Plugged In)	Disabled
Allow Standby States (S1-S3) When Sleeping (Battery)	Disabled

In addition to power management Group Policy settings, you might also consider hiding the drive letter of the system partition from Windows Shell (My Computer, folder views, etc.). The drive letter is still visible from the command prompt. This is the unencrypted partition that BitLocker and other Windows components use when booting the system. This setting can be used to prevent users from easily saving data to this partition in an unencrypted state.

The following policy setting can be used to hide drive letters from Windows Explorer:

Windows Explorer Group Policy settings

Setting	Configuration
Hide these specified drives in My Computer	System partition drive letter



Note

This setting allows hiding only drive letters A through D. If you need to hide other drive letters, see Microsoft Knowledge Base article 231289 (<http://go.microsoft.com/fwlink/?LinkId=93477>).

Define password and key management policies

In the previous sections, you determined how your organization will use BitLocker. Now begin to define policies for managing the recovery material that BitLocker creates. Depending on your configuration specifications, there are many different processes to manage the recovery information for BitLocker. For example, you might choose to use recovery keys, and recovery keys must be managed.

Define your security policies to support BitLocker password and key management. These policies should be comprehensive enough to ensure that the information is secure, but not so restrictive as to make supporting BitLocker difficult.

The list below contains security policy examples:

- Always require backup of recovery passwords to AD DS.
- Always require backup of key package data to AD DS.
- Always require backup of TPM owner information to AD DS.

- Use recovery keys along with recovery passwords as a backup or alternate recovery method.
- If you are using TPM + PIN or USB startup keys, change them regularly.
- On TPM-enabled computers, use a BIOS administrator password to prohibit unauthorized access to TPM administrative functions.
- Educate users that they should not store key material such as USB startup keys with the system that such material unlocks.
- If you use recovery keys, store them in a central location for purposes of support and disaster recovery.
- Back up recovery material to secure offline storage for long-term recoverability.

Define support processes

In the previous section, you defined how BitLocker recovery material will be managed in your environment. You should now consider how this information will be used in the support process. Prepare to use the recovery material saved by BitLocker by defining and testing the necessary support processes.

- **Document what recovery material is created by BitLocker and where it is stored**
For example, you might have chosen to use recovery keys in addition to recovery passwords. Because recovery keys are not stored in AD DS, you might choose to store them in another secure, documented location. Document what tools are available for accessing this information, and any associated procedures or approval processes.
- **Determine who in your organization will have access to BitLocker recovery material**
You might choose to limit the number of support personnel who have access to this type of information. In some organizations with tiered Helpdesk support, access to this information might exist only in the top tier. Conversely, in some organizations first-tier Helpdesk personnel might have access to the recovery material for faster end-user recovery. Regardless of how you choose to grant access to this recovery information, ensure that only the individuals who need appropriate access have it.
- **Develop processes for remote and local recovery**
Local recovery is the recovery of a BitLocker-protected computer when an IT technician is physically present at the computer. Remote recovery is the recovery of a BitLocker-protected computer by the user of the computer when an IT technician is not physically present. Fully document how users are supported, whether they are considered local or remote.
- **Define the end-to-end support model that is used to support BitLocker for each of the supported BitLocker configurations**
You can use the [Create a BitLocker support matrix](#) topic to help create the end-to-end support model for BitLocker.



Note

Refer to the "Define password and key management policies" section in [Case study: Contoso Pharmaceuticals strategy design](#) to understand how Contoso documented its current environment.

Define inventory and tracking processes

After you have deployed BitLocker-protected computers in your environment, it is important to inventory these computers. You might need to manage these systems differently than most of your environment. Management tasks, such as BIOS updates, might need to be done differently than computers that are not protected with BitLocker. If you choose to use multi-factor BitLocker authentication, this inventory process will be more important to your organization because of the impact on systems management tools. Develop a strategy for managing and tracking these computers.

Determine when to configure computers for BitLocker

When choosing a deployment method for BitLocker computers, there is no single recommended method. You should first decide at what point you will configure and enable BitLocker on targeted computers. Configuration of BitLocker could fall into one or more of the following categories depending on your organizations management and deployment processes:

- [Pre-build configuration](#)
- [Configuration during the build process](#)
- [Post-build configuration](#)
- [User-initiated configuration](#)

Pre-build configuration

In the pre-build configuration phase you may choose to make BIOS setting changes to enable and activate the TPM, meet the physical presence requirement, and set BIOS passwords. However this phase of the deployment may not necessarily be done by your organization it could be a service provided by your OEM.

If you or your OEM complete pre-build configuration, you must still configure the hard disk for BitLocker and enable BitLocker, either during or after the build process.

Configuration during the build process

During the build process you may choose to enable and configure BitLocker. Take the following points into consideration when using this method:

1. A user must be physically present to enable and activate a TPM. If the OEM has enabled and activated the TPM, or if the computer has no TPM, then this restriction does not apply.

2. To enable recovery information to be stored in AD DS, BitLocker must be enabled after the computer has joined the AD DS domain.
3. Consider starting encryption at the very end of the build process to minimize the impact that encryption might have on system performance. This is especially important if you have additional tasks to perform on the computers, such as installing applications.

You can use three Windows deployment methods to configure and enable BitLocker during the build process: Windows Deployment Services, unattended installation, and Windows imaging.

Windows Deployment Services

Windows Deployment Services is the updated and redesigned version of Remote Installation Services (RIS). Windows Deployment Services is part of the Windows Server® 2008. A Windows Deployment Services update is also available for Windows Server 2003.



Note

This document does not provide high-level information about how Windows Deployment Services works and its benefits. To learn more about Windows Deployment Services, see the Windows Vista Deployment Step by Step Guide (<http://go.microsoft.com/fwlink/?LinkID=53553>).

Typically, you use Windows Deployment Services when you want to install pre-configured custom images to computers that have no operating system installed, or to computers whose existing data you want to overwrite.

Unattended installation

In the unattended installation design, an image of Windows Vista is deployed to computers using an unattended answer file. Unattended installation is a Windows installation method that does not require user interaction during installation. Windows Setup works with an unattended installation answer file to automate online installations and customizations of Windows. This method is useful for large-scale rollouts and for achieving consistency and precision in the configuration of each computer.

Unattended installation requires the creation of one or more answer files that contain customizations for an installation. For example, you can change the Internet Explorer configuration or partition and format hard disks.



Note

This document does not provide high-level information about how unattended setup works and its benefits. To learn more about unattended installation, see the Unattended Installation Settings Reference (<http://go.microsoft.com/fwlink/?LinkId=93479>).

Windows imaging

Windows imaging is a Windows installation method that uses the ImageX command-line tool and Windows image (.wim) format files. Windows imaging enables you to automate much of the BitLocker setup, but requires that you perform some final setup tasks manually.



Note

This document does not provide high-level information about how ImageX works and its benefits. To learn more about ImageX, see the ImageX Technical Reference (<http://go.microsoft.com/fwlink/?LinkId=93480>).

Windows imaging with ImageX requires that all of the existing data on the hard drive, including any existing operating system, be overwritten. Typically, you use a Windows imaging with ImageX when you want to install pre-configured custom images to computers that have no operating system installed, or to computers whose existing data you want to overwrite.

Post-build configuration

The post-build configuration method is very flexible and can be accomplished using numerous methods. You can configure a computer for BitLocker immediately after the system build process completes, or at a later time after the computer is delivered to the end user. The IT administrators in your organization may choose to enable and configure BitLocker at a later time using another software distribution tool, Group Policy scripting, or logon scripts.

Before you enable BitLocker, the hard disk must be partitioned to meet BitLocker requirements. If the computer was not prepared for BitLocker during the build process, you must use the BitLocker Drive Preparation Tool (<http://go.microsoft.com/fwlink/?LinkId=83261>) to prepare the hard disk BitLocker. After you have prepared the hard drive for BitLocker, you can use either the **manage-bde.wsf** tool or the BitLocker and TPM WMI providers to enable and configure BitLocker for computers that already have Windows Vista installed.

Recommendation

The following table shows recommendations for using both of these methods.

Post-build method	Number of computers
Manage-bde.wsf	25 or fewer
BitLocker and TPM WMI providers	Large enterprise deployments

User-initiated configuration

You may choose to provide BitLocker as a service to individual internal organizations or to the end users themselves. A custom solution could be created to allow users the ability to selectively enroll and configure their computers to use BitLocker.







Checklist: Designing a BitLocker strategy









This checklist includes cross-reference links to important topics that will assist you with designing a BitLocker strategy for your organization.

Note

Complete the tasks in this checklist in order. When a reference link takes you to a conceptual topic, review the topic and complete the tasks detailed in the topic, and then return to this topic so that you can proceed with the remaining tasks in this checklist.

Checklist: Designing a BitLocker strategy

	Task	Reference
<input type="checkbox"/>	Audit your environment to determine your current hardware and software infrastructure.	 Audit your environment
<input type="checkbox"/>	Select authentication methods that your computers can support and that meet your desired level of protection.	 Evaluate BitLocker authentication methods
<input type="checkbox"/>	Document the BitLocker authentication methods and platforms that you will support by creating a support matrix.	 Create a BitLocker support matrix
<input type="checkbox"/>	Using the data you have gathered from auditing your environment and evaluating the BitLocker authentication methods, define your organization's hardware implementation standards for BitLocker.	 Define hardware implementation standards
<input type="checkbox"/>	Define how you will configure the hard disk for BitLocker.	 Define disk configuration
<input type="checkbox"/>	Determine whether to store	 Define Active Directory Domain Services

	Task	Reference
	BitLocker recovery information in Active Directory Domain Services.	configuration
<input type="checkbox"/>	Determine which Group Policy settings you would like to apply for BitLocker and how to configure those settings for your environment.	 Define BitLocker and Windows Vista Group Policy settings
<input type="checkbox"/>	Define how your organization will manage BitLocker keys and passwords.	 Define password and key management policies
<input type="checkbox"/>	Define internal processes for managing BitLocker and the computers that use it.	 Define support processes
<input type="checkbox"/>	Define a process for maintaining an inventory of your BitLocker-protected computers.	 Define inventory and tracking processes
<input type="checkbox"/>	Based on your organization's build processes, determine when and how to configure computers for BitLocker.	 Determine when to configure computers for BitLocker
<input type="checkbox"/>	Review the hardware, software, and client requirements for deploying BitLocker.	 Appendix: Reviewing BitLocker Requirements
<input type="checkbox"/>	Document your BitLocker strategy for implementation in your organization.	 Document your BitLocker design
<input type="checkbox"/>	Use the Windows	 Windows BitLocker Drive Encryption

	Task	Reference
	BitLocker Drive Encryption Deployment Guide to implement your BitLocker strategy.	Deployment Guide (http://go.microsoft.com/fwlink/?LinkID=96685)

Document your BitLocker design

You can use the tables in this section to document your BitLocker strategy.

- [Audit your environment](#)
- [Create a BitLocker support matrix](#)
- [Define hardware implementation standards](#)
- [Define disk configuration](#)
- [Define Active Directory Domain Services configuration](#)
- [Define BitLocker and Windows Vista Group Policy settings](#)
- [Define password and key management policies](#)
- [Define support processes](#)
- [Define inventory and tracking processes](#)

Audit your environment

You can use these tables in coordination with the [Audit your environment](#) topic to document your organization's topography, scale, and core requirements.

Current IT organization

You can use the following table to document service roles, users, and computers in your organization.

IT organization	Service roles	Users supported	Computers supported

System configuration and build processes

The following table shows how you can document your system configuration process.

IT department	System configuration	Configuration location

You can use the following table to document how systems are built in your organization.

Business unit	Windows deployment method	Windows delivery method	Application delivery method	Infrastructure dependencies

Understanding the BitLocker functionality that you want to enable can help you select the appropriate goals for your deployment. Specify whether your scenario requires each of the areas of functionality in the following table.

Functionality	Yes/No
Use BitLocker on computers with a TPM	
Use BitLocker on computers without a TPM	

Create a BitLocker support matrix

Based on the BitLocker key protectors that you have decided to use, and how you have grouped your various computers, document the BitLocker authentication methods in your environment. You can use the following table as a guideline.

Platform support	TPM only	TPM + PIN	TPM + startup key	Startup key	Recovery password

Define hardware implementation standards

For each of the types of hardware listed in the following table, specify your implementation standards going forward.

Classification	BitLocker policy and configuration

Define disk configuration

You can use the following table to document your planned disk configuration.

Disk configuration	Partition 1	Partition 2	Partition 3

Caution

If you place Windows RE and BitLocker on the same (active) partition, you cannot perform a restore from a Complete PC backup without using a Windows RE CD. This is because Complete PC must always restore the active partition, but fails to do so when the files that Windows RE uses to start from are also on the active partition. To ensure that you can perform a complete PC backup without requiring a Windows RE CD, install Windows RE and BitLocker on separate partitions.

Define Active Directory Domain Services configuration

You can use the following table to determine whether your AD DS deployment will require schema modification to store BitLocker recovery information.

Computer type	Recovery password storage	Requires schema modification

Define BitLocker and Windows Vista Group Policy settings

Create one table for each computer classification. An example of a computer classification is a group for corporate desktops in secure sites.

[Computer classification BitLocker Group Policy settings]

Setting	Configuration

Define password and key management policies

Create one table for each computer classification. An example of a computer classification is a group for corporate desktops in secure sites.

TPM	Startup key	Recovery password	Recovery key	Script command

The following table shows sample values that document key management policies. For a sample BitLocker WMI deployment script, see the sample WMI script `enablebitlocker.vbs`, which is part of the Microsoft BitLocker Deployment Code Samples (<http://go.microsoft.com/fwlink/?LinkID=96685>).

Define support processes

You can use the following table to define support processes for your organization at a high-level.

Computer type	Location	Support process

Define inventory and tracking processes

You can use the following table to document your high-level inventory and tracking processes.

Component	Process

Case study: Contoso Pharmaceuticals strategy design

This case study shows the process that Contoso Pharmaceuticals used to go design its BitLocker strategy.

Audit and build process

The Contoso IT department reviewed their current build process and security policies to determine if they needed to make any changes to deploy BitLocker and incorporate it into the company's infrastructure.

Current IT department structure

The Contoso IT department consists of three distinct IT groups: a central IT department and two business IT departments. The Contoso IT team manages a mix of centralized and decentralized organizations.

Central IT

This department manages the company-wide IT technologies and core infrastructure services, such as user authentication, e-mail services, networking services, and core desktop deployment and management services.

Business IT

The two business unit-focused IT organizations, Sales and Research, manage IT functions and engineering for their respective organizations. However, they do not provide support to the larger organization.

The following table shows that new desktop deployments at Contoso occur within all three of the company's organizations. It is important to know where computers enter and exit the organization, as well as how they are configured and deployed when they arrive.

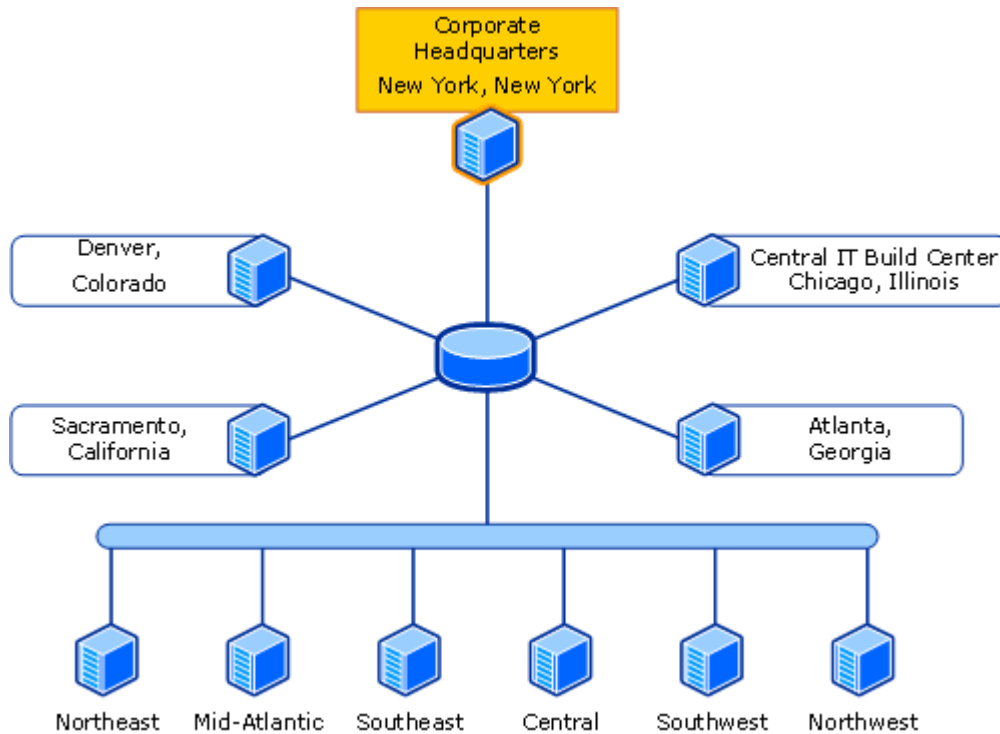
Contoso IT department service roles and scope

IT organization	Service roles	Users supported	Desktops supported
Central	<ul style="list-style-type: none">• All networking support• E-mail services for all users• User authentication• Desktop management services• Core platform Helpdesk support	120,000	100,000

IT organization	Service roles	Users supported	Desktops supported
	<ul style="list-style-type: none"> • New desktop deployment and decommissioning • Corporate security 		
Sales	<ul style="list-style-type: none"> • Business unit application support • Business unit-specific Helpdesk • New desktop deployment 	30,000	35,000
Research	<ul style="list-style-type: none"> • Business unit application support • Business unit-specific Helpdesk • New desktop deployment 	45,000	55,000

Complicating deployment and management, Contoso has several physical locations. The following figure shows the physical layout of Contoso.

Contoso physical layout



System build process

When new computers enter the Contoso environment, the delivery location is determined by their destination.

For example, if a new computer was ordered for an IT administrator who is part of the Central IT group, the computer is configured in Chicago, IL. If this computer is destined for a sales location in the southwest region, then it is shipped directly to the destination site for configuration.

The following table shows how the basic system configuration tasks are handled at Contoso.

System configuration tasks

IT department	System configuration	Configuration location
Central	Central IT configures new computers at a central location and delivers them to the users.	Chicago, IL
Sales Research	Users get their new computers directly, and Sales and Research IT must configure them remotely.	Sales or Research office location.

Each of the three groups has created its own new method of building and deploying Windows Vista operating systems to take advantage of the significant changes to Windows Vista deployment tools. Contoso is installing only Windows Vista as the standard corporate operating system.

The process that each business unit follows is independent. However, they do share some infrastructure dependencies. The following table shows the processes that each business unit uses, as well as the infrastructure components on which they rely.

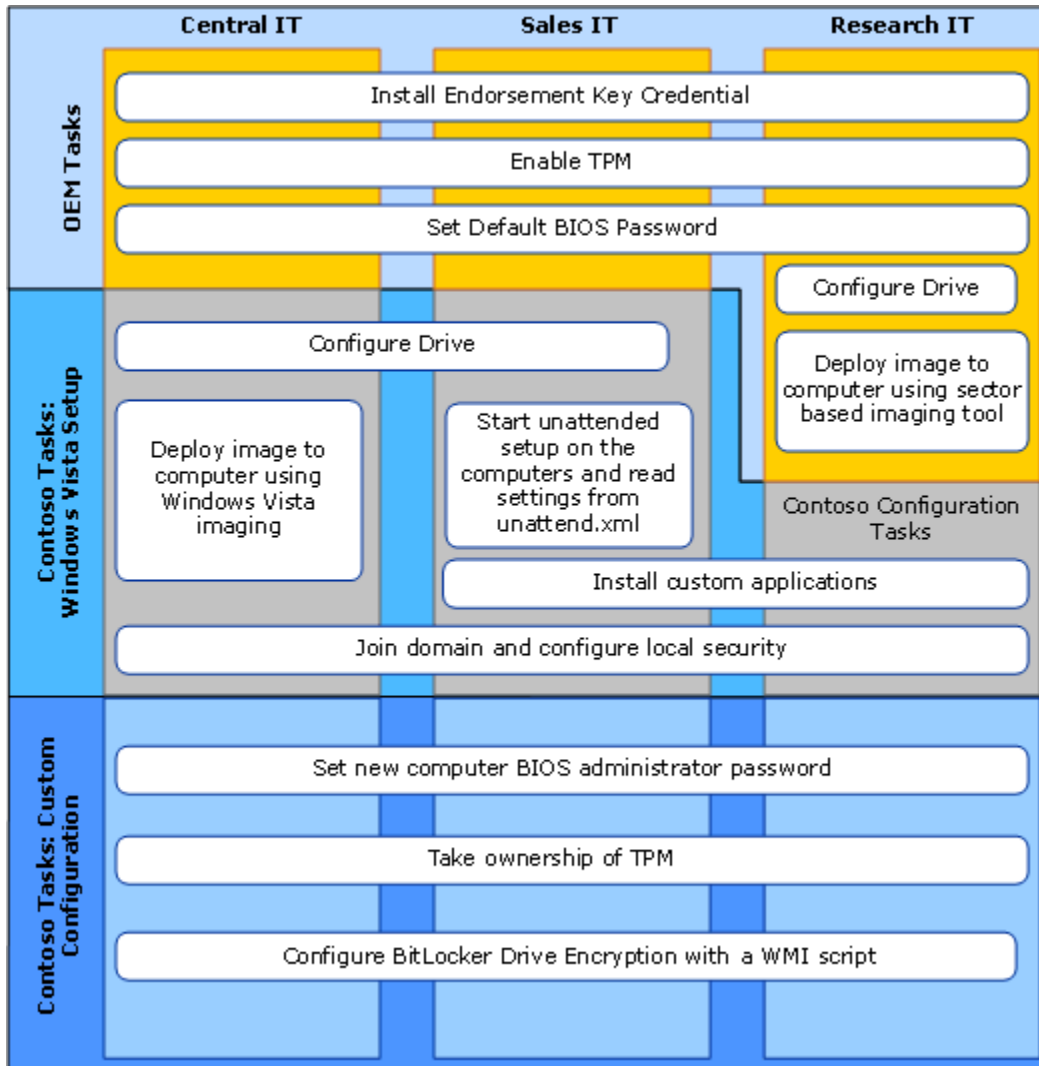
Contoso build processes

Business unit	Windows deployment method	Windows delivery method	Application delivery method	Infrastructure dependencies
Central	Windows Vista imaging format	PXE boot Windows PE	Integrated with image	PXE boot servers File share servers Authentication
Sales	Windows Vista unattended setup	PXE boot Windows PE	Scripted unattended installation	PXE boot servers File share servers Authentication
Research	OEM applied sector-based image	OEM applied image	Some integrated with image, others scripted	File share servers Authentication

Various Contoso departments use unattended setup, sector-based, and file-based imaging technology to build computers before issuing them to end users' computers. Some departments have the computers pre-configured by the OEM.

The following figure shows a comparison among the three build processes that exist at Contoso.

Contoso build processes



Each vertical pillar represents a build process flow for an individual business unit. Task boxes framed in red are described in the deployment section of this guide. These tasks are described because they relate to deploying Windows Vista with BitLocker Drive Encryption. Most of these tasks overlap all three of the build processes, even though the processes are different from each other.

BitLocker authentication methods

Contoso evaluated the BitLocker authentication methods using the following questions.

- Will you support computers without TPM version 1.2?

Contoso's security organization recently mandated that all computer systems that run Windows Vista will use BitLocker Drive Encryption. Contoso had recently gone through a hardware refresh, which allowed the company to support Windows Vista on most of its computers. Not all of the devices in the first wave have a TPM version 1.2. However, most of the second-wave replacements have this capability. Because of the mix of TPM and non-TPM hardware, and the security mandate, they have decided to support BitLocker on both TPM-based and non-TPM-based computers.

- **What areas of your organization need a baseline level of data protection?**

Most Contoso computers in the Corporate – Secure Sites that will be running Windows Vista with BitLocker do not contain highly sensitive data and are not mobile computers. For this reason, Contoso wants to configure these computers with the most transparent configuration of BitLocker, and the configuration that will have the least impact on users. They have decided to enable BitLocker using the TPM-only mode on these types of systems.

- **What areas of your organization need a more secure level of data protection?**

There are several areas in the Contoso environment where the level of data protection needs to be increased because of the sensitivity of data on these computers. In the Research and Sales departments, the data that is stored on these computers is classified as very sensitive. These groups also have more laptop computers than desktop computers in the environment. For this reason, Contoso has decided to use the TPM + PIN on the laptop computers and the TPM + USB startup key on the desktop computers.

- **What multifactor authentication mode does your organization prefer?**

Contoso decided to use multifactor authentication on their computers with highly sensitive data. For their laptop computers, they chose to use a PIN rather than a USB startup key, because of the possibility that a user might leave the USB startup key with the computer in an unprotected situation. For the desktop computers, they have chosen a USB key because all of these computers are located in field sales locations where the USB startup keys can be secured when the computers are left unattended.

Contoso standard configuration

For security and secure asset management purposes, Contoso has decided to support and enable BitLocker on all of their corporate workstation and laptop computers. The following table outlines the corporate standards support matrix for enabling BitLocker on Contoso corporate systems.

Corporate standards for enabling BitLocker on Contoso systems

System classification	Description
Corporate desktop – secure site	Systems will use BitLocker encryption with a TPM or USB startup key, depending on

System classification	Description
	hardware availability. This will be used to control data exposure and manage asset retirement.
Corporate desktop – field site	Systems will use BitLocker encryption with a TPM and a USB startup key. These desktops are shared-use computers in field sales locations with limited security. USB drives will contain startup keys and will be locked in a safe when not in use. This will be used to control data exposure and to manage asset retirement.
Corporate laptop	New systems will use a TPM and a PIN for all computers. Non-TPM computers will use startup keys on USB drives, but all new computers will be purchased with TPM devices. This will be used to control data exposure and manage asset retirement.

Active Directory Domain Services configuration

Contoso decided to extend its Active Directory schema to support storing BitLocker recovery material. Central IT used the information in *Configuring Active Directory to Back up Windows BitLocker Drive Encryption and Trusted Platform Module Recovery Information* (<http://go.microsoft.com/fwlink/?LinkId=82827>) to help them enable key escrow with Active Directory Domain Services (AD DS).

Contoso support processes

There are three supported BitLocker configurations. For each of these supported configurations, there is a required level of support and a defined process.

- Corporate desktop (secure site)
- Corporate desktop (field site)
- Corporate laptop

The following figure is an example of process flow for BitLocker system recovery at Contoso.

Contoso support process

1. User's computer enters recovery.
2. User calls Helpdesk.

3. Helpdesk technician creates a support ticket and initiates the recovery process.
4. Helpdesk technician questions the user and identifies the root cause of recovery.
5. Helpdesk technician validates the user's identity and gives the user the recovery password to unlock the volume.
6. User unlocks the volume by typing the 48-digit recovery password into the BitLocker recovery console.
7. Helpdesk technician verifies that the user has successfully unlocked the volume.
8. Helpdesk technician creates a new recovery password and escrows it to AD DS.
9. AD DS deletes the used recovery password.
10. Helpdesk technician documents the root cause of the recovery for organizational tracking and closes the support ticket.

Inventory and tracking processes

Central IT uses an asset management system to track hardware based on custom attributes: for example, computers that have TPMs versus computers that do not. The department also tracks required BIOS updates based on their corporate standard Contoso computers. If a BIOS update is required, Central IT works with the OEM to obtain the BIOS and create a deployment method.

Deployment

As part of its deployment planning, Contoso identified both Group Policy settings and key management policies.

BitLocker and Windows Vista Group Policy settings

In the Contoso enterprise deployment of BitLocker, users are not allowed to change the existing configuration or affect the initial configuration, other than choosing a PIN.

To configure BitLocker computers in the Contoso environment, three top-level domain Group Policy objects (GPOs) control the three computer types that are identified in the computer matrix. Because the Contoso BitLocker computers are broken up by platform type and location, the Contoso IT department configured the Group Policy settings to use WMI filtering, so that the policies apply only to platform types that are defined in the standard configuration. Settings that are not shown in the following tables are left at the default setting.

Contoso-BitLocker-Desk-SecureSite

Setting	Configuration
Turn on BitLocker backup to Active Directory Domain Services	Require Active Directory Domain Services backup of BitLocker Recovery passwords and key packages

Setting	Configuration
Turn on TPM backup to Active Directory Domain Services	Require Active Directory Domain Services backup of TPM owner information
WMI filter	Root\CimV2; select * from Win32_OperatingSystem where Version = "6.0"

Contoso-BitLocker-Desk-FieldSite

Setting	Configuration
Turn on BitLocker backup to Active Directory Domain Services	Require Active Directory Domain Services backup of BitLocker Recovery passwords and key packages
Turn on TPM backup to Active Directory Domain Services	Require Active Directory Domain Services backup of TPM owner information
WMI filter	Root\CimV2; select * from Win32_OperatingSystem where Version = "6.0"

Contoso-BitLocker-Laptop

Setting	Configuration
Turn on BitLocker backup to Active Directory Domain Services	Require Active Directory Domain Services backup of BitLocker Recovery passwords and key packages
Control Panel Setup: Enable Advanced Startup Options	Require Startup PIN with TPM
Turn on TPM backup to Active Directory Domain Services	Require Active Directory Domain Services backup of TPM owner Information
WMI filter	Root\CimV2; select * from win32_systemenclosure where chassistypes = "10" or chassistypes = "9" or chassistypes = "8"
WMI filter	Root\CimV2; select * from Win32_OperatingSystem where Version = "6.0"

**Note**

Client support for WMI filters exists only on Windows XP, Windows Server 2003, and later operating systems. WMI filters are available only in domains that have at least one Windows Server 2003 domain controller.

Other Group Policy settings

Additional Group Policy settings establish a default power plan and restrict access to the Power Options Control Panel item. This applies to the computer object portion of the Group Policy. The following tables detail the specific Group Policy settings that are configured in the Contoso environment.

Contoso-BitLocker-Desk-SecureSite

Computer setting	Configuration
Allow Standby States (S1-S3) When Sleeping (Plugged In)	Not configured
Allow Standby States (S1-S3) When Sleeping (Battery)	Not configured

Contoso-BitLocker-Desk-FieldSite

Computer setting	Configuration
Allow Standby States (S1-S3) When Sleeping (Plugged In)	Not configured
Allow Standby States (S1-S3) When Sleeping (Battery)	Not configured

Contoso-BitLocker-Laptop

Computer setting	Configuration
Allow Standby States (S1-S3) When Sleeping (Plugged In)	Disabled
Allow Standby States (S1-S3) When Sleeping (Battery)	Disabled
Require a Password When Computer Wakes (Plugged In)	Yes
Require a Password When Computer Wakes	Yes

Computer setting	Configuration
(Battery)	

Pre-build configuration

Contoso has defined its pre-build configuration by using OEM-specific configuration and defining the disk configuration that will be implemented for each department.

OEM-specific configuration

All three business units have their computers preconfigured from the OEM with the following settings:

- Endorsement keys are generated and managed by a value-added-reseller after the computer is manufactured.
- TPM is shipped in the enabled and activated state.
- Default BIOS administrator password is set.

The Research IT business unit at Contoso also has the OEM apply a Contoso image before the computers are shipped. The other business units apply the operating system to their computers after they receive them from the OEM.

Configuring the disk for BitLocker

At Contoso, each business unit installs Windows Vista differently.

- The Central IT business unit uses Windows Vista imaging technology to deploy the operating system.
- The Sales IT business unit performs an unattended installation of Windows Vista.
- The Research IT business unit has its OEM apply images to its computers using a sector-based imaging tool.
- The Sales IT business unit deploys the operating system to computers using an unattended installation process. To configure the disks, configuration options are placed in the unattended answer file. This allows setup to configure the disk automatically.

The following entries are placed in the Windows-Setup section of the answer file:

```
<DiskConfiguration>
  <WillShowUI>Never</WillShowUI>

  <Disk>

    <DiskID>0</DiskID>

    <WillWipeDisk>true</WillWipeDisk>

    <CreatePartitions>
```

```
<CreatePartition>
  <Order>1</Order>
  <Type>Primary</Type>
  <Size>1500</Size>
</CreatePartition>
<CreatePartition>
  <Order>2</Order>
  <Type>Primary</Type>
  <Extend>>true</Extend>
</CreatePartition>
</CreatePartitions>
<ModifyPartitions>
  <ModifyPartition>
    <Order>1</Order>
    <PartitionID>1</PartitionID>
    <Letter>S</Letter>
    <Label>SYSTEM</Label>
    <Format>NTFS</Format>
    <Active>true</Active>
  </ModifyPartition>
  <ModifyPartition>
    <Order>2</Order>
    <PartitionID>2</PartitionID>
    <Letter>C</Letter>
    <Label>OS</Label><Label>OS</Label>
    <Format>NTFS</Format>
    <Active>>false</Active>
  </ModifyPartition>
</MoDifyPartitions>
</Disk>
</DiskConfiguration>
```

Post-build configuration

Contoso has created definitions for TPM management and encryption configuration.

TPM management

Taking ownership of the TPM is automated during the computer build process. This is accomplished by auto-logging on to the computer at the end of the build process with a domain user account. Logon with a domain account because the Contoso BitLocker Group Policy settings require the TPM owner information be backed up to AD DS. During the take-ownership process, a hash of the TPM owner password is saved to the computers object in AD DS. This only happens at the point you take ownership so it is important to have access to AD DS and the computer object.

To automate the process, add the following entries to the Windows-Shell-Setup section of the unattended installation answer files which are part of the image based and unattended build processes.

```
<AutoLogon>
  <Enabled>>true</Enabled>
  <Username>buildaccount</Username>
  <Password>*****</Password>
  <LogonCount>1</LogonCount>
</AutoLogon>
<FirstLogonCommands>
  <SynchronousCommand>
    <Order>1</Order>
    <CommandLine>enablebitlocker.vbs /on:tpm /1:%temp%\enablebde.log</CommandLine>
    <Description>Take ownership of the TPM</Description>
  </SynchronousCommand>
</FirstLogonCommands>
```

Encryption configuration

At Contoso, there are three standard BitLocker configurations: secure site computers, field site computers, and laptop computers. During the build process at Contoso, one of the last steps is to enable BitLocker and start the volume encryption. The following tables show the commands that are issued on the various computer types, depending on the desired configuration.

Contoso-BitLocker-Desk-SecureSite

Command	Description
Enablebitlocker.vbs /on:tpm /rk /promptuser /l:%temp%\enablebde.log	For computers with a TPM, enable BitLocker using a TPM, recovery password, and recovery key.
Enablebitlocker.vbs /on:tpm /rk /promptuser /l:%temp%\enablebde.log	For computers without a TPM, enable BitLocker using a startup key, recovery password, and recovery key.

Contoso-BitLocker-Desk-FieldSite

Command	Description
Enablebitlocker.vbs /on:tsk /rk /promptuser /l:%temp%\enablebde.log	Enable BitLocker using a startup key, recovery password, and recovery key.

Contoso-BitLocker-Laptop

Command	Description
Enablebitlocker.vbs /on:tp /rk /promptuser /l:%temp%\enablebde.log	For laptop computers with a TPM, enable BitLocker using a TPM + PIN, recovery password, and recovery key.
Enablebitlocker.vbs /on:usb /rk /promptuser /l:%temp%\enablebde.log	For computers without a TPM, enable BitLocker using a startup key, recovery password, and recovery key.

Appendix: Reviewing BitLocker Requirements

To take advantage of all BitLocker features, your computer must meet the hardware and software requirements listed in the table below.

BitLocker hardware and software requirements

Requirement	Description
Hardware configuration	Computer must meet the minimum requirements for Windows Vista. For more information about Windows Vista requirements, see

Requirement	Description
	http://go.microsoft.com/fwlink/?LinkId=83233 . For more information about Windows Logo requirements for hardware, see http://go.microsoft.com/fwlink/?LinkId=94017 .
Operating system	Windows Vista Ultimate or Windows Vista Enterprise. Both include BitLocker Drive Encryption.
Hardware Trusted Platform Module (TPM)*	TPM version 1.2
BIOS configuration	<ul style="list-style-type: none"> • Trusted Computing Group (TCG)-compliant BIOS. • BIOS must be set to boot first from the hard drive and not from the USB or CD drives. • BIOS must be able to read from a USB flash drive during startup.
File system	Two NTFS drive partitions, one for the system volume and one for the operating system volume. The system volume partition must be at least 1.5 GB and set as the active partition.

*A TPM is not required for BitLocker. However, only a computer with a TPM can provide the additional security of pre-boot system integrity verification.