BitLocker Group Policy Settings

Updated: September 13, 2013

Applies To: Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2

This reference topic for the IT professional describes the function, location, and effect of each Group Policy setting that is used to manage BitLocker Drive Encryption.

Overview

To control what drive encryption tasks the user can perform from the Windows Control Panel or to modify other configuration options, you can use Group Policy administrative templates or local computer policy settings. How you configure these policy settings depends on how you implement BitLocker and what level of user interaction will be allowed.

Note
A separate set of Group Policy settings supports the use of the Trusted Platform Module (TPM). For details about those settings, see Trusted Platform Module Services Group Policy Settings.

BitLocker Group Policy settings can be accessed using the Local Group Policy Editor and the Group Policy Management Console (GPMC) under **Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption**.

Most of the BitLocker Group Policy settings are applied when BitLocker is initially turned on for a drive. If a computer is not compliant with existing Group Policy settings, BitLocker may not be turned on or modified until the computer is in a compliant state. When a drive is out of compliance with Group Policy settings (for example, if a Group Policy setting was changed after the initial BitLocker deployment in your organization, and then the setting was applied to previously encrypted drives), no change can be made to the BitLocker configuration of that drive except a change that will bring it into compliance.

If multiple changes are necessary to bring the drive into compliance, you must suspend BitLocker protection, make the necessary changes, and then resume protection. This situation could occur, for example, if a removable drive was initially configured to be unlocked with a password and then Group Policy settings are changed to disallow passwords and require smart cards. In this situation, you need to suspend BitLocker protection by using the **Manage-bde** command-line tool, delete the password unlock method, and add the smart card method. After this is complete, BitLocker is compliant with the Group Policy setting and BitLocker protection on the drive can be resumed.

BitLocker Group Policy settings

The following sections provide a comprehensive list of BitLocker Group Policy settings that are organized by usage. BitLocker Group Policy settings include settings for specific drive types (operating system drives, fixed data drives, and removable data drives) and settings that are applied to all drives.

The following policy settings can be used to determine how a BitLocker-protected drive can be unlocked.

- Allow network unlock at startup
- Require additional authentication at startup
- Allow enhanced PINs for startup
- Configure minimum PIN length for startup
- Disallow standard users from changing the PIN or password
- Configure use of passwords for operating system drives
- Require additional authentication at startup (Windows Server 2008 and Windows Vista)
- Configure use of smart cards on fixed data drives
- Configure use of passwords on fixed data drives
- Configure use of smart cards on removable data drives
- Configure use of passwords on removable data drives
- Validate smart card certificate usage rule compliance
- Enable use of BitLocker authentication requiring preboot keyboard input on slates

The following policy settings are used to control how users can access drives and how they can use BitLocker on their computers.

- Deny write access to fixed drives not protected by BitLocker
- Deny write access to removable drives not protected by BitLocker
- Control use of BitLocker on removable drives

The following policy settings determine the encryption methods and encryption types that are used with BitLocker.

- Choose drive encryption method and cipher strength
- Configure use of hardware-based encryption for fixed data drives
- Configure use of hardware-based encryption for operating system drives
- Configure use of hardware-based encryption for removable data drives
- Enforce drive encryption type on fixed data drives
- Enforce drive encryption type on operating system drives
- Enforce drive encryption type on removable data drives

The following policy settings define the recovery methods that can be used to restore access to a BitLocker-protected drive if an authentication method fails or is unable to be used.

- Choose how BitLocker-protected operating system drives can be recovered
- Choose how users can recover BitLocker-protected drives (Windows Server 2008 and Windows Vista)
- Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista)
- Choose default folder for recovery password
- Choose how BitLocker-protected fixed drives can be recovered
- Choose how BitLocker-protected removable drives can be recovered

The following policies are used to support customized deployment scenarios in your organization.

- Allow Secure Boot for integrity validation
- Provide the unique identifiers for your organization
- Prevent memory overwrite on restart
- Configure TPM platform validation profile for BIOS-based firmware configurations
- Configure TPM platform validation profile (Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2)
- Configure TPM platform validation profile for native UEFI firmware configurations
- Reset platform validation data after BitLocker recovery

- Use enhanced Boot Configuration Data validation profile
- Allow access to BitLocker-protected fixed data drives from earlier versions of Windows
- Allow access to BitLocker-protected removable data drives from earlier versions of Windows

Allow network unlock at startup

This policy controls a portion of the behavior of the Network Unlock feature in BitLocker. This policy is required to enable BitLocker Network Unlock on a network because it allows clients running BitLocker to create the necessary network key protector during encryption. This policy is used in addition to the BitLocker Drive Encryption Network Unlock Certificate security policy (located in the **Public Key Policies** folder of Local Computer Policy) to allow systems that are connected to a trusted network to properly utilize the Network Unlock feature.

Policy description	With this policy setting, you can control whether a BitLocker-protected computer that is connected to a trusted local area network and joined to a domain can create and use network key protectors on TPM-enabled computers to automatically unlock the operating system drive when the computer is started.
Introduced	Windows Server 2012 and Windows 8
Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	None
When enabled	Clients configured with a BitLocker Network Unlock certificate can create and use Network Key Protectors.
When disabled or not configured	Clients cannot create and use Network Key Protectors

Reference

To use a network key protector to unlock the computer, the computer and the server that hosts BitLocker Drive Encryption Network Unlock must be provisioned with a Network Unlock certificate. The Network Unlock certificate is used to create a network key protector and to protect the information exchange with the server to unlock the computer. You can use the Group Policy setting **Computer Configuration\Windows Settings\Security Settings\Public Key Policies\BitLocker Drive Encryption Network Unlock Certificate** on the domain controller to distribute this certificate to computers in your organization. This unlock method uses the TPM on the computer, so computers that do not have a TPM cannot create network key protectors to automatically unlock by using Network Unlock.

Note
For reliability and security, computers should also have a TPM startup PIN that can be used when the computer is disconnected from the wired network or cannot connect to the domain controller at startup.

For more information about Network Unlock, see BitLocker: How to enable Network Unlock.

Require additional authentication at startup

This policy setting is used to control which unlock options are available for operating system drives.

Policy description	With this policy setting, you can configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
	If one authentication method is required, the other methods cannot be allowed.
Conflicts	Use of BitLocker with a TPM startup key or with a TPM startup key and a PIN must be disallowed if the **Deny write access to removable drives not protected by BitLocker** policy setting is enabled.
When enabled	Users can configure advanced startup options in the BitLocker Setup Wizard.
When disabled or not configured	Users can configure only basic options on computers with a TPM.
	Only one of the additional authentication options can be required at startup; otherwise, a policy error occurs.

Reference

If you want to use BitLocker on a computer without a TPM, select the **Allow BitLocker without a compatible TPM** check box. In this mode, a USB drive is required for startup. Key information that is used to encrypt the drive is stored on the USB drive, which creates a USB key. When the USB key is inserted, access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable, you need to use one of the BitLocker recovery options to access the drive.

On a computer with a compatible TPM, four types of authentication methods can be used at startup to provide added protection for encrypted data. When the computer starts, it can use:

- only the TPM for authentication
- insertion of a USB flash drive containing the startup key
- the entry of a 4-digit to 20-digit personal identification number (PIN)
- a combination of the PIN and the USB flash drive

There are four options for TPM-enabled computers or devices:

- Configure TPM startup
    - Allow TPM
    - Require TPM
    - Do not allow TPM
- Configure TPM startup PIN
    - Allow startup PIN with TPM
    - Require startup PIN with TPM
    - Do not allow startup PIN with TPM
- Configure TPM startup key
    - Allow startup key with TPM
    - Require startup key with TPM
    - Do not allow startup key with TPM
- Configure TPM startup key and PIN
    - Allow TPM startup key with PIN
    - Require startup key and PIN with TPM
    - Do not allow TPM startup key with PIN

Allow enhanced PINs for startup

This policy setting permits the use of enhanced PINs when you use an unlock method that includes a PIN.

Policy description	With this policy setting, you can configure whether enhanced startup PINs are used with BitLocker.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	None
When enabled	All new BitLocker startup PINs that are set will be enhanced PINs. Existing drives that were protected by using standard startup PINs are not affected.
When disabled or not configured	Enhanced PINs will not be used.

Reference

Enhanced startup PINs permit the use of characters (including uppercase and lowercase letters, symbols, numbers, and spaces). This policy setting is applied when you turn on BitLocker.

Important
Not all computers support enhanced PIN characters in the preboot environment. It is strongly recommended that users perform a system check during the BitLocker setup to verify that enhanced PIN characters can be used.

Configure minimum PIN length for startup

This policy setting is used to set a minimum PIN length when you use an unlock method that includes a PIN.

Policy description	With this policy setting, you can configure a minimum length for a TPM startup PIN. This policy setting is applied when you turn on BitLocker. The startup PIN must have a minimum length of 4 digits, and it can have a maximum length of 20 digits.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	None
When enabled	You can require that users enter a minimum number of digits to when setting their startup PINs.
When disabled or not	Users can configure a startup PIN of any length between 4 and 20 digits.

configured

Reference

This policy setting is applied when you turn on BitLocker. The startup PIN must have a minimum length of 4 digits and can have a maximum length of 20 digits.

Disallow standard users from changing the PIN or password

This policy setting allows you to configure whether standard users are allowed to change the PIN or password that is used to protect the operating system drive.

Policy description	With this policy setting, you can configure whether standard users are allowed to change the PIN or password used to protect the operating system drive.
Introduced	Windows Server 2012 and Windows 8
Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	None
When enabled	Standard users are not allowed to change BitLocker PINs or passwords.
When disabled or not configured	Standard users are permitted to change BitLocker PINs or passwords.

Reference

To change the PIN or password, the user must be able to provide the current PIN or password. This policy setting is applied when you turn on BitLocker.

Configure use of passwords for operating system drives

This policy controls how non-TPM based systems utilize the password protector. Used in conjunction with the **Password must meet complexity requirements** policy, this policy allows administrators to require password length and complexity for using the password protector. By default, passwords must be eight characters in length. Complexity configuration options determine how important domain connectivity is for the client. For the strongest password security, administrators should choose **Require password complexity** because it requires domain connectivity, and it requires that the BitLocker password meets the same password complexity requirements as domain sign-in passwords.

For more information, see Password must meet complexity requirements.

Policy description	With this policy setting, you can specify the constraints for passwords that are used to unlock operating system drives that are protected with BitLocker.
Introduced	Windows Server 2012 and Windows 8
Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	Passwords cannot be used if FIPS-compliance is enabled. **Note** The **System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing** policy setting, which is located at **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options** specifies whether FIPS-compliance is enabled.
When enabled	Users can configure a password that meets the requirements you define. To enforce complexity requirements for the password, select **Require complexity**.
When disabled or not configured	The default length constraint of 8 characters will apply to operating system drive passwords and no complexity checks will occur.

Reference

If non-TPM protectors are allowed on operating system drives, you can provision a password, enforce complexity requirements on the password, and configure a minimum length for the password. For the complexity requirement setting to be effective, the Group Policy setting **Password must meet complexity requirements**, which is located at **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy** must be also enabled.

For more information, see Password must meet complexity requirements.

Note

These settings are enforced when turning on BitLocker, not when unlocking a volume. BitLocker allows unlocking a drive with any of the protectors that are available on the drive.

When set to **Require complexity**, a connection to a domain controller is necessary when BitLocker is enabled to validate the complexity the password. When set to **Allow complexity**, a connection to a domain controller is attempted to validate that the complexity adheres to the rules set by the policy. If no domain controllers are found, the password will be accepted regardless of actual password complexity, and the drive will be encrypted by using that password as a protector. When set to **Do not allow complexity**, there is no password complexity validation.

Passwords must be at least 8 characters. To configure a greater minimum length for the password, enter the desired number of characters in the **Minimum password length** box.

When this policy setting is enabled, you can set the option **Configure password complexity for operating system drives** to:

- Allow password complexity
- Do not allow password complexity
- Require password complexity

Require additional authentication at startup (Windows Server 2008 and Windows Vista)

This policy setting is used to control what unlock options are available for computers running Windows Server 2008 or Windows Vista.

Policy description	With this policy setting, you can control whether the BitLocker Setup Wizard on computers running Windows Vista or Windows Server 2008 can set up an additional authentication method that is required each time the computer starts.
Introduced	Windows Server 2008 and Windows Vista
Drive type	Operating system drives (Windows Server 2008 and Windows Vista)
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	If you choose to require an additional authentication method, other authentication methods cannot be allowed.
When enabled	The BitLocker Setup Wizard displays the page that allows the user to configure advanced startup options for BitLocker. You can further configure setting options for computers with or without a TPM.
When disabled or not configured	The BitLocker Setup Wizard displays basic steps that allow users to enable BitLocker on computers with a TPM. In this basic wizard, no additional startup key or startup PIN can be configured.

Reference

On a computer with a compatible TPM, two authentication methods can be used at startup to provide added protection for encrypted data. When the computer starts, it can require users to insert a USB drive that contains a startup key. It can also require users to enter a 4-digit to 20-digit startup PIN.

A USB drive that contains a startup key is needed on computers without a compatible TPM. Without a TPM, BitLocker-encrypted data is protected solely by the key material that is on this USB drive.

There are two options for TPM-enabled computers or devices:

- Configure TPM startup PIN
    - Allow startup PIN with TPM
    - Require startup PIN with TPM
    - Do not allow startup PIN with TPM
- Configure TPM startup key
    - Allow startup key with TPM
    - Require startup key with TPM
    - Do not allow startup key with TPM

These options are mutually exclusive. If you require the startup key, you must not allow the startup PIN. If you require the startup PIN, you must not allow the startup key. Otherwise, a policy error will occur.

To hide the advanced page on a TPM-enabled computer or device, set these options to **Do not allow** for the startup key and for the startup PIN.

Configure use of smart cards on fixed data drives

This policy setting is used to require, allow, or deny the use of smart cards with fixed data drives.

Policy description	With this policy setting, you can specify whether smart cards can be used to authenticate user access to the BitLocker-protected fixed data drives on a computer.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Fixed data drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives
Conflicts	To use smart cards with BitLocker, you may also need to modify the object identifier setting in the **Computer Configuration\Administrative Templates\BitLocker Drive Encryption\Validate smart card certificate usage rule compliance** policy setting to match the object identifier of your smart card

	certificates.
When enabled	Smart cards can be used to authenticate user access to the drive. You can require smart card authentication by selecting the **Require use of smart cards on fixed data drives** check box.
When disabled	Users cannot use smart cards to authenticate their access to BitLocker-protected fixed data drives.
When not configured	Smart cards can be used to authenticate user access to a BitLocker-protected drive.

Reference

Note

These settings are enforced when turning on BitLocker, not when unlocking a drive. BitLocker allows unlocking a drive by using any of the protectors that are available on the drive.

Configure use of passwords on fixed data drives

This policy setting is used to require, allow, or deny the use of passwords with fixed data drives.

Policy description	With this policy setting, you can specify whether a password is required to unlock BitLocker-protected fixed data drives.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Fixed data drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives
Conflicts	To use password complexity, the **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements** policy setting must also be enabled.
When enabled	Users can configure a password that meets the requirements you define. To require the use of a password, select **Require password for fixed data drive**. To enforce complexity requirements on the password, select **Require complexity**.
When disabled	The user is not allowed to use a password.
When not configured	Passwords are supported with the default settings, which do not include password complexity requirements and require only 8 characters.

Reference

When set to **Require complexity**, a connection to a domain controller is necessary to validate the complexity of the password when BitLocker is enabled.

When set to **Allow complexity**, a connection to a domain controller is attempted to validate that the complexity adheres to the rules set by the policy. However, if no domain controllers are found, the password is accepted regardless of the actual password complexity, and the drive is encrypted by using that password as a protector.

When set to **Do not allow complexity**, no password complexity validation is performed.

Passwords must be at least 8 characters. To configure a greater minimum length for the password, enter the desired number of characters in the **Minimum password length** box.

Note

These settings are enforced when turning on BitLocker, not when unlocking a drive. BitLocker allows unlocking a drive with any of the protectors that are available on the drive.

For the complexity requirement setting to be effective, the Group Policy setting **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements** must also be enabled.

This policy setting is configured on a per-computer basis. This means that it applies to local user accounts and domain user accounts. Because the password filter that is used to validate password complexity is located on the domain controllers, local user accounts cannot access the password filter because they are not authenticated for domain access. When this policy setting is enabled, if you sign in with a local user account, and you attempt to encrypt a drive or change a password on an existing BitLocker-protected drive, an "Access denied" error message is displayed. In this situation, the password key protector cannot be added to the drive.

Enabling this policy setting requires that connectivity to a domain be established before adding a password key protector to a BitLocker-protected drive. Users who work remotely and have periods of time in which they cannot connect to the domain should be made aware of this requirement so that they can schedule a time when they will be connected to the domain to turn on BitLocker or to change a password on a BitLocker-protected data drive.

Important

Passwords cannot be used if FIPS compliance is enabled. The **System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing** policy setting in **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options** specifies whether FIPS compliance is enabled.

Configure use of smart cards on removable data drives

This policy setting is used to require, allow, or deny the use of smart cards with removable data drives.

Policy description	With this policy setting, you can specify whether smart cards can be used to authenticate user access to BitLocker-protected removable data drives on a computer.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Removable data drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives
Conflicts	To use smart cards with BitLocker, you may also need to modify the object identifier setting in the **Computer Configuration\Administrative Templates\BitLocker Drive Encryption\Validate smart card certificate usage rule compliance** policy setting to match the object identifier of your smart card certificates.
When enabled	Smart cards can be used to authenticate user access to the drive. You can require smart card authentication by selecting the **Require use of smart cards on removable data drives** check box.
When disabled or not configured	Users are not allowed to use smart cards to authenticate their access to BitLocker-protected removable data drives.
When not configured	Smart cards are available to authenticate user access to a BitLocker-protected removable data drive.

Reference

Note

These settings are enforced when turning on BitLocker, not when unlocking a drive. BitLocker allows unlocking a drive with any of the protectors that are available on the drive.

Configure use of passwords on removable data drives

This policy setting is used to require, allow, or deny the use of passwords with removable data drives.

Policy description	With this policy setting, you can specify whether a password is required to unlock BitLocker-protected removable data drives.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Removable data drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives
Conflicts	To use password complexity, the **Password must meet complexity requirements** policy setting, which is located at **Computer Configuration\Windows Settings\Security Settings\Account**

	Policies\Password Policy must also be enabled.
When enabled	Users can configure a password that meets the requirements you define. To require the use of a password, select **Require password for removable data drive**. To enforce complexity requirements on the password, select **Require complexity**.
When disabled	The user is not allowed to use a password.
When not configured	Passwords are supported with the default settings, which do not include password complexity requirements and require only 8 characters.

Reference

If you choose to allow the use of a password, you can require a password to be used, enforce complexity requirements, and configure a minimum length. For the complexity requirement setting to be effective, the Group Policy setting **Password must meet complexity requirements**, which is located at **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy** must also be enabled.

For information about this setting, see Password must meet complexity requirements.

Note
These settings are enforced when turning on BitLocker, not when unlocking a drive. BitLocker allows unlocking a drive with any of the protectors that are available on the drive.

Passwords must be at least 8 characters. To configure a greater minimum length for the password, enter the desired number of characters in the **Minimum password length** box.

When set to **Require complexity**, a connection to a domain controller is necessary when BitLocker is enabled to validate the complexity the password.

When set to **Allow complexity**, a connection to a domain controller will be attempted to validate that the complexity adheres to the rules set by the policy. However, if no domain controllers are found, the password will still be accepted regardless of actual password complexity and the drive will be encrypted by using that password as a protector.

When set to **Do not allow complexity**, no password complexity validation will be done.

Note
Passwords cannot be used if FIPS compliance is enabled. The **System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing** policy setting in **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options** specifies whether FIPS compliance is enabled.

For information about this setting, see System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing.

Validate smart card certificate usage rule compliance

This policy setting is used to determine what certificate to use with BitLocker.

Policy description	With this policy setting, you can associate an object identifier from a smart card certificate to a BitLocker-protected drive.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Fixed and removable data drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption
Conflicts	None
When enabled	The object identifier that is specified in the **Object identifier** setting must match the object identifier in the smart card certificate.
When disabled or not configured	The default object identifier is used.

Reference

This policy setting is applied when you turn on BitLocker.

The object identifier is specified in the enhanced key usage (EKU) of a certificate. BitLocker can identify which certificates can be used to authenticate a user certificate to a BitLocker-protected drive by matching the object identifier in the certificate with the object identifier that is defined by this policy setting.

The default object identifier is 1.3.6.1.4.1.311.67.1.1.

Note

BitLocker does not require that a certificate have an EKU attribute; however, if one is configured for the certificate, it must be set to an object identifier that matches the object identifier configured for BitLocker.

Enable use of BitLocker authentication requiring preboot keyboard input on slates

This policy setting allows users to enable authentication options that require user input from the preboot environment even if the platform indicates a lack of preboot input capability.

Policy description	With this policy setting, you can allow users to enable authentication options that require user input from the preboot environment, even if the platform indicates a lack of preboot input capability.
Introduced	Windows Server 2012 and Windows 8
Drive type	Operating system drive
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drive
Conflicts	None
When enabled	Devices must have an alternative means of preboot input (such as an attached USB keyboard).
When disabled or not configured	The Windows Recovery Environment must be enabled on tablets to support entering the BitLocker recovery password.

Reference

The Windows touch keyboard (such as used by tablets) is not available in the preboot environment where BitLocker requires additional information, such as a PIN or password.

It is recommended that administrators enable this policy only for devices that are verified to have an alternative means of preboot input, such as attaching a USB keyboard.

When the Windows Recovery Environment is not enabled and this policy is not enabled, you cannot turn on BitLocker on a device that uses the Windows touch keyboard.

If you do not enable this policy setting, the following options in the **Require additional authentication at startup** policy might not be available:

- Configure TPM startup PIN: Required and Allowed
- Configure TPM startup key and PIN: Required and Allowed
- Configure use of passwords for operating system drives

Deny write access to fixed drives not protected by BitLocker

This policy setting is used to require encryption of fixed drives prior to granting Write access.

Policy description	With this policy setting, you can set whether BitLocker protection is required for fixed data drives to be writable on a computer.
Introduced	Windows Server 2008 R2 and Windows 7

Drive type	Fixed data drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives
Conflicts	See the Reference section for a description of conflicts.
When enabled	All fixed data drives that are not BitLocker-protected are mounted as Read-only. If the drive is protected by BitLocker, it is mounted with Read and Write access.
When disabled or not configured	All fixed data drives on the computer are mounted with Read and Write access.

Reference

This policy setting is applied when you turn on BitLocker.

Conflict considerations include:

1. When this policy setting is enabled, users receive "Access denied" error messages when they try to save data to unencrypted fixed data drives. See the Reference section for additional conflicts.

2. If BdeHdCfg.exe is run on a computer when this policy setting is enabled, you could encounter the following issues:

    - If you attempted to shrink the drive and create the system drive, the drive size is successfully reduced and a raw partition is created. However, the raw partition is not formatted. The following error message is displayed: "The new active drive cannot be formatted. You may need to manually prepare your drive for BitLocker."

    - If you attempt to use unallocated space to create the system drive, a raw partition will be created. However, the raw partition will not be formatted. The following error message is displayed: "The new active drive cannot be formatted. You may need to manually prepare your drive for BitLocker."

    - If you attempt to merge an existing drive into the system drive, the tool fails to copy the required boot file onto the target drive to create the system drive. The following error message is displayed: "BitLocker setup failed to copy boot files. You may need to manually prepare your drive for BitLocker."

3. If this policy setting is enforced, a hard drive cannot be repartitioned because the drive is protected. If you are upgrading computers in your organization from a previous version of Windows, and those computers were configured with a single partition, you should create the required BitLocker system partition before you apply this policy setting to the computers.

Deny write access to removable drives not protected by BitLocker

This policy setting is used to require that removable drives are encrypted prior to granting Write access, and to control whether BitLocker-protected removable drives that were configured in another organization can be opened with Write access.

Policy description	With this policy setting, you can configure whether BitLocker protection is required for a computer to be able to write data to a removable data drive.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Removable data drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives
Conflicts	See the Reference section for a description of conflicts.
When enabled	All removable data drives that are not BitLocker-protected are mounted as Read-only. If the drive is protected by BitLocker, it is mounted with Read and Write access.
When disabled or not configured	All removable data drives on the computer are mounted with Read and Write access.

Reference

If the **Deny write access to devices configured in another organization** option is selected, only drives with identification fields that match the computer's identification fields are given Write access. When a removable data drive is accessed, it is checked for a valid identification field and allowed identification fields. These fields are defined by the **Provide the unique identifiers for your organization** policy setting.

Note

You can override this policy setting with the policy settings under **User Configuration\Administrative Templates\System\Removable Storage Access**. If the **Removable Disks: Deny write access** policy setting is enabled, this policy setting will be ignored.

Conflict considerations include:

1. Use of BitLocker with the TPM plus a startup key or with the TPM plus a PIN and startup key must be disallowed if the **Deny write access to removable drives not protected by BitLocker** policy setting is enabled.

2. Use of recovery keys must be disallowed if the **Deny write access to removable drives not protected by BitLocker** policy setting is enabled.

3. You must enable the **Provide the unique identifiers for your organization** policy setting if you want to deny Write access to drives that were configured in another organization.

Control use of BitLocker on removable drives

This policy setting is used to prevent users from turning BitLocker on or off on removable data drives.

Policy description	With this policy setting, you can control the use of BitLocker on removable data drives.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Removable data drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives
Conflicts	None
When enabled	You can select property settings that control how users can configure BitLocker.
When disabled	Users cannot use BitLocker on removable data drives.
When not configured	Users can use BitLocker on removable data drives.

Reference

This policy setting is applied when you turn on BitLocker.

For information about suspending BitLocker protection, see BitLocker Basic Deployment.

The options for choosing property settings that control how users can configure BitLocker are:

- **Allow users to apply BitLocker protection on removable data drives** Enables the user to run the BitLocker Setup Wizard on a removable data drive.
- **Allow users to suspend and decrypt BitLocker on removable data drives** Enables the user to remove BitLocker from the drive or to suspend the encryption while performing maintenance.

Choose drive encryption method and cipher strength

This policy setting is used to control the encryption method and cipher strength.

Policy description	With this policy setting, you can control the encryption method and strength for drives.
Introduced	Windows Server 2012 and Windows 8
Drive type	All drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption
Conflicts	None
When enabled	You can choose an encryption algorithm and key cipher strength for BitLocker to use to encrypt drives.
When disabled or not configured	BitLocker uses the default encryption method of AES 128-bit or the encryption method that is specified by the setup script.

Reference

By default, BitLocker uses AES 128-bit encryption. Available options are AES-128 and AES-256. The values of this policy determine the strength of the cipher that BitLocker uses for encryption. Enterprises may want to control the encryption level for increased security (AES-256 is stronger than AES-128).

Changing the encryption method has no effect if the drive is already encrypted or if encryption is in progress. In these cases, this policy setting is ignored.

Warning

This policy does not apply to encrypted drives. Encrypted drives utilize their own algorithm, which is set by the drive during partitioning.

When this policy setting is disabled, BitLocker uses AES with the same bit strength (128-bit or 256-bit) as specified in the policy setting **Choose drive encryption method and cipher strength (Windows Vista, Windows Server 2008, Windows 7)**. If neither policy is set, BitLocker uses the default encryption method, AES-128, or the encryption method that is specified in the setup script.

Configure use of hardware-based encryption for fixed data drives

This policy controls how BitLocker reacts to systems that are equipped with encrypted drives when they are used as fixed data volumes. Using hardware-based encryption can improve the performance of drive operations that involve frequent reading or writing of data to the drive.

Policy description	With this policy setting, you can manage BitLocker’s use of hardware-based encryption on fixed data drives and to specify which encryption algorithms BitLocker can use with hardware-based encryption.

Introduced	Windows Server 2012 and Windows 8
Drive type	Fixed data drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives
Conflicts	None
When enabled	You can specify additional options that control whether BitLocker software-based encryption is used instead of hardware-based encryption on computers that do not support hardware-based encryption. You can also specify whether you want to restrict the encryption algorithms and cipher suites that are used with hardware-based encryption.
When disabled	BitLocker cannot use hardware-based encryption with fixed data drives, and BitLocker software-based encryption is used by default when the drive in encrypted.
When not configured	BitLocker uses hardware-based encryption with the encryption algorithm that is set for the drive. If hardware-based encryption is not available, BitLocker software-based encryption is used instead.

Reference

Note

The **Choose drive encryption method and cipher strength** policy setting does not apply to hardware-based encryption.

The encryption algorithm that is used by hardware-based encryption is set when the drive is partitioned. By default, BitLocker uses the algorithm that is configured on the drive to encrypt the drive. The **Restrict encryption algorithms and cipher suites allowed for hardware-based encryption** option of this setting enables you to restrict the encryption algorithms that BitLocker can use with hardware encryption. If the algorithm that is set for the drive is not available, BitLocker disables the use of hardware-based encryption. Encryption algorithms are specified by object identifiers (OID), for example:

- Advanced Encryption Standard (AES) 128 in Cipher Block Chaining (CBC) mode OID: 2.16.840.1.101.3.4.1.2
- AES 256 in CBC mode OID: 2.16.840.1.101.3.4.1.42

Configure use of hardware-based encryption for operating system drives

This policy controls how BitLocker reacts when encrypted drives are used as operating system drives. Using hardware-based encryption can improve the performance of drive operations that involve frequent reading or writing of data to the drive.

Policy description	With this policy setting, you can manage BitLocker's use of hardware-based encryption on operating system drives and specify which encryption algorithms it can use with hardware-based encryption.
Introduced	Windows Server 2012 and Windows 8
Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	None
When enabled	You can specify additional options that control whether BitLocker software-based encryption is used instead of hardware-based encryption on computers that do not support hardware-based encryption. You can also specify whether you want to restrict the encryption algorithms and cipher suites that are used with hardware-based encryption.
When disabled	BitLocker cannot use hardware-based encryption with operating system drives, and BitLocker software-based encryption is used by default when the drive in encrypted.
When not configured	BitLocker uses hardware-based encryption with the encryption algorithm that is set for the drive. If hardware-based encryption is not available, BitLocker software-based encryption is used instead.

Reference

If hardware-based encryption is not available, BitLocker software-based encryption is used instead.

Note

The **Choose drive encryption method and cipher strength** policy setting does not apply to hardware-based encryption.

The encryption algorithm that is used by hardware-based encryption is set when the drive is partitioned. By default, BitLocker uses the algorithm that is configured on the drive to encrypt the drive. The **Restrict encryption algorithms and cipher suites allowed for hardware-based encryption** option of this setting enables you to restrict the encryption algorithms that BitLocker can use with hardware encryption. If the algorithm that is set for the drive is not available, BitLocker disables the use of hardware-based encryption. Encryption algorithms are specified by object identifiers (OID), for example:

- Advanced Encryption Standard (AES) 128 in Cipher Block Chaining (CBC) mode OID: 2.16.840.1.101.3.4.1.2
- AES 256 in CBC mode OID: 2.16.840.1.101.3.4.1.42

Configure use of hardware-based encryption for removable data drives

This policy controls how BitLocker reacts to encrypted drives when they are used as removable data drives. Using hardware-based encryption can improve the performance of drive operations that involve frequent reading or writing of data to the drive.

Policy description	With this policy setting, you can manage BitLocker's use of hardware-based encryption on removable data drives and specify which encryption algorithms it can use with hardware-based encryption.
Introduced	Windows Server 2012 and Windows 8
Drive type	Removable data drive
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives
Conflicts	None
When enabled	You can specify additional options that control whether BitLocker software-based encryption is used instead of hardware-based encryption on computers that do not support hardware-based encryption. You can also specify whether you want to restrict the encryption algorithms and cipher suites that are used with hardware-based encryption.
When disabled	BitLocker cannot use hardware-based encryption with removable data drives, and BitLocker software-based encryption is used by default when the drive in encrypted.
When not configured	BitLocker uses hardware-based encryption with the encryption algorithm that is set for the drive. If hardware-based encryption is not available, BitLocker software-based encryption is used instead.

Reference

If hardware-based encryption is not available, BitLocker software-based encryption is used instead.

Note

The **Choose drive encryption method and cipher strength** policy setting does not apply to hardware-based encryption.

The encryption algorithm that is used by hardware-based encryption is set when the drive is partitioned. By default, BitLocker uses the algorithm that is configured on the drive to encrypt the drive. The **Restrict encryption algorithms and cipher suites allowed for hardware-based encryption** option of this setting enables you to restrict the encryption algorithms that BitLocker can use with hardware encryption. If the algorithm that is set for the drive is not available, BitLocker disables the use of hardware-based encryption. Encryption algorithms are specified by object identifiers (OID), for example:

- Advanced Encryption Standard (AES) 128 in Cipher Block Chaining (CBC) mode OID: 2.16.840.1.101.3.4.1.2
- AES 256 in CBC mode OID: 2.16.840.1.101.3.4.1.42

Enforce drive encryption type on fixed data drives

This policy controls whether fixed data drives utilize Used Space Only encryption or Full encryption. Setting this policy also causes the BitLocker Setup Wizard to skip the encryption options page so no encryption selection displays to the user.

Policy description	With this policy setting, you can configure the encryption type that is used by BitLocker.
Introduced	Windows Server 2012 and Windows 8
Drive type	Fixed data drive
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives
Conflicts	None
When enabled	This policy defines the encryption type that BitLocker uses to encrypt drives, and the encryption type option is not presented in the BitLocker Setup Wizard.
When disabled or not configured	The BitLocker Setup Wizard asks the user to select the encryption type before turning on BitLocker.

Reference

This policy setting is applied when you turn on BitLocker. Changing the encryption type has no effect if the drive is already encrypted or if encryption is in progress. Choose Full encryption to require that the entire drive be encrypted when BitLocker is turned on. Choose Used Space Only encryption to require that only the portion of the drive that is used to store data is encrypted when BitLocker is turned on.

Note

This policy is ignored when you are shrinking or expanding a volume and the BitLocker driver uses the current encryption method. For example, when a drive that is using Used Space Only encryption is expanded, the new free space is not wiped as it would be for a drive that is using Full encryption. The user could wipe the free space on a Used Space Only drive by using the following command: **manage-bde -w**. If the volume is shrunk, no action is taken for the new free space.

For more information about the tool to manage BitLocker, see Manage-bde.

Enforce drive encryption type on operating system drives

This policy controls whether operating system drives utilize Full encryption or Used Space Only encryption. Setting this policy also causes the BitLocker Setup Wizard to skip the encryption options page, so no encryption selection displays to the user.

Policy description	With this policy setting, you can configure the encryption type that is used by BitLocker.
Introduced	Windows Server 2012 and Windows 8
Drive type	Operating system drive
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	None
When enabled	The encryption type that BitLocker uses to encrypt drives is defined by this policy, and the encryption type option is not presented in the BitLocker Setup Wizard.
When disabled or not configured	The BitLocker Setup Wizard asks the user to select the encryption type before turning on BitLocker.

Reference

This policy setting is applied when you turn on BitLocker. Changing the encryption type has no effect if the drive is already encrypted or if encryption is in progress. Choose Full encryption to require that the entire drive be encrypted when BitLocker is turned on. Choose Used Space Only encryption to require that only the portion of the drive that is used to store data is encrypted when BitLocker is turned on.

Note

This policy is ignored when shrinking or expanding a volume, and the BitLocker driver uses the current encryption method. For example, when a drive that is using Used Space Only encryption is expanded, the new free space is not wiped as it would be for a drive that uses Full encryption. The user could wipe the free space on a Used Space Only drive by using the following command: **manage-bde -w**. If the volume is shrunk, no action is taken for the new free space.

For more information about the tool to manage BitLocker, see Manage-bde.

Enforce drive encryption type on removable data drives

This policy controls whether fixed data drives utilize Full encryption or Used Space Only encryption. Setting this policy also causes the BitLocker Setup Wizard to skip the encryption options page, so no encryption selection displays to the user.

Policy description	With this policy setting, you can configure the encryption type that is used by BitLocker.
Introduced	Windows Server 2012 and Windows 8
Drive type	Removable data drive
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives
Conflicts	None
When enabled	The encryption type that BitLocker uses to encrypt drives is defined by this policy, and the encryption type option is not presented in the BitLocker Setup Wizard.
When disabled or not configured	The BitLocker Setup Wizard asks the user to select the encryption type before turning on BitLocker.

Reference

This policy setting is applied when you turn on BitLocker. Changing the encryption type has no effect if the drive is already encrypted or if encryption is in progress. Choose Full encryption to require that the entire drive be encrypted when BitLocker is turned on. Choose Used Space Only encryption to require that only the portion of the drive that is used to store data is encrypted when BitLocker is turned on.

Note

This policy is ignored when shrinking or expanding a volume, and the BitLocker driver uses the current encryption method. For example, when a drive that is using Used Space Only encryption is expanded, the new free space is not wiped as it would be for a drive that is using Full Encryption. The user could wipe the free space on a Used Space Only drive by using the following command: **manage-bde -w**. If the volume is shrunk, no action is taken for the new free space.

For more information about the tool to manage BitLocker, see Manage-bde.

Choose how BitLocker-protected operating system drives can be recovered

This policy setting is used to configure recovery methods for operating system drives.

Policy description	With this policy setting, you can control how BitLocker-protected operating system drives are recovered in the absence of the required startup key information.
Introduced	Windows Server 2008 R2 and Windows 7

Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	You must disallow the use of recovery keys if the **Deny write access to removable drives not protected by BitLocker** policy setting is enabled. When using data recovery agents, you must enable the **Provide the unique identifiers for your organization** policy setting.
When enabled	You can control the methods that are available to users to recover data from BitLocker-protected operating system drives.
When disabled or not configured	The default recovery options are supported for BitLocker recovery. By default, a data recovery agent is allowed, the recovery options can be specified by the user (including the recovery password and recovery key), and recovery information is not backed up to AD DS.

Reference

This policy setting is applied when you turn on BitLocker.

The **Allow data recovery agent** check box is used to specify whether a data recovery agent can be used with BitLocker-protected operating system drives. Before a data recovery agent can be used, it must be added from **Public Key Policies**, which is located in the Group Policy Management Console (GPMC) or in the Local Group Policy Editor.

For more information about adding data recovery agents, see BitLocker Basic Deployment.

In **Configure user storage of BitLocker recovery information**, select whether users are allowed, required, or not allowed to generate a 48-digit recovery password.

Select **Omit recovery options from the BitLocker setup wizard** to prevent users from specifying recovery options when they enable BitLocker on a drive. This means that you will not be able to specify which recovery option to use when you enable BitLocker. Instead, BitLocker recovery options for the drive are determined by the policy setting.

In **Save BitLocker recovery information to Active Directory Domain Services**, choose which BitLocker recovery information to store in Active Directory Domain Services (AD DS) for operating system drives. If you select **Store recovery password and key packages**, the BitLocker recovery password and the key package are stored in AD DS. Storing the key package supports recovering data from a drive that is physically corrupted. If you select **Store recovery password only**, only the recovery password is stored in AD DS.

Select the **Do not enable BitLocker until recovery information is stored in AD DS for operating system drives** check box if you want to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds.

Note

If the **Do not enable BitLocker until recovery information is stored in AD DS for operating system drives** check box is selected, a recovery password is automatically generated.

Choose how users can recover BitLocker-protected drives (Windows Server 2008 and Windows Vista)

This policy setting is used to configure recovery methods for BitLocker-protected drives on computers running Windows Server 2008 or Windows Vista.

Policy description	With this policy setting, you can control whether the BitLocker Setup Wizard can display and specify BitLocker recovery options.
Introduced	Windows Server 2008 and Windows Vista
Drive type	Operating system drives and fixed data drives on computers running Windows Server 2008 and Windows Vista
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption
Conflicts	This policy setting provides an administrative method of recovering data that is encrypted by BitLocker to prevent data loss due to lack of key information. If you choose the **Do not allow** option for both user recovery options, you must enable the **Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista)** policy setting to prevent a policy error.
When enabled	You can configure the options that the Bitlocker Setup Wizard displays to users for recovering BitLocker encrypted data.
When disabled or not configured	The BitLocker Setup Wizard presents users with ways to store recovery options.

Reference

This policy is only applicable to computers running Windows Server 2008 or Windows Vista. This policy setting is applied when you turn on BitLocker.

Two recovery options can be used to unlock BitLocker-encrypted data in the absence of the required startup key information. Users can type a 48-digit numerical recovery password, or they can insert a USB drive that contains a 256-bit recovery key.

Saving the recovery password to a USB drive stores the 48-digit recovery password as a text file and the 256-bit recovery key as a hidden file. Saving it to a folder stores the 48-digit recovery password as a text file. Printing it sends the 48-digit recovery password to the default printer. For

example, not allowing the 48-digit recovery password prevents users from printing or saving recovery information to a folder.

Important

If TPM initialization is performed during the BitLocker setup, TPM owner information is saved or printed with the BitLocker recovery information.
The 48-digit recovery password is not available in FIPS-compliance mode.

Important

To prevent data loss, you must have a way to recover BitLocker encryption keys. If you do not allow both recovery options, you must enable the backup of BitLocker recovery information to AD DS. Otherwise, a policy error occurs.

Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista)

This policy setting is used to configure the storage of BitLocker recovery information in AD DS. This provides an administrative method of recovering data that is encrypted by BitLocker to prevent data loss due to lack of key information.

Policy description	With this policy setting, you can manage the AD DS backup of BitLocker Drive Encryption recovery information.
Introduced	Windows Server 2008 and Windows Vista
Drive type	Operating system drives and fixed data drives on computers running Windows Server 2008 and Windows Vista.
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption
Conflicts	None
When enabled	BitLocker recovery information is automatically and silently backed up to AD DS when BitLocker is turned on for a computer.
When disabled or not configured	BitLocker recovery information is not backed up to AD DS.

Reference

This policy is only applicable to computers running Windows Server 2008 or Windows Vista.

This policy setting is applied when you turn on BitLocker.

BitLocker recovery information includes the recovery password and unique identifier data. You can also include a package that contains an encryption key for a BitLocker-protected drive. This

key package is secured by one or more recovery passwords, and it can help perform specialized recovery when the disk is damaged or corrupted.

If you select **Require BitLocker backup to AD DS**, BitLocker cannot be turned on unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds. This option is selected by default to help ensure that BitLocker recovery is possible.

A recovery password is a 48-digit number that unlocks access to a BitLocker-protected drive. A key package contains a drive's BitLocker encryption key, which is secured by one or more recovery passwords. Key packages may help perform specialized recovery when the disk is damaged or corrupted.

If the **Require BitLocker backup to AD DS** option is not selected, AD DS backup is attempted, but network or other backup failures do not prevent the BitLocker setup. The Backup process is not automatically retried, and the recovery password might not be stored in AD DS during BitLocker setup.

TPM initialization might be needed during the BitLocker setup. Enable the **Turn on TPM backup to Active Directory Domain Services** policy setting in **Computer Configuration\Administrative Templates\System\Trusted Platform Module Services** to ensure that TPM information is also backed up.

For more information about this setting, see Turn on TPM backup to Active Directory Domain Services.

If you are using domain controllers running Windows Server 2003 with Service Pack 1, you must first set up appropriate schema extensions and access control settings on the domain before a backup to AD DS can succeed. For more information, see Backing Up BitLocker and TPM Recovery Information to AD DS.

Choose default folder for recovery password

This policy setting is used to configure the default folder for recovery passwords.

Policy description	With this policy setting, you can specify the default path that is displayed when the BitLocker Setup Wizard prompts the user to enter the location of a folder in which to save the recovery password.
Introduced	Windows Vista
Drive type	All drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption
Conflicts	None

When enabled	You can specify the path that will be used as the default folder location when the user chooses the option to save the recovery password in a folder. You can specify a fully qualified path or include the target computer's environment variables in the path. If the path is not valid, the BitLocker Setup Wizard displays the computer's top-level folder view.
When disabled or not configured	The BitLocker Setup Wizard displays the computer's top-level folder view when the user chooses the option to save the recovery password in a folder.

Reference

This policy setting is applied when you turn on BitLocker.

Note

This policy setting does not prevent the user from saving the recovery password in another folder.

Choose how BitLocker-protected fixed drives can be recovered

This policy setting is used to configure recovery methods for fixed data drives.

Policy description	With this policy setting, you can control how BitLocker-protected fixed data drives are recovered in the absence of the required credentials.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Fixed data drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives
Conflicts	You must disallow the use of recovery keys if the **Deny write access to removable drives not protected by BitLocker** policy setting is enabled. When using data recovery agents, you must enable and configure the **Provide the unique identifiers for your organization** policy setting.
When enabled	You can control the methods that are available to users to recover data from BitLocker-protected fixed data drives.
When disabled or not configured	The default recovery options are supported for BitLocker recovery. By default, a data recovery agent is allowed, the recovery options can be specified by the user (including the recovery password and recovery key), and recovery information is not backed up to AD DS.

Reference

This policy setting is applied when you turn on BitLocker.

The **Allow data recovery agent** check box is used to specify whether a data recovery agent can be used with BitLocker-protected fixed data drives. Before a data recovery agent can be used, it must be added from **Public Key Policies**, which is located in the Group Policy Management Console (GPMC) or in the Local Group Policy Editor.

In **Configure user storage of BitLocker recovery information**, select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key.

Select **Omit recovery options from the BitLocker setup wizard** to prevent users from specifying recovery options when they enable BitLocker on a drive. This means that you cannot specify which recovery option to use when you enable BitLocker. Instead, BitLocker recovery options for the drive are determined by the policy setting.

In **Save BitLocker recovery information to Active Directory Doman Services**, choose which BitLocker recovery information to store in AD DS for fixed data drives. If you select **Backup recovery password and key package**, the BitLocker recovery password and the key package are stored in AD DS. Storing the key package supports recovering data from a drive that has been physically corrupted. To recover this data, you can use the **Repair-bde** command-line tool. If you select **Backup recovery password only**, only the recovery password is stored in AD DS.

For more information about the BitLocker repair tool, see Repair-bde.

Select the **Do not enable BitLocker until recovery information is stored in AD DS for fixed data drives** check box if you want to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds.

Note
If the **Do not enable BitLocker until recovery information is stored in AD DS for fixed data drives** check box is selected, a recovery password is automatically generated.

Choose how BitLocker-protected removable drives can be recovered

This policy setting is used to configure recovery methods for removable data drives.

Policy description	With this policy setting, you can control how BitLocker-protected removable data drives are recovered in the absence of the required credentials.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Removable data drives
Policy path	Computer Configuration\Administrative Templates\Windows

	Components\BitLocker Drive Encryption\Removable Data Drives
Conflicts	You must disallow the use of recovery keys if the **Deny write access to removable drives not protected by BitLocker** policy setting is enabled. When using data recovery agents, you must enable and configure the **Provide the unique identifiers for your organization** policy setting.
When enabled	You can control the methods that are available to users to recover data from BitLocker-protected removable data drives.
When disabled or not configured	The default recovery options are supported for BitLocker recovery. By default, a data recovery agent is allowed, the recovery options can be specified by the user (including the recovery password and recovery key), and recovery information is not backed up to AD DS.

Reference

This policy setting is applied when you turn on BitLocker.

The **Allow data recovery agent** check box is used to specify whether a data recovery agent can be used with BitLocker-protected removable data drives. Before a data recovery agent can be used, it must be added from **Public Key Policies** , which is accessed using the GPMC or the Local Group Policy Editor.

In **Configure user storage of BitLocker recovery information**, select whether users are allowed, required, or not allowed to generate a 48-digit recovery password.

Select **Omit recovery options from the BitLocker setup wizard** to prevent users from specifying recovery options when they enable BitLocker on a drive. This means that you cannot specify which recovery option to use when you enable BitLocker. Instead, BitLocker recovery options for the drive are determined by the policy setting.

In **Save BitLocker recovery information to Active Directory Domain Services**, choose which BitLocker recovery information to store in AD DS for removable data drives. If you select **Backup recovery password and key package**, the BitLocker recovery password and the key package are stored in AD DS. If you select **Backup recovery password only**, only the recovery password is stored in AD DS.

Select the **Do not enable BitLocker until recovery information is stored in AD DS for removable data drives** check box if you want to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of BitLocker recovery information to AD DS succeeds.

Note

If the **Do not enable BitLocker until recovery information is stored in AD DS for fixed data drives** check box is selected, a recovery password is automatically generated.

Allow Secure Boot for integrity validation

This policy controls how BitLocker-enabled system volumes are handled in conjunction with the Secure Boot feature. Enabling this feature forces Secure Boot validation during the boot process and verifies Boot Configuration Data (BCD) settings according to the Secure Boot policy.

Policy description	With this policy setting, you can configure whether Secure Boot will be allowed as the platform integrity provider for BitLocker operating system drives.
Introduced	Windows Server 2012 and Windows 8
Drive type	All drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	If the **Configure TPM platform validation profile for native UEFI firmware configurations** Group Policy setting is enabled and PCR 7 is omitted, BitLocker is prevented from using Secure Boot for platform or BCD integrity validation. For more information about PCR 7, see About the Platform Configuration Register (PCR) in this topic.
When enabled or not configured	BitLocker uses Secure Boot for platform integrity if the platform is capable of Secure Boot-based integrity validation.
When disabled	BitLocker uses legacy platform integrity validation, even on systems that are capable of Secure Boot-based integrity validation.

Reference

Secure Boot ensures that the computer's preboot environment loads only firmware that is digitally signed by authorized software publishers. Secure Boot also provides more flexibility for managing preboot configurations than BitLocker integrity checks prior to Windows Server 2012 and Windows 8.

When this policy is enabled and the hardware is capable of using Secure Boot for BitLocker scenarios, the **Use enhanced Boot Configuration Data validation profile** Group Policy setting is ignored, and Secure Boot verifies BCD settings according to the Secure Boot policy setting, which is configured separately from BitLocker.

Warning

Enabling this policy might result in BitLocker recovery when manufacturer-specific firmware is updated. If you disable this policy, suspend BitLocker prior to applying firmware updates.

Provide the unique identifiers for your organization

This policy setting is used to establish an identifier that is applied to all drives that are encrypted in your organization.

Policy description	With this policy setting, you can associate unique organizational identifiers to a new drive that is enabled with BitLocker.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	All drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption
Conflicts	Identification fields are required to manage certificate-based data recovery agents on BitLocker-protected drives. BitLocker manages and updates certificate-based data recovery agents only when the identification field is present on a drive and it is identical to the value that is configured on the computer.
When enabled	You can configure the identification field on the BitLocker-protected drive and any allowed identification field that is used by your organization.
When disabled or not configured	The identification field is not required.

Reference

These identifiers are stored as the identification field and the allowed identification field. The identification field allows you to associate a unique organizational identifier to BitLocker-protected drives. This identifier is automatically added to new BitLocker-protected drives, and it can be updated on existing BitLocker-protected drives by using the **Manage-bde** command-line tool.

An identification field is required to manage certificate-based data recovery agents on BitLocker-protected drives and for potential updates to the BitLocker To Go Reader. BitLocker manages and updates data recovery agents only when the identification field on the drive matches the value that is configured in the identification field. In a similar manner, BitLocker updates the BitLocker To Go Reader only when the identification field on the drive matches the value that is configured for the identification field.

For more information about the tool to manage BitLocker, see Manage-bde.

The allowed identification field is used in combination with the **Deny write access to removable drives not protected by BitLocker** policy setting to help control the use of

removable drives in your organization. It is a comma-separated list of identification fields from your organization or external organizations.

You can configure the identification fields on existing drives by using the **Manage-bde** command-line tool.

When a BitLocker-protected drive is mounted on another BitLocker-enabled computer, the identification field and the allowed identification field are used to determine whether the drive is from an outside organization.

Multiple values separated by commas can be entered in the identification and allowed identification fields. The identification field can be any value up to 260 characters.

Prevent memory overwrite on restart

This policy setting is used to control whether the computer's memory will be overwritten the next time the computer is restarted.

Policy description	With this policy setting, you can control computer restart performance at the risk of exposing BitLocker secrets.
Introduced	Windows Vista
Drive type	All drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption
Conflicts	None
When enabled	The computer will not overwrite memory when it restarts. Preventing memory overwrite may improve restart performance, but it increases the risk of exposing BitLocker secrets.
When disabled or not configured	BitLocker secrets are removed from memory when the computer restarts.

Reference

This policy setting is applied when you turn on BitLocker. BitLocker secrets include key material that is used to encrypt data. This policy setting applies only when BitLocker protection is enabled.

Configure TPM platform validation profile for BIOS-based firmware configurations

This policy setting determines what values the TPM measures when it validates early boot components before it unlocks an operating system drive on a computer with a BIOS configuration or with UEFI firmware that has the Compatibility Support Module (CSM) enabled.

Policy description	With this policy setting, you can configure how the computer's TPM security hardware secures the BitLocker encryption key.
Introduced	Windows Server 2012 and Windows 8
Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	None
When enabled	You can configure the boot components that the TPM validates before unlocking access to the BitLocker-encrypted operating system drive. If any of these components change while BitLocker protection is in effect, the TPM does not release the encryption key to unlock the drive. Instead, the computer displays the BitLocker Recovery console and requires that the recovery password or the recovery key is provided to unlock the drive.
When disabled or not configured	The TPM uses the default platform validation profile or the platform validation profile that is specified by the setup script.

Reference

This policy setting does not apply if the computer does not have a compatible TPM or if BitLocker has already been turned on with TPM protection.

Important

This Group Policy setting only applies to computers with BIOS configurations or to computers with UEFI firmware with the CSM enabled. Computers that use a native UEFI firmware configuration store different values in the Platform Configuration Registers (PCRs). Use the **Configure TPM platform validation profile for native UEFI firmware configurations** Group Policy setting to configure the TPM PCR profile for computers that use native UEFI firmware.

A platform validation profile consists of a set of PCR indices that range from 0 to 23. The default platform validation profile secures the encryption key against changes to the following:

- Core Root of Trust of Measurement (CRTM), BIOS, and Platform Extensions (PCR 0)
- Option ROM Code (PCR 2)
- Master Boot Record (MBR) Code (PCR 4)

- NTFS Boot Sector (PCR 8)
- NTFS Boot Block (PCR 9)
- Boot Manager (PCR 10)
- BitLocker Access Control (PCR 11)

Note
Changing from the default platform validation profile affects the security and manageability of your computer. BitLocker's sensitivity to platform modifications (malicious or authorized) is increased or decreased depending on inclusion or exclusion (respectively) of the PCRs.

The following list identifies all of the PCRs available:

- PCR 0: Core root-of-trust for measurement, BIOS, and Platform extensions
- PCR 1: Platform and motherboard configuration and data.
- PCR 2: Option ROM code
- PCR 3: Option ROM data and configuration
- PCR 4: Master Boot Record (MBR) code
- PCR 5: Master Boot Record (MBR) partition table
- PCR 6: State transition and wake events
- PCR 7: Computer manufacturer-specific
- PCR 8: NTFS boot sector
- PCR 9: NTFS boot block
- PCR 10: Boot manager
- PCR 11: BitLocker access control
- PCR 12-23: Reserved for future use

Configure TPM platform validation profile (Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2)

This policy setting determines what values the TPM measures when it validates early boot components before unlocking a drive on a computer running Windows Vista, Windows Server 2008, or Windows 7.

Policy description	With this policy setting, you can configure how the computer's TPM security hardware secures the BitLocker encryption key.
Introduced	Windows Server 2008 and Windows Vista
Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	None
When enabled	You can configure the boot components that the TPM validates before unlocking access to the BitLocker-encrypted operating system drive. If any of these components change while BitLocker protection is in effect, the TPM does not release the encryption key to unlock the drive. Instead, the computer displays the BitLocker Recovery console and requires that the recovery password or the recovery key is provided to unlock the drive.
When disabled or not configured	The TPM uses the default platform validation profile or the platform validation profile that is specified by the setup script.

Reference

This policy setting does not apply if the computer does not have a compatible TPM or if BitLocker is already turned on with TPM protection.

A platform validation profile consists of a set of PCR indices that range from 0 to 23. The default platform validation profile secures the encryption key against changes to the following:

- Core Root of Trust of Measurement (CRTM), BIOS, and Platform Extensions (PCR 0)
- Option ROM Code (PCR 2)
- Master Boot Record (MBR) Code (PCR 4)
- NTFS Boot Sector (PCR 8)
- NTFS Boot Block (PCR 9)
- Boot Manager (PCR 10)
- BitLocker Access Control (PCR 11)

Note
The default TPM validation profile PCR settings for computers that use an Extensible Firmware Interface (EFI) are the PCRs 0, 2, 4, and 11 only.

The following list identifies all of the PCRs available:

- PCR 0: Core root-of-trust for measurement, EFI boot and run-time services, EFI drivers embedded in system ROM, ACPI static tables, embedded SMM code, and BIOS code
- PCR 1: Platform and motherboard configuration and data. Hand-off tables and EFI variables that affect system configuration
- PCR 2: Option ROM code
- PCR 3: Option ROM data and configuration
- PCR 4: Master Boot Record (MBR) code or code from other boot devices
- PCR 5: Master Boot Record (MBR) partition table. Various EFI variables and the GPT table
- PCR 6: State transition and wake events
- PCR 7: Computer manufacturer-specific
- PCR 8: NTFS boot sector
- PCR 9: NTFS boot block
- PCR 10: Boot manager
- PCR 11: BitLocker access control
- PCR 12 - 23: Reserved for future use

Warning

Changing from the default platform validation profile affects the security and manageability of your computer. BitLocker's sensitivity to platform modifications (malicious or authorized) is increased or decreased depending on inclusion or exclusion (respectively) of the PCRs.

Configure TPM platform validation profile for native UEFI firmware configurations

This policy setting determines what values the TPM measures when it validates early boot components before unlocking an operating system drive on a computer with native UEFI firmware configurations.

Policy description	With this policy setting, you can configure how the computer's Trusted Platform Module (TPM) security hardware secures the BitLocker encryption key.

Introduced	Windows Server 2012 and Windows 8
Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	Setting this policy with PCR 7 omitted, overrides the **Allow Secure Boot for integrity validation** Group Policy setting, and it prevents BitLocker from using Secure Boot for platform or Boot Configuration Data (BCD) integrity validation. If your environments use TPM and Secure Boot for platform integrity checks, this policy should not be configured. For more information about PCR 7, see About the Platform Configuration Register (PCR) in this topic.
When enabled	Before you turn on BitLocker, you can configure the boot components that the TPM validates before it unlocks access to the BitLocker-encrypted operating system drive. If any of these components change while BitLocker protection is in effect, the TPM does not release the encryption key to unlock the drive. Instead, the computer displays the BitLocker Recovery console and requires that the recovery password or the recovery key is provided to unlock the drive.
When disabled or not configured	BitLocker uses the default platform validation profile or the platform validation profile that is specified by the setup script.

Reference

This policy setting does not apply if the computer does not have a compatible TPM or if BitLocker is already turned on with TPM protection.

Important

This Group Policy setting only applies to computers with a native UEFI firmware configuration. Computers with BIOS or UEFI firmware with a Compatibility Support Module (CSM) enabled store different values in the Platform Configuration Registers (PCRs). Use the **Configure TPM platform validation profile for BIOS-based firmware configurations** Group Policy setting to configure the TPM PCR profile for computers with BIOS configurations or for computers with UEFI firmware with a CSM enabled.

A platform validation profile consists of a set of Platform Configuration Register (PCR) indices ranging from 0 to 23. The default platform validation profile secures the encryption key against changes to the core system firmware executable code (PCR 0), extended or pluggable executable code (PCR 2), boot manager (PCR 4), and the BitLocker access control (PCR 11).

The following list identifies all of the PCRs available:

- PCR 0: Core System Firmware executable code
- PCR 1: Core System Firmware data
- PCR 2: Extended or pluggable executable code
- PCR 3: Extended or pluggable firmware data
- PCR 4: Boot Manager
- PCR 5: GPT/Partition Table
- PCR 6: Resume from S4 and S5 Power State Events
- PCR 7: Secure Boot State

  For more information about this PCR, see About the Platform Configuration Register (PCR) in this topic.
- PCR 8: Initialized to 0 with no Extends (reserved for future use)
- PCR 9: Initialized to 0 with no Extends (reserved for future use)
- PCR 10: Initialized to 0 with no Extends (reserved for future use)
- PCR 11: BitLocker access control
- PCR 12: Data events and highly volatile events
- PCR 13: Boot Module Details
- PCR 14: Boot Authorities
- PCR 15 – 23: Reserved for future use

Warning
Changing from the default platform validation profile affects the security and manageability of your computer. BitLocker's sensitivity to platform modifications (malicious or authorized) is increased or decreased depending on inclusion or exclusion (respectively) of the PCRs.

Reset platform validation data after BitLocker recovery

This policy setting determines if you want platform validation data to refresh when Windows is started following a BitLocker recovery. A platform validation data profile consists of the values in a set of Platform Configuration Register (PCR) indices that range from 0 to 23.

Policy description	With this policy setting, you can control whether platform validation data is refreshed when Windows is started following a BitLocker recovery.
Introduced	Windows Server 2012 and Windows 8
Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	None
When enabled	Platform validation data is refreshed when Windows is started following a BitLocker recovery.
When disabled	Platform validation data is not refreshed when Windows is started following a BitLocker recovery.
When not configured	Platform validation data is refreshed when Windows is started following a BitLocker recovery.

Reference

For more information about the recovery process, see the BitLocker Recovery Guide.

Use enhanced Boot Configuration Data validation profile

This policy setting determines specific Boot Configuration Data (BCD) settings to verify during platform validation. A platform validation uses the data in the platform validation profile, which consists of a set of Platform Configuration Register (PCR) indices that range from 0 to 23.

Policy description	With this policy setting, you can specify Boot Configuration Data (BCD) settings to verify during platform validation.
Introduced	Windows Server 2012 and Windows 8
Drive type	Operating system drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
Conflicts	When BitLocker is using Secure Boot for platform and Boot Configuration Data integrity validation, the **Use enhanced Boot Configuration Data validation profile** Group Policy setting is ignored (as defined by the **Allow Secure Boot for integrity validation** Group Policy setting).
When enabled	You can add additional BCD settings, exclude the BCD settings you specify, or combine inclusion and exclusion lists to create a customized BCD validation profile, which gives you the ability to verify those BCD settings.
When disabled	The computer reverts to a BCD profile validation similar to the default BCD profile that is used by Windows 7.
When not	The computer verifies the default BCD settings in Windows.

configured

Reference

Note
The setting that controls boot debugging (0x16000010) is always validated, and it has no effect if it is included in the inclusion or the exclusion list.

Allow access to BitLocker-protected fixed data drives from earlier versions of Windows

This policy setting is used to control whether access to drives is allowed by using the BitLocker To Go Reader, and if the application is installed on the drive.

Policy description	With this policy setting, you can configure whether fixed data drives that are formatted with the FAT file system can be unlocked and viewed on computers running Windows Vista, Windows XP with Service Pack 3 (SP3), or Windows XP with Service Pack 2 (SP2).
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Fixed data drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives
Conflicts	None
When enabled and **When not configured**	Fixed data drives that are formatted with the FAT file system can be unlocked on computers running Windows Server 2008, Windows Vista, Windows XP with SP3, or Windows XP with SP2, and their content can be viewed. These operating systems have Read-only access to BitLocker-protected drives.
When disabled	Fixed data drives that are formatted with the FAT file system and are BitLocker-protected cannot be unlocked on computers running Windows Vista, Windows XP with SP3, or Windows XP with SP2. BitLocker To Go Reader (bitlockertogo.exe) is not installed.

Reference

Note
This policy setting does not apply to drives that are formatted with the NTFS file system.

When this policy setting is enabled, select the **Do not install BitLocker To Go Reader on FAT formatted fixed drives** check box to help prevent users from running BitLocker To Go Reader from their fixed drives. If BitLocker To Go Reader (bitlockertogo.exe) is present on a drive that does not have an identification field specified, or if the drive has the same identification field as

specified in the **Provide unique identifiers for your organization** policy setting, the user is prompted to update BitLocker, and BitLocker To Go Reader is deleted from the drive. In this situation, for the fixed drive to be unlocked on computers running Windows Vista, Windows XP with SP3, or Windows XP with SP2, BitLocker To Go Reader must be installed on the computer. If this check box is not selected, BitLocker To Go Reader will be installed on the fixed drive to enable users to unlock the drive on computers running Windows Vista, Windows XP with SP3, or Windows XP with SP2.

Allow access to BitLocker-protected removable data drives from earlier versions of Windows

This policy setting controls access to removable data drives that are using the BitLocker To Go Reader and whether the BitLocker To Go Reader can be installed on the drive.

Policy description	With this policy setting, you can configure whether removable data drives that are formatted with the FAT file system can be unlocked and viewed on computers running Windows Vista, Windows XP with SP3, or Windows XP with SP2.
Introduced	Windows Server 2008 R2 and Windows 7
Drive type	Removable data drives
Policy path	Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives
Conflicts	None
When enabled and **When not configured**	Removable data drives that are formatted with the FAT file system can be unlocked on computers running Windows Vista, Windows XP with SP3, or Windows XP with SP2, and their content can be viewed. These operating systems have Read-only access to BitLocker-protected drives.
When disabled	Removable data drives that are formatted with the FAT file system that are BitLocker-protected cannot be unlocked on computers running Windows Vista, Windows XP with SP3, or Windows XP with SP2. BitLocker To Go Reader (bitlockertogo.exe) is not installed.

Reference

Note

This policy setting does not apply to drives that are formatted with the NTFS file system.

When this policy setting is enabled, select the **Do not install BitLocker To Go Reader on FAT formatted removable drives** check box to help prevent users from running BitLocker To Go Reader from their removable drives. If BitLocker To Go Reader (bitlockertogo.exe) is present on a drive that does not have an identification field specified, or if the drive has the same identification field as specified in the **Provide unique identifiers for your organization** policy

setting, the user will be prompted to update BitLocker, and BitLocker To Go Reader is deleted from the drive. In this situation, for the removable drive to be unlocked on computers running Windows Vista, Windows XP with SP3, or Windows XP with SP2, BitLocker To Go Reader must be installed on the computer. If this check box is not selected, BitLocker To Go Reader will be installed on the removable drive to enable users to unlock the drive on computers running Windows Vista, Windows XP with SP3, or Windows XP with SP2 that do not have BitLocker To Go Reader installed.

FIPS setting

You can configure the Federal Information Processing Standard (FIPS) setting for FIPS compliance. As an effect of FIPS compliance, users cannot create or save a BitLocker password for recovery or as a key protector. The use of a recovery key is permitted.

Policy description	Notes
Introduced	Windows Server 2003 with SP1
Drive type	System-wide
Policy path	Local Policies\Security Options\System cryptography: **Use FIPS compliant algorithms for encryption, hashing, and signing**
Conflicts	Some applications, such as Terminal Services, do not support FIPS-140 on all operating systems.
When enabled	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 Setup izard to create a recovery password.
When disabled or not configured	No BitLocker encryption key is generated

Reference

This policy needs to be enabled before any encryption key is generated for BitLocker. Note that when this policy is enabled, BitLocker prevents creating or using recovery passwords, so recovery keys should be used instead.

You can save the optional recovery key to a USB drive. Because recovery passwords cannot be saved to AD DS when FIPS is enabled, an error is caused 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 these procedures.

For more information about setting this policy, see System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.

Power management Group Policy settings: Sleep and Hibernate

PCs default power settings for a computer will cause the computer to enter Sleep mode frequently to conserve power when idle and to help extend the system's battery life. When a computer transitions to Sleep, open programs and documents are persisted in memory. When a computer resumes 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.

However, when a computer hibernates the drive is locked, and when it resumes from hibernation the drive is unlocked, which means that users will need to provide a PIN or a startup key if using multifactor authentication with BitLocker. Therefore, organizations that use BitLocker may want to use Hibernate instead of Sleep for improved security. This setting does not have an impact on TPM-only mode, because it provides a transparent user experience at startup and when resuming from the Hibernate states.

You can use disable the following Group Policy settings, which are located in **Computer Configuration\Administrative Templates\System\Power Management** to disable all available sleep states:

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

About the Platform Configuration Register (PCR)

A platform validation profile consists of a set of PCR indices that range from 0 to 23. The scope of the values can be specific to the version of the operating system.

Changing from the default platform validation profile affects the security and manageability of your computer. BitLocker's sensitivity to platform modifications (malicious or authorized) is increased or decreased depending on inclusion or exclusion (respectively) of the PCRs.

About PCR 7

PCR 7 measures the state of Secure Boot. With PCR 7, BitLocker can leverage Secure Boot for integrity validation. Secure Boot ensures that the computer's preboot environment loads only firmware that is digitally signed by authorized software publishers. PCR 7 measurements indicate whether Secure Boot is on and which keys are trusted on the platform. If Secure Boot is on and the firmware measures PCR 7 correctly per the UEFI specification, BitLocker can bind to this information rather than to PCRs 0, 2, and 4 which have the measurements of the exact

firmware and Bootmgr images loaded. This reduces the likelihood of BitLocker starting in recovery mode as a result of firmware and image updates, and it provides you with greater flexibility to manage the preboot configuration.

PCR 7 measurements must follow the guidance that is described in Appendix A Trusted Execution Environment EFI Protocol.

PCR 7 measurements are a mandatory logo requirement for systems that support InstantGo (also known as Always On, Always Connected PCs), such as the Microsoft Surface RT. On such systems, if the TPM with PCR 7 measurement and Secure Boot are correctly configured, BitLocker binds to PCR 7 and PCR 11 by default.