

► Your BitLocker To Go Active Directory Policy Options

Tech Tip
by Philip Cox

Learn about your BitLocker To Go Active Directory policy options, including use on removable data drives and smart cards, write access to removable drives, access to drives from Windows XP or earlier, password length and recovery of keys.

In the second installment of his two part series, Phil Cox reviews recommended BitLocker To Go settings that should be configured in your organization.

▶ Your BitLocker To Go Active Directory Policy Options

Previously, we reviewed the basic features of BitLocker To Go. In this tip, we will explore specific BitLocker Active Directory policy options that will help you prevent accidental data loss. It is important to note that the configurations discussed here are controlled via Active Directory Group Policy, and thus are set and maintained by your organizations Group Policy administrators. They are not configured or controlled by the end user.

The Group Policy settings for BitLocker are located under the “Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\” tree. For the sake of space, we will only look at the portion of the policy tree that applies to removable drives (“Removable Data Drives” as they are referred to in BitLocker), but you should take the time to familiarize yourself with the other BitLocker policies as well (see <http://technet.microsoft.com/en-us/library/ee706521.aspx> for details). For each of the policy settings, we’ll cover their functions, and then I’ll give you my recommendation for how you should configure it and why (assuming you have decided that using BTG for data loss protection will be required).

- ▶ **Control use of BitLocker on removable drives:** This policy allows you to control if a user can enable, disable, or pause BitLocker functionality on removable drives. A “disabled” setting prevents users from enabling BitLocker To protect drives. A “Not configured” or “Enabled” setting will allow users to protect the devices. The “Enabled” setting gives you two more granular options: “Allow users to apply BitLocker protection on removable data drives” and “Allow users to suspend and decrypt BitLocker on removable data drives”. The first allows users to use the BitLocker Wizard to configure BitLocker on a drive. The second allows a user to remove or suspend the encryption.

Recommended settings: Enabled control, Allow users to apply protection, and do not allow users to “suspend and decrypt.” This will ensure that drives are protected, and that users will not disable that protection.

- ▶ **Configure use of smart cards on removable data drives:** This policy allows you to control whether smart cards can be used with BTG. A “disabled” setting prevents users from using smart cards. A “Not configured” or “Enabled” setting will allow users to protect (or not protect) devices. Another option, if enabled, is to “Require use of smart cards on removable drives.” This setting is enforced when placing BitLocker on a drive. If the drive has been enabled with smart cards from another system, BitLocker will allow unlocking with that mechanism.

Recommended settings: Not configured, as I assume most SMBs do not have ubiquitous use of smart cards deployed. If you have smart cards use in your organization that is an option I would choose.

- ▶ **Deny write access to removable drives not protected by BitLocker:** This policy basically allows you to force encryption on the drive before you write to it. A “Disabled” or “Not configured” setting will allow normal use (i.e., mounted with read and write access) of removable drives not protected by BitLocker. An “Enabled” setting will enforce BTG protection on the drive, as well as provide an option to “Deny write access to devices configured in another organization.” If you choose that setting, only BitLocker drives with identification fields that match the computer’s identification field will be mounted with write access. The option would allow you to enforce a corporate policy of using only company-issued removable media. This field is defined in the main BitLocker “Provide the unique identifiers for your organization” policy setting.

Recommended settings: Enable both settings. I believe that non-corporate owned/vetted USB thumb drives account for a significant amount of malicious code brought into an organization. By requiring the use of corporate supplied (i.e., they have been vetted before distribution) USB drives, a significant threat vector is reduced (although not completely eliminated).

▶ Your BitLocker To Go Active Directory Policy Options

- ▶ **Allow access to BitLocker-protected removable data drives from earlier versions of Windows:** This policy determines if removable data drives formatted with the FAT file system can be unlocked and viewed. A “Disabled” setting will prevent use of a FAT-based drive on Server 2008, Vista, XP (SP2/SP3) systems. A “Not configured” option will allow unlocking of a drive with a FAT file system. An “Enabled” setting will allow the unlocking, and provide another setting choice: “Do not install BitLocker To Go Reader on FAT formatted removable drives.” This latter option basically means that on Server 2008, Vista, or XP (SP2/SP3) an USB with a FAT file system would have to already have the BitLocker To Go Reader already installed on the computer. If the “do not install” option is not selected, BitLocker To Go Reader will be installed on the removable drive, thus enabling users to unlock the drive on the earlier systems.

Recommended settings: This should be dictated by corporate policy. If there is no policy addressing this situation, I would recommend you keep it as “Not configured”.

- ▶ **Configure use of passwords for removable data drives:** This policy controls the use of passwords for unlocking BitLocker-protected removable data drives. A “Disabled” setting will prevent the use of passwords, thus requiring smart cards. A “Not configured” selection will allow the use of passwords that are a minimum of 8 characters (no complexity). An “Enabled” setting will allow the use of passwords, as well as provide the ability to enforce complexity requirements, and configure a minimum length. You can allow, not allow, or require complexity, as well as set the minimum password length. Note: You will need to ensure the Group Policy setting “Password must meet complexity requirements” in the domain password policy is set as well.

Recommended settings: Enable password use, require complexity, and set the minimum length to be consistent with your corporate password policy. Two quick notes on this setting: First, you

will need access to a domain controller when enabling the protection, because that is where the complexity is validated. If you won’t have access, then set it to “allow complexity.” Second, as with earlier settings, these are enforced when enabling BitLocker on a drive, not when unlocking it. BTG will unlock a drive with any of the protectors available on the drive once it is enabled.

- ▶ **Choose how BitLocker-protected removable drives can be recovered:** This policy controls how data can be recovered without the required credentials. A “Disabled” or “Not configured” setting will allow for default recovery. Default recovery allows a Data Recovery Agent (DRA) to be configured on the system, and recovery options to be specified by the user. However, in the default mode, the recovery information is not backed up to AD. An “Enabled” setting allows you to “Allow data recovery agent” and “Configure user storage of BitLocker recovery information,” as well as “Omit recovery options from the BitLocker setup wizard” and “Save BitLocker recovery information to Active Directory Domain Services.” By default, if you enable the setting, a DRA is allowed, providing a 48-digit recovery password and a 256-bit recovery key. The recovery options are in the setup wizard, and both recovery password and keys are stored in the AD.

Recommended settings: Enable the policy, and use the default settings. This allows the user to configure recovery if they desire. One assumption is that there is nothing on removable drives that is irreplaceable. If you have an environment where there is an expectation that you can recover data that is on a removable drive, you should “require” the password and recovery key.

BitLocker To Go is an effective means to protect data on removable media such as thumb drives from accidental loss, if you have Windows 7. It is integrated into the Windows 7 operating system, it is easy to implement, reasonable to manage, and likely to be used. It is worth your time to investigate.

► Your BitLocker To Go Active Directory Policy Options

About The Author

Philip Cox is Director, Security and Compliance at SystemExperts Corporation, a consulting firm that specializes in system security and management. He is a well-known authority in the areas of system integration and security.

His experience includes Windows, UNIX, and IP-based networks integration, firewall design and implementation and ISO 17799 and PCI compliance. Phil frequently writes and lectures on issues dealing with heterogeneous system integration and compliance with PCI-DSS. He is the lead author of Windows 2000 Security Handbook Second Edition (Osborne McGraw-Hill) and contributing author for Windows NT/2000 Network Security (Macmillan Technical Publishing).