What's New in BitLocker for Windows 8 and Windows Server 2012

56 out of 74 rated this helpful - Rate this topic

Published: February 15, 2012

Updated: February 15, 2012

Applies To: Windows 8, Windows Server 2012

The following is a list of new functionality in BitLocker for Windows 8 and Windows Server 2012:

- New functionality in Windows 8 and Windows Server 2012:
  -
    - BitLocker provisioning

      BitLocker can be used to deploy drives to an encrypted state during installation prior to calling setup.
    - Used Disk Space Only encryption

      BitLocker now offers two encryption methods, Used Disk Space Only and Full volume encryption. Used Disk Space Only allows for a much quicker encryption experience by only encrypting used blocks on the targeted volume.
    - Standard User PIN and password change

      Allows a standard user to change the BitLocker PIN or password on operating system volumes and the BitLocker password on data volumes, reducing internal help desk call volume.
    - Network Unlock

      Enables a BitLocker system on a wired network to automatically unlock the system volume during boot (on capable Windows Server 2012 networks), reducing internal help desk call volumes for lost PINs.
    - Support for Encrypted Hard Drives for Windows

      BitLocker support for Encrypted Hard Drives provides users a familiar method for managing drive encryption along with the benefit of using hardware-based encryption.

BitLocker provisioning

In Windows Vista and Windows 7, BitLocker is provisioned post installation for system and data volumes through either the manage-bde command line interface or the Control Panel user interface. In Windows 8 and Windows 8.1, BitLocker can also be easily provisioned before the operating system is installed.

With this improvement administrators can enable BitLocker from the Windows Preinstallation Environment (WinPE) prior to operating system deployment. This is done with a randomly generated clear protector applied to the formatted volume and encrypting the volume prior to running the Windows setup process. If the encryption uses the Used Disk Space Only option described in the next section, this step takes only a few seconds and so incorporates well into regular deployment processes.

To check the BitLocker status of a particular volume, administrators can look at the status of the drive in the BitLocker control panel applet or Windows Explorer. When a drive is pre-provisioned for BitLocker, a status of "Waiting For Activation" is displayed with a yellow exclamation icon in the BitLocker Control Panel. This status means that there was only a clear protector used when encrypting the volume. In this case, the volume is not protected and needs to have a secure key added to the volume before the drive is considered fully protected. You can use the control panel, manage-bde tool or WMI APIs to add an appropriate key protector and the volume status will be updated. The following table shows the appropriate key protectors that can be added to drives that have been pre-provisioned with BitLocker protection:

Drive Type	**Key protector**
Operating System	TPM TPM+PIN Startup Key (for systems without a TPM) Password (for systems without a TPM)
Fixed data drive	Automatic unlock Password Smart card
Removable data drive	Password Smart card

Used Disk Space Only encryption

In Windows 7, BitLocker requires that all data and free space on the drive are encrypted. The encryption process can take a very long time on larger volumes. In Windows 8 and Windows 8.1, administrators can choose to encrypt the entire volume or the used space only. When you choose the Used Disk Space Only encryption option, only the portion of the drive that has data will be encrypted. Free disk space will not be encrypted. Used Disk Space Only encryption allows encryption to complete much faster on empty or partly empty drives than previous implementations of BitLocker. When provisioning BitLocker during Windows deployments, Used Disk Space Only encryption allows BitLocker to encrypt a drive in a short amount of time before installing the operating system. Full Encryption encrypts both data and free space on the volume, similar to the way BitLocker works in Windows 7 and Windows Vista.

New Group Policy settings for encryption type

You can use Group Policy settings to enforce that either Used Disk Space Only or Full Encryption is used when BitLocker is enabled on a drive. Group Policy settings for BitLocker Drive Encryption are located under the **\Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption** path of the Local Group Policy Editor

The following new Group Policies are available:

- **Fixed Data Drives\Enforce drive encryption type on fixed data drives**
- **Operating System Drives\Enforce drive encryption type on operating system drives**
- **Removable Data Drives\Enforce drive encryption type on removable data drives**

For each of these policies, once they are enabled you can then specify which type of encryption is required to be used on which drive type. If the policy is not configured the user will be able to choose the encryption method when they turn on BitLocker.

Standard User PIN and password change

Administrative privileges are required to configure BitLocker for operating system drives. In an organization where computers are managed by IT professionals and users are not normally granted administrative privileges, deploying the TPM + PIN protection option to large numbers of computers can be challenging. In Windows 8, administrative privileges are still required to configure BitLocker, however standard users are allowed to change the BitLocker PIN or password for the operating system volume or the BitLocker password for fixed data volumes by default. This gives users the ability to choose PINs and passwords that correspond to a personal mnemonic instead of requiring the user remember a randomly generated character set and allows IT professionals to use the same initial PIN or password setting for all computer images. This also presents the opportunity for users to choose passwords and PINs that are more susceptible to password guessing, dictionary attacks, and social engineering attacks and gives users the ability unlock any computer that still uses the original PIN or password assignment. Requiring password complexity and PIN complexity by Group Policy is recommended to help ensure that users take appropriate care when setting passwords and PINs.

Standard users are required to enter the current PIN or password for the drive to change the BitLocker PIN or BitLocker password. If a user enters an incorrect current PIN or password, the default tolerance for retry attempts is set to 5. Once the retry limit is reached, a standard user will not be able to change the BitLocker PIN or BitLocker password. The retry counter is set to zero when the computer is restarted or when an administrator resets the BitLocker PIN or BitLocker password.

You can disable the option to allow standard users to change PINs and passwords using the Group Policy setting **Disallow standard users from changing the PIN** located in the **\Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives** section of Local Group Policy Editor.

Network Unlock

Windows Server 2012 has added a new BitLocker protector option for Operating System Volumes called Network Unlock. Network Unlock will enable easier management for BitLocker enabled desktops and servers in a domain environment by providing automatic unlock of operating system volumes at system reboot when connected to a trusted wired corporate network. This feature requires the client hardware to have a DHCP driver implemented in its UEFI firmware.

Operating system volumes protected by TPM+PIN protectors require a PIN to be entered when a machine reboots or resumes from hibernation (for example, when configured for Wake on LAN). The requirement to enter a PIN can make it difficult for enterprises to install software patches to unattended desktops and servers. Network Unlock provides a method by which computers that are configured to use a TPM+PIN key protector can start Windows without user intervention. Network Unlock works in a similar fashion to the TPM+StartupKey. Rather than needing to read the StartupKey from USB media, however, the key for Network Unlock is composed from a key stored in the TPM and an encrypted network key that is sent to the server, decrypted and returned to the client in a secure session. The network key is stored on the system drive along with an AES 256 session key, and encrypted with the 2048-bit RSA public key of the unlock server's certificate. The network key is decrypted with the help of a provider on a Windows Server 2012 WDS server and returned encrypted with its corresponding session key. In instances where the Network Unlock provider is unavailable, the standard TPM+PIN unlock screen is presented to unlock the drive. The server side configuration to enable Network Unlock also requires provisioning a 2048 bit RSA public/private key pair in the form of an X.509 certificate, and for the public key certificate to be distributed to the clients. This certificate must be managed and deployed through the Group Policy Management Console directly on Windows Server 2012 Domain Controller. For more information see BitLocker: How to enable Network Unlock

Support for Encrypted Hard Drives for Windows

BitLocker provides Full Volume Encryption (FVE) of Windows operating system and data volumes using software-based encryption. In Windows 8 BitLocker also provide support for a new enhanced storage device type, the Encrypted Hard Drive, that is becoming a more common option in new servers and computers. Encrypted Hard Drives offer Full Disk Encryption (FDE), which means encryption occurs on each block of the physical drive. Encryption operations are more efficient on Encrypted Hard Drives because the encryption process is offloaded to the storage controller on the drive (also known as hardware-based encryption).

Windows 8 supports Encrypted Hard Drives natively in the operating system through the following mechanisms:

- Identification: Windows 8 will be able to identify that the drive is a Encrypted Hard Drive device type

- Activation: Windows 8 disk management will activate, create and map volumes to ranges/bands as appropriate

- Configuration: Windows 8 will create and map volumes to ranges/bands as appropriate

- API: Windows 8 provides API support for applications to manage Encrypted Hard Drives independently of BitLocker Drive Encryption

- BitLocker: BitLocker Control Panel will enable users to manage Encrypted Hard Drives in the same manner as full volume encrypted drives.