



Data security in HP ProLiant servers using the Trusted Platform Module and Microsoft® Windows® BitLocker™ Drive Encryption

HOWTO

Abstract.....	2
Overview.....	2
Enabling and configuring the TPM	2
Enabling BitLocker on HP ProLiant servers	4
BitLocker Drive Preparation Tool	5
Windows imaging with ImageX.....	5
BitLocker recovery process	6
Precautions affecting server maintenance and management.....	6
For more information.....	8
Call to action	8

Abstract

This HOWTO explains the Trusted Platform Module (TPM) and Microsoft® Windows® BitLocker™ Drive Encryption technologies and shows how they work together to provide data security in the HP ProLiant server line. It also includes best practices and explains other factors that affect server maintenance.

Overview

The need for robust security solutions to ensure trustworthy electronic transactions and prevent unauthorized access is a major concern of many businesses and institutions. HP is a founding member of the Trusted Computing Group (TCG), an organization established in 2003 to develop industry-standard specifications for hardware-enabled trusted computing and security technologies. To accomplish this, Trusted Computing uses the Trusted Platform Module (TPM), a hardware-based security feature.

The TPM is a hardware-based system security feature that can securely store information, such as passwords and encryption keys, which can be used to authenticate the platform. It can also be used to store platform measurements that help ensure that the platform remains trustworthy. The TPM v1.2 is supported on Generation 6 ProLiant servers and on select Generation 5 ProLiant servers. The optional TPM v1.2 module can be attached and secured to the system board with a rivet supplied with the module. To prevent possible damage to the TPM module or to the system board, the TPM cannot be removed from the board once it has been installed.

BitLocker is a feature in Windows Server 2008 that works with features in the TPM to provide authenticated system boot and logical disk drive encryption. The TPM logically and physically protects the key used for encryption to safeguard operating system integrity and data. BitLocker-based physical protection is active even when the server is not powered or operating. Therefore, BitLocker protects data if a disk is stolen and mounted on another machine for data mining. BitLocker also protects data if an attacker uses a different operating system or runs a software hacking tool to access a disk.

Enabling and configuring the TPM

IT administrators can use the HP ROM-Based Setup Utility (RBSU) to enable and configure the TPM installed on a ProLiant server. Since the RBSU is embedded in the server's system ROM, users must complete the following steps to access the TPM menu:

1. To start the RBSU, press the **F9** key when prompted during the startup sequence.
2. Select **Server Security**.
3. Select **Trusted Platform Module**.

IMPORTANT

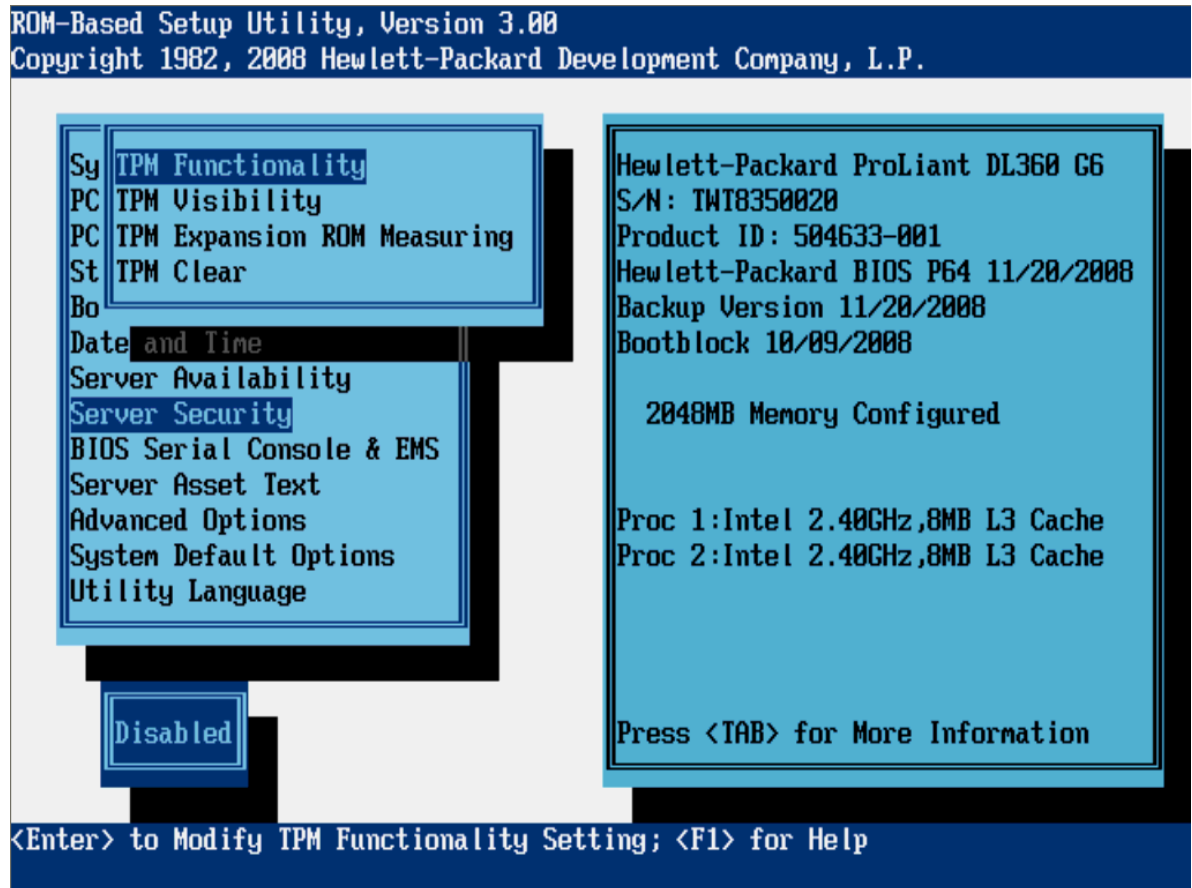
The TPM is a customer-configured option. HP will not configure the TPM as part of the CTO or other pre-installation process and is not liable for maintaining recovery keys or inability to access data. Customers are strongly advised to perform the recommended procedures to back up customer keys and data. Disaster recovery requires use of data created by those procedures. HP is unable to override or bypass the protections provided by BitLocker and the TPM, or to decrypt data protected by BitLocker and the TPM.

The TPM menu identifies user options for configuring the TPM installed on an HP ProLiant server. Figure 1 shows the available options: TPM Functionality, TPM Visibility, TPM Expansion ROM Measuring, and TPM Clear.

NOTE

Figure 1 represents HP ProLiant 200-series and above servers. Menu selections may look slightly different on ProLiant 100-series servers.

Figure 1. RBSU Trusted Platform Module menu



Selecting TPM Functionality provides the ability to enable or disable the TPM and BIOS secure startup. The TPM is fully functional when enabled. Disabling TPM functionality disables the BIOS secure startup but still allows the TPM to be visible to the operating system (OS). The TPM can respond to most commands in this mode, depending on how it was disabled. Selecting Disable may prevent the server from booting to a TPM-aware OS.

The TPM Visibility option can make the TPM invisible to the OS. When the TPM is hidden, BIOS secure startup is disabled, and the TPM does not respond to commands from any software. Hiding the TPM may prevent the server from booting to a TPM-aware OS. TPM Visibility can be set to **Hide** if the TPM is installed but no longer needed. Hiding the TPM is a way to prevent the OS and runtime users from seeing the TPM and attempting to re-enable it.

The TPM expansion ROM measuring option allows the BIOS to measure PCI or PCIe expansion ROM code and store that measurement in the TPM. On subsequent reboots, validation software or operating systems that utilize the measurements stored in the TPM can use this data to detect modifications to PCI or PCIe expansion ROM versions. If the TPM expansion ROM measuring option is enabled and a PCI or PCIe card with an option ROM is inserted, the change will be detected and a password will be required.

The TPM Clear option allows the user to reset the TPM to factory settings, which clears any passwords, keys, or ownership. Clearing the TPM may prevent the server from booting to a TPM-aware OS.

Enabling BitLocker on HP ProLiant servers

For Windows Server 2008, BitLocker uses the TPM to ensure the integrity of the startup sequence and lets IT administrators encrypt both the OS volume and additional data volumes on the same server. BitLocker makes the encrypted volume accessible only if it has not been tampered with and if the encrypted drive is located in the original computer. BitLocker is not installed by default with Windows Server 2008; users can add it from the Server Manager page.

Before installing the OS, IT administrators should enable the TPM and create two disk partitions. BitLocker requires at least two New Technology File System (NTFS) volumes: an OS volume and a system volume. The system volume must be the active partition and must have a capacity of at least 1.5 GB. During the initial OS installation, follow the steps below to enable BitLocker.

To enable BitLocker support after initial OS installation, set the 1.5-GB system partition to **Active** using the Disk Manager, and reboot the system so the server boots from the 1.5-GB partition. Then follow the steps below to enable BitLocker.

1. Add the BitLocker feature from Server Manager and reboot the server.
2. After the OS boots, log in as Administrator, go to Control Panel, click **Security**, and then click **BitLocker Drive Encryption**.
3. If the User Account Control dialog box appears, confirm the action and then click **Continue**. The BitLocker Drive Encryption page appears.
4. Click **Turn On BitLocker** on the OS volume. The following warning appears: *BitLocker encryption might have a performance impact on your server. If the TPM is not initialized, the TPM Security Hardware wizard appears. Follow the directions to initialize the TPM. You must shut down or restart the computer to complete the changes.*
5. On the Save the Recovery Password page, the following options appear:
 - Save the password on a USB drive. This saves the password to a USB flash drive.
 - Save the password in a folder. This saves the password to a folder on a network drive or other location.
 - Print the password. This prints the password.

Use one or more of these options to preserve the recovery password. Select each preferred option and follow the wizard steps to set the location for saving or printing the recovery password.
6. When finished saving the recovery password, click **Next**. The Encrypt the Selected Disk Volume page appears.

IMPORTANT

The recovery password is required in the event the encrypted disk is moved to another computer or changes are made to the

system startup information. This password is so important that HP recommends that the administrator make additional copies of the password and store them in safe places away from the computer to assure access to the data. The recovery password is needed to unlock the encrypted data on the volume if BitLocker enters a locked state. The recovery password is unique to this particular BitLocker encryption. It cannot be used to recover encrypted data from any other BitLocker encryption session.

7. Confirm that the Run BitLocker System check box is selected, and then click **Continue**.
8. Click **Restart Now**. The computer restarts and BitLocker verifies whether the computer is compatible with BitLocker and ready for encryption. If it is not, an error message appears.
9. If the computer is ready for encryption, the Encryption in Progress status bar appears. Monitor the ongoing completion status of the disk volume encryption by dragging the mouse cursor over the BitLocker Drive Encryption icon in the notification area at the bottom of the screen.

When this procedure is complete, the OS volume is encrypted and a recovery password unique to this volume is created. If the TPM ever changes or cannot be accessed, if there are changes to key system files, or if someone tries to start the computer from a product CD or DVD to circumvent the operating system, the computer switches to recovery mode until the recovery password is entered.

CAUTION

When BitLocker is installed and enabled on the server, data access is locked if the administrator fails to follow the proper procedures for any of the following: updating the system or option firmware, replacing the system board, replacing a hard drive, or modifying OS application TPM settings. Data access may also be locked if the TPM is used for other functionality.

BitLocker Drive Preparation Tool

The BitLocker Drive Preparation Tool allows the system administrator to prepare an existing Windows Server 2008 system before enabling BitLocker Drive Encryption. This tool configures and prepares the system and operating system disk volumes after Windows Server 2008 has been installed through any of the standard and supported setup methods. This tool is available at the Microsoft Download Center: <http://www.microsoft.com/downloads/details.aspx?FamilyId=320B9AA9-47E8-44F9-B8D0-4D7D6A75ADD0>.

This tool is an alternative to the manual steps formerly required for partitioning and configuring server storage devices prior to installing an operating system. For specific and advanced configuration needs, such as the ability to determine the size and placement of an OS volume, other methods are described in the Microsoft TechNet library: <http://technet.microsoft.com/en-us/library/cc732774.aspx>.

Windows imaging with ImageX

ImageX is a Windows command-line tool that allows IT administrators to capture disk images for rapid deployment on other computers. When used with Windows image (.wim) format files, ImageX automates much of the BitLocker setup. ImageX requires that all existing data on the hard drive be overwritten. It is typically used to install custom images on computers that have no OS installed or

when data can be overwritten. IT administrators can build one DVD that does all partitioning, installation, and drive letter adjusting automatically.

More information about ImageX is available at this URL: <http://technet.microsoft.com/en-us/library/cc748966.aspx>.

BitLocker recovery process

BitLocker locks the server and enters recovery mode when the USB recovery key or recovery password is not available. This can happen if one of the early boot files is changed or if the TPM is inadvertently cleared or turned off and the computer is subsequently turned off. Either the USB recovery key or the recovery password is required to recover access to the data. Detailed information about the recovery process is available in the Windows BitLocker Drive Encryption Step-by-Step Guide at this URL: <http://go.microsoft.com/fwlink/?LinkID=53779>.

WARNING

HP is not liable for data loss resulting from administrator failure to properly manage keys and passwords.

The BitLocker Repair Tool can be used to help recover data from an encrypted volume if the hard drive has been damaged. It reconstructs critical parts of the drive to recover data. A recovery key or recovery password is required to decrypt the data. The BitLocker Repair Tool is available at <http://support.microsoft.com/kb/928201>.

If an HP ProLiant server with the TPM installed experiences a hardware failure on the TPM or the system board on which the TPM is mounted, both parts must be replaced. The IT administrator should contact the service provider or the HP Global Support Center (GSC) to report the problem. The GSC or the service provider will dispatch a service technician to replace the board and the TPM. When the defective parts are replaced, the IT administrator must reset the recovery password to access the data on the hard drives.

Precautions affecting server maintenance and management

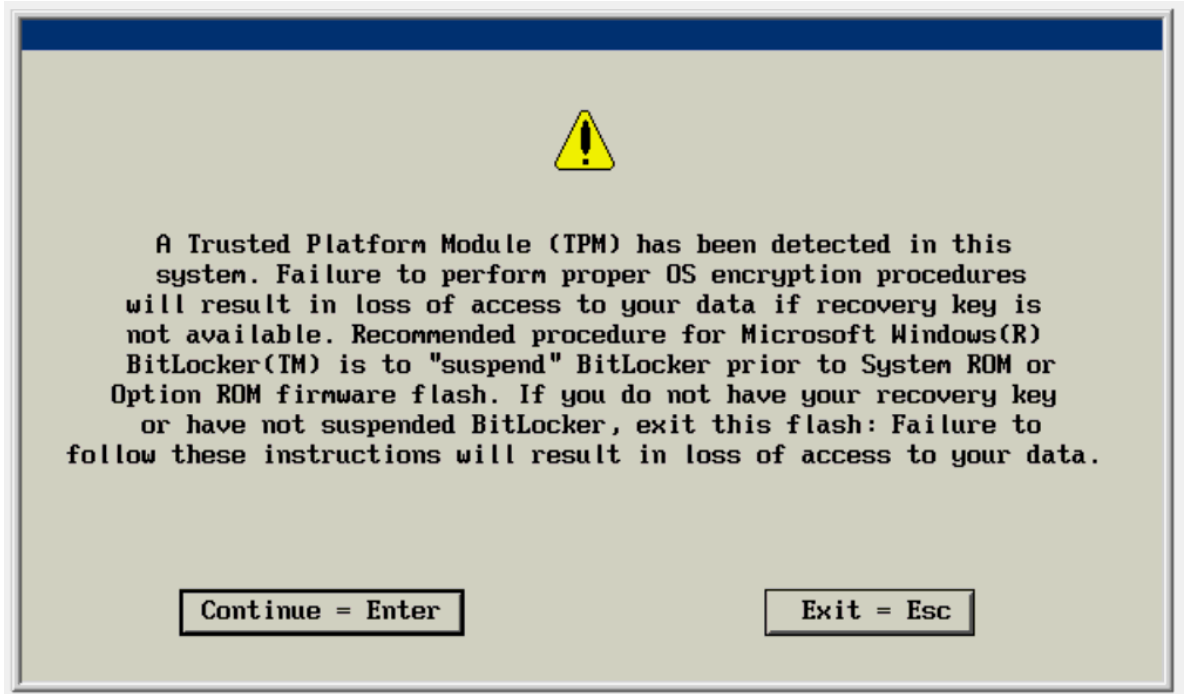
Microsoft recommends temporarily disabling BitLocker prior to updating any system firmware. After the firmware flash is complete, the server should be rebooted and BitLocker can be re-enabled. If BitLocker is enabled with TPM functionality or if TPM Expansion ROM Measuring functionality is turned on, the system will be locked out and the recovery key will be required to recover the system. If the key is not available, all BitLocker-protected volumes will be inaccessible. Some examples of activities that can cause the system to be locked out are listed below:

- Flashing System ROMs
- Flashing Option ROMs (NIC, storage, and so forth)
- Flashing iLO 2
- Installing new PCI devices
- Changing position of hard drives

During the execution of online flash tools, the presence and state of the TPM module will be detected. If the TPM is detected and enabled when a firmware flash is attempted, a pop-up warning message will be displayed. The administrator must acknowledge this warning before the installation can continue. If the administrator is using a command line interface, no pop-up warning message will be given. The installation will be terminated and a log file will be generated.

A warning message is displayed when the system ROM is being updated with System ROMPaq, Windows Online Flash, Linux Online Flash, or HP SUM (Figure 2). The message will also be displayed if TPM functionality or TPM Expansion ROM Measuring are enabled and the IT administrator is flashing iLO 2 firmware, NIC option ROMs, storage option ROMs, or other option ROMs. Updating the option ROM on third party cards or older HP options may not result in a warning message but may initiate the recovery process.

Figure 2. Warning message displayed by the System ROMPaq flashing mechanism



Integrated Lights-Out 2 (iLO 2) is integrated on the motherboard of all 200-series and above HP ProLiant servers and provides remote management capabilities over Ethernet. The iLO 2 v1.70 and later firmware releases support the TPM. The firmware allows system administrators to view the TPM module configuration status. It also displays a warning message about the risk of updating option ROMs when the TPM is installed and TPM Expansion ROM Measuring is enabled. IT administrators can also use Insight Diagnostics to see if the TPM is enabled on the server.

For more information

For additional information, refer to the resources listed below.

Resource description	Web address
BitLocker Drive Preparation Tool	http://support.microsoft.com/kb/933246
BitLocker Repair Tool	http://support.microsoft.com/kb/928201
BitLocker Drive Encryption Technical Overview	http://technet.microsoft.com/en-us/library/cc732774.aspx
BitLocker Drive Encryption Step-by-Step Guide	http://technet.microsoft.com/en-us/library/cc732725.aspx
ImageX Technical Reference	http://technet.microsoft.com/en-us/library/cc748966.aspx

Call to action

Send comments about this paper to TechCom@HP.com.

© 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

BitLocker is a trademark of Microsoft Corporation.