7.Demostrate how to use the bitlocker feature. Provide some steps and screenshots (or video).

Installing BitLocker on Windows Server 2008

As we already mentioned, BitLocker is a Feature of Windows Server 2008 and is not installed by default. To install BitLocker you use Server Manager as you would with all other roles and features. Be aware that a restart is required after installation. You can also install BitLocker from the command line by typing ServerManagerCmd -install BitLocker --restart.

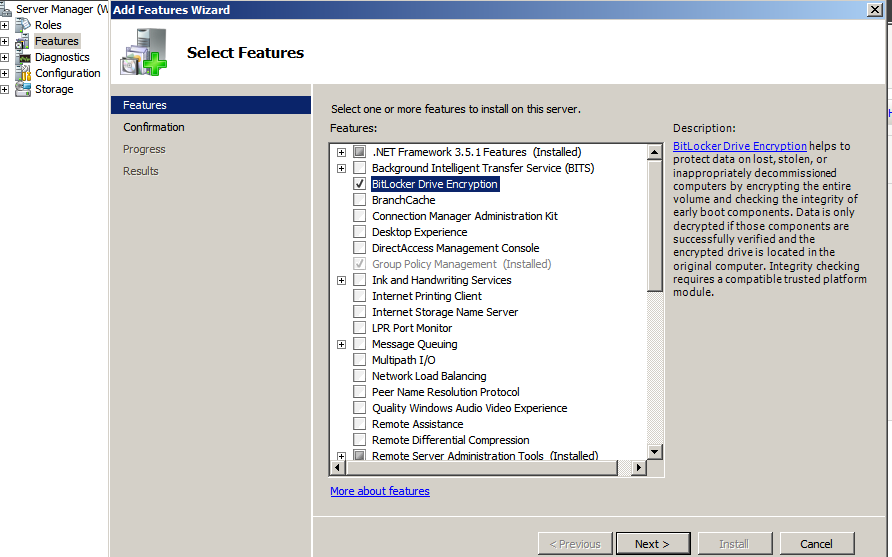
Here are the steps to follow to install Bitlocker on Windows Server 2008.

1. Log on as an administrator.

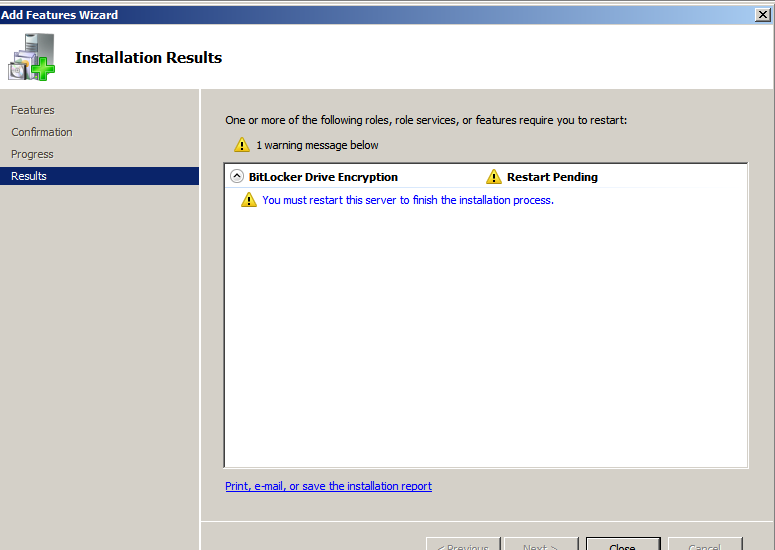
2. Click Start | Administrative Tools | Server Manager.

3. Scroll down to Feature Summary; click Add Features.

4. On the Select Features page, choose BitLocker Drive Encryption and then click Next.



5. On the Confirm Installation Selectionspage, click Install.   
6. When installation is complete, click Close.   
7. In the Do you want to restartWindow click Yes.

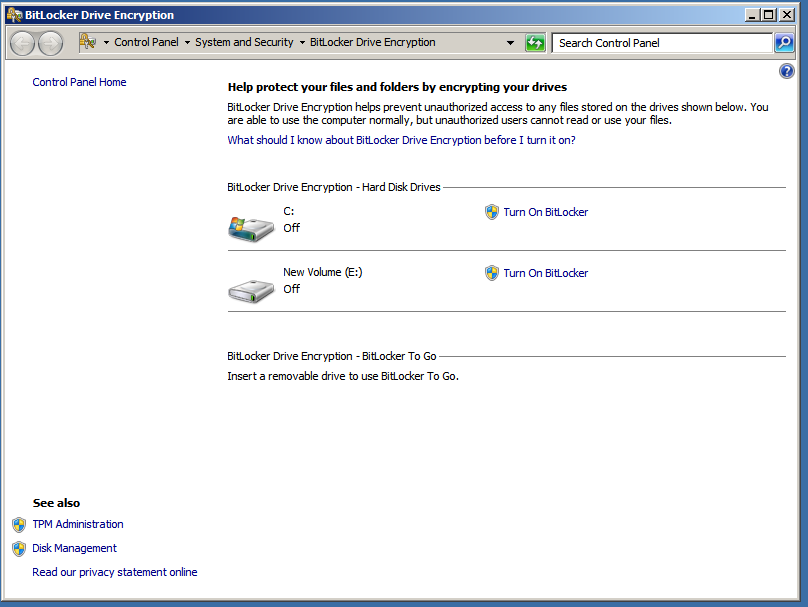


Turning on and Configuring BitLocker

After installing the BitLocker Feature on your Server and rebooting the system, you need to turn on BitLocker via a Control Panel applet. Make sure you are logged on as an administrator on the system and you have decided where to store the recovery password. In case your computer does not have a Trusted Platform Module (TPM) or the TPM is not supported, you will receive a warning.

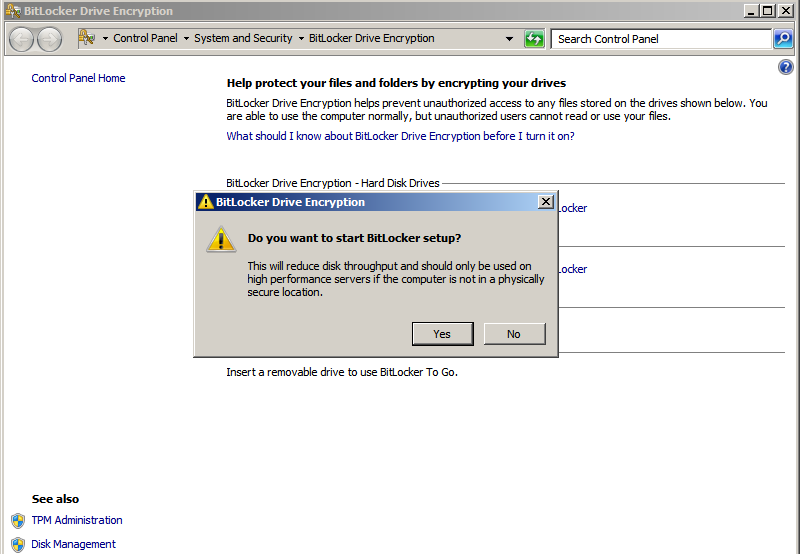
Here are the steps to follow for turning on BitLocker.

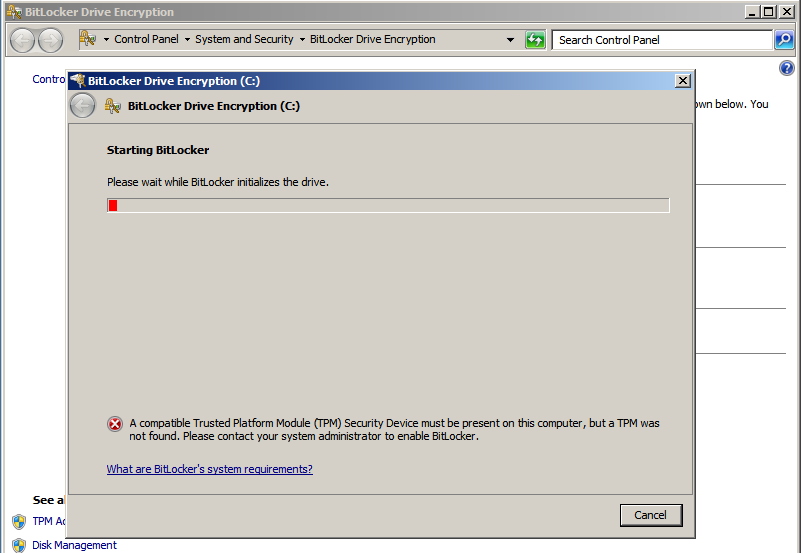
1. Log on as an administrator.   
2. Click Start, click Control Panel, and then click BitLocker Drive Encryption.   
3. On the BitLocker Drive Encryption page, click Turn On BitLocker on the operating system volume.

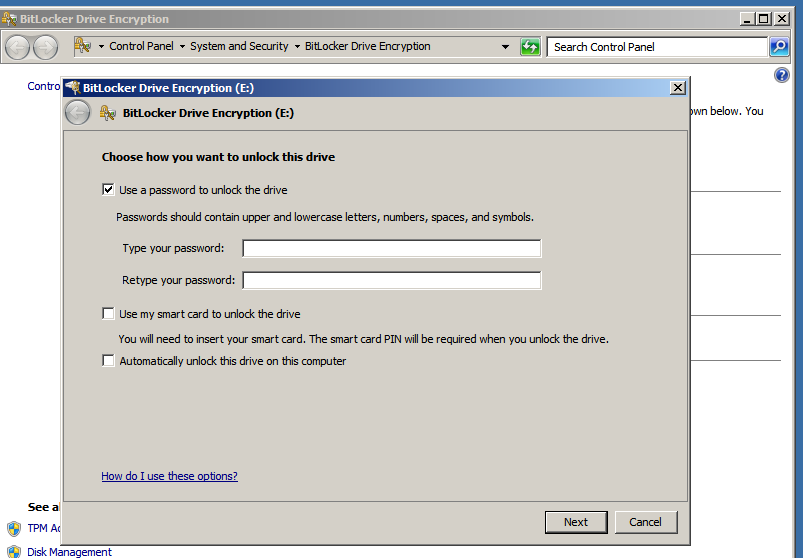


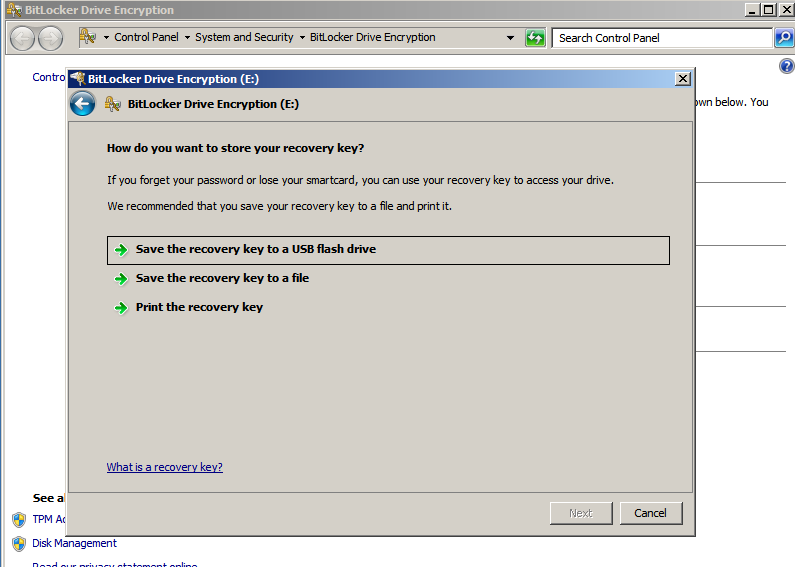
4. On the BitLocker Drive Encryption Platform Check dialog box click Continue with BitLocker Drive Encryption.   
5. If your TPM is not initialized already, you will see the Initialize TPM Security Hardware screen.

6. On the Save the recovery password page, click Save the password on a USB drive.   
7. On the Save a Recovery Password to a USB Drive box, select your USB drive and click Save.   
8. On the Encrypt the selected disk volume page, confirm that the Run BitLocker System Check checkbox is selected, and then click Continue.   
9. Confirm that you want to reboot.

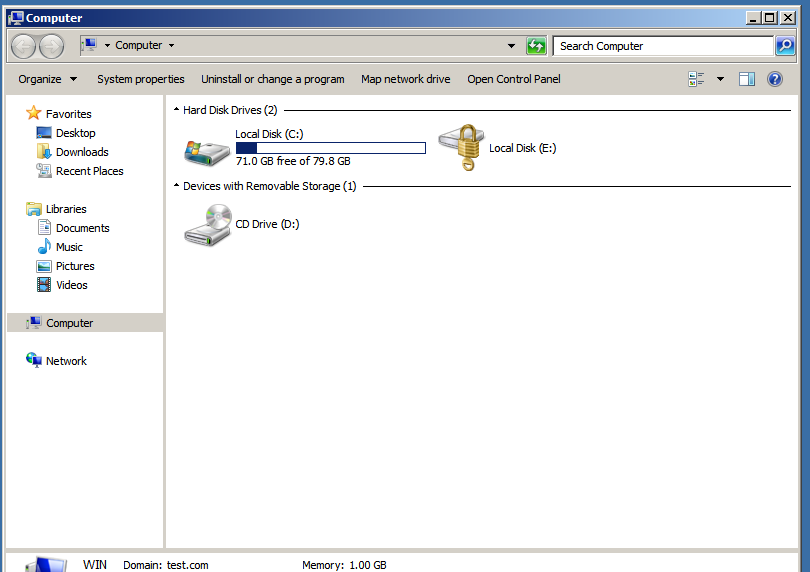








During the reboot phase, BitLocker verifies the system and makes sure it is ready for encryption. After rebooting the system, you should log back on to the system and verify that the Encryption inProgress status bar is displayed in the BitLocker Control Panel applet. In case your system cannot be enabled for BitLocker, an error message pops up during logon.



Disabling BitLocker Drive Encryption

BitLocker Drive Encryption may be disabled on either a temporary or permanent basis. To temporarily turn off encryption open the BitLocker control panel (*Start -> Control Panel -> Security -> BitLocker Drive Encryption*) and select *Turn off BitLocker Drive Encryption* under the desired volume and select *Disable BitLocker Drive Encryption* in the resulting screen.

To turn off BitLocker and decrypt a system volume repeat the above steps, selecting *Decrypt the volume* when asked to specify the level of decryption.

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1339.pdf

http://technet.microsoft.com/en-us/library/cc731549%28v=ws.10%29.aspx

http://technet.microsoft.com/en-us/library/cc732774.aspx

http://blogs.technet.com/b/uspartner\_ts2team/archive/2010/03/17/what-is-bitlocker-what-does-it-do-what-does-it-not-do.aspx