Bitlocker Setup without TPM

To use BitLocker on a the Slate 8 without a TPM, you must change the default behavior of the BitLocker setup wizard by using Group Policy editor, or configure BitLocker by using a script. When BitLocker is used without a TPM, the required encryption keys are stored on a USB flash drive that must be presented to unlock the data stored on a volume. On computers and the models of Slate 8 without a compatible TPM chipset, BitLocker can provide encryption, but not the added security of locking keys with the TPM. In this case, the user is required to create a startup key that is stored on a USB flash drive. How does this all work on the Samsung Slate 8? Read on...

The real key Bitlocker working on the Samsun Slate 8 is the setting in the bios. I wanted to salvage the USB port and write the key to the MicroSD card. Since you cannot boot off a MicroSD this was not an option. So I purchased one of those small USB devices with the smallest size I could find. I still could not get the Slate to recognize this device until I read another article on how to set the bios on the Slate 8 to recognize legacy USB devices. I changed the setting and boot priority and everything came together. Now the only issue I have will be our corporate environment. We limit the use of non-secure USB devices. Since the slate is a pilot I may have to ask security to bend the rules. Or ask my manager to purchase the upgraded Samsung that supports the security chip.

These instuctions below are right off the MS$ site and you can find these most anywhere. In my case the most important piece of this was the bios setting. Good luck...

To turn on BitLocker Drive Encryption on a computer without a compatible TPM

- Click Start, type gpedit.msc in the

- Start Search box, and then press ENTER. If the User Account Control dialog box appears, verify that the proposed action is what you requested, and then click Continue. For more information, see Additional Resources later in this document.

- In the Group Policy Object Editor console tree, click Local Computer Policy, click Administrative Templates, click Windows Components, and then double-click BitLocker Drive Encryption.
- Double-click the setting Control Panel Setup: Enable Advanced Startup Options.
- The Control Panel Setup: Enable Advanced Startup Options dialog box appears. Select the Enabled option, select the Allow BitLocker without a compatible TPM check box, and then click OK.

- You have changed the policy setting so that you can use a startup key instead of a TPM.

- Close the Group Policy Object Editor. To force Group Policy to apply immediately, you can click Start, type gpupdate.exe /force in the Start Searchbox, and then press ENTER. Wait for the process to finish.
- Click Start, click Control Panel, click Security, and then click BitLocker Drive Encryption. If the User Account Control message appears, verify that the proposed action is what you requested, and then click Continue.

- For more information, see Additional Resources later in this document.
- On the BitLocker Drive Encryption page, click Turn On BitLocker on the operating system volume.
- On the Set BitLocker Startup Preferences page, select the Require Startup USB Key at every startup option. This is the only option available for non-TPM configurations. This key must be inserted each time before you start the computer.
- Insert your USB flash drive in the computer, if it is not already there.
- On the Save your Startup Key page, choose the location of your USB flash drive, and then click Save. On the Save the recovery password page, you will see the following options:

1. Save the password on a USB drive. Saves the password to a USB flash drive.
2. Save the password in a folder. Saves the password to a network drive or other location.
3. Print the password. Prints the password. Use one or more of these options to preserve the recovery password.

For each option, select the option and follow the wizard steps to set the location for saving or printing the recovery password. When you have finished saving the recovery password, click Next.

Important

The recovery password will be required in the event the encrypted drive must be moved to another computer, or changes are made to the system startup information. This password is so important that it is recommended that you make additional copies of the password stored in safe places to assure you access to your data. You will need your recovery password to unlock the encrypted data on the volume if BitLocker enters a locked state (see Scenario 4: Recovering Data Protected by BitLocker Drive Encryption). This recovery password is unique to this particular BitLocker encryption. You cannot use it to recover encrypted data from any other BitLocker encryption session.

Important

Store recovery passwords apart from the computer for maximum security.

- On the Encrypt the selected disk volume page, confirm that the Run BitLocker System Check check box is selected, and then click Continue.
- Confirm that you want to restart the computer by clicking Restart Now.
- The computer restarts and BitLocker ensures that the computer is BitLocker-compatible and ready for encryption. If it is not, you will see an error message alerting you to the problem before encryption starts. If it is ready for encryption, the Encryption in Progress status bar is displayed. You can monitor the ongoing completion status of the disk volume encryption by dragging your mouse cursor over the BitLocker Drive Encryption icon in the tool bar at the bottom of your screen or clicking on the Encryption balloon. By completing this procedure, you have encrypted the operating system volume and created a recovery password unique to that volume.
- The next time you turn your computer on, the USB flash drive must be plugged into a USB port on the computer. If it is not, you will not be able to access data on your encrypted volume. Store the startup key away from the computer to increase security. If you do not have the USB flash drive containing your startup key, then to access the data, you will need to use recovery mode and supply the recovery password.