Enabling Hardware Encryption on a Samsung 980 PRO NVMe SSD with Windows 11 using BitLocker

Author: Rob Collins
Last Updated: 26 April 2023

System Specs

SSD: 1TB Samsung 980 PRO M.2 NVMe
Mobo: MSI MAG B660M MORTAR DDR4
OS: Windows 11 Pro

Goal

Encrypt the Windows C: drive using Bitlocker on Windows 11, utilising the hardware encryption capabilities of the Samsung 980 PRO SSD. Using hardware encryption instead of software encryption reduces the performance overhead on the CPU and provides additional security benefits.

Pre-requisites

1. 3 x blank USB drives or external SSDs, at least 8GB capacity each.
    a. A USB drive (or preferably a fast external SSD) for a Windows To Go installation. This is basically running a full version of Windows from an external drive, so you want a drive with fast random I/O speeds. I used an NVMe SSD in an external USB drive enclosure.
    b. A second USB drive for a standard Windows 11 installation image.
    c. A third USB drive for the Samsung Magician Secure Erase bootable USB. You can use any slow, old, or low capacity USB drive for this.

Acknowledgements

My guide is based on this excellent guide by Frederik here:

- https://blog.odenthal.cc/how-to-enable-bitlocker-hw-encryption-with-modern-ssds-e-g-samsung-980-pro/

Detailed Instructions

1. Download the Windows 11 installation ISO from Microsoft. You can use Microsoft's "Media Creation Tool" to do this.
2. Download the Rufus app, which creates bootable USB drives for installing Windows 11.
3. Use Rufus to create a standard Windows 11 USB installation drive. Let's call this "USB Drive 1".
4. Use Rufus to create a "Windows 11 To Go" installation on a fast USB drive or external SSD. Let's call this "USB Drive 2". Make sure you specify the option in Rufus to ALLOW access to internal drives. Note that this drive will take longer to create than a standard Windows install.
5. If not done already, physically install the Samsung 980 PRO SSD into your motherboard.

6. If not done already, install a standard version of Windows 11 on your internal Samsung SSD in the usual way.
7. Install Samsung Magician app.
    a. Look in the “Data Management” section, for “Encrypted Drive”. It will probably say “Disabled” in red.
    b. Toggle the switch next to Encrypted Drive. It should now say “Ready to enable” in green.
8. Restart your PC and enter your computer’s UEFI BIOS.
    a. Ensure your motherboard is set to boot in UEFI mode (CSM disabled).
    b. Disable “Secure Boot”. It prevents the Samsung Magician bootable USB from working later on.
    c. Ensure that TPM is Enabled. This is required for BitLocker to work.
9. Boot your computer from USB Drive 2, containing the Windows To Go image you created earlier.
10. Insert your 3rd USB stick into your PC. Let’s call this USB Drive 3. This will be used for the Secure Erase utility.
11. Install Samsung Magician into Windows To Go.
12. Go to the “Secure Erase” section. Select your USB Drive C. Choose the “UEFI BIOS” option and then Start. This will create the bootable Secure Erase USB drive.
13. NOTE: You have to do the above when you’re booted into your Windows To Go USB drive. Samsung Magician will fail with an error if you try to create the Secure Erase drive when you’re booted into Windows on an internal drive. Don’t ask me why!
14. Shutdown your PC and disconnect USB Drive 2 (the one with the Windows To Go image).
15. Boot your PC from USB Drive 3, the one with the Samsung Secure Erase utility on it.
16. NOTE: If you still have Secure Boot enabled in your UEFI BIOS, the Secure Erase utility won’t be able to start.
17. Follow the on-screen instructions to perform a Secure Erase of your internal Samsung 980 PRO SSD. This will wipe all data on the drive.
18. Shutdown your PC and disconnect USB Drive 3 (the Secure Erase one). Reconnect USB Drive 2 (Windows To Go).
19. Boot your PC and enter the BIOS.
20. [Optional] Re-enable Secure Boot if desired. It enhances security.
21. Look under the Security section in the BIOS for an option called “Disable Block SID”. It will probably be set to Disabled. Set it to Enabled.
22. NOTE 1: On most motherboards, setting this option to Enabled only lasts for the next boot. After that, it’ll go back to Disabled automatically.
23. NOTE 2: Not all motherboard BIOS have an option called “Disable Block SID”. Mine doesn’t (MSI MAG B660M MORTAR). But don’t worry, you can set this option in Windows instead using PowerShell.
    a. Boot into Windows To Go using USB Drive 2.
    b. Open a PowerShell prompt with Admin rights.
    c. Type: $tpm = gwmi -n root\cimv2\security\microsofttpm win32_tpm
    d. Type: $tpm.SetPhysicalPresenceRequest(97)
    e. You should get an output in PowerShell to indicate this has worked successfully.
    f. On the next boot, the POST screen will alert you that "a configuration change was requested issuing a Block SID command".

24. Now you need to plug in your standard Windows installation stick (USB Drive 1) and remove the Windows To Go stick (USB Drive 2).
25. Boot from USB Drive 1 and install Windows to your internal Samsung SSD.
26. Once Windows is fully installed, remove USB Drive 1 from your computer.
27. [Optional] Install your usual drivers, such as Intel chipset drivers.
28. Install Samsung Magician and check the Encrypted Drive settings. It should now be set to “Enabled”.
29. We now need to force Bitlocker to use hardware encryption. We do this using Group Policy. Click Start and type Edit Group Policy to open the Local Group Policy Editor.
30. In the left-hand pane, navigate to Computer Configuration / Administrative Templates / Windows Components / Bitlocker Drive Encryption / Operating System Drives.
31. In the right-hand pane, Find the policy called “Configure use of hardware-based encryption for operating system drives” and double-click on it.
32. Set the policy to Enabled. Also ensure the following option is disabled: “Use BitLocker software-based encryption when hardware encryption is not enabled”.
33. Reboot the PC to ensure the Group Policy settings take effect.
34. In Windows, click Start and type Bitlocker. Start the BitLocker encryption on your internal C: Drive.
35. NOTE: For me, within a few seconds this encryption process failed with an error and then my PC bluescreened. Thanks Microsoft! To work around this, I enabled BitLocker from the command line:
    a. Reboot into Windows
    b. Open a Command Prompt (not PowerShell) with Admin rights
    c. Type: manage-bde -status
    d. Type: manage-bde -on c:
    e. The drive will now encrypt, which only takes a few seconds.
    f. To check it worked properly, again type: manage-bde -status
    g. Check the output under “Encryption method”, it should say “Hardware Encryption”
36. Voila! Your C: drive (Samsung 980 PRO) should now be hardware encrypted! That was easy, wasn’t it!!