BitLocker - TPM

These instructions are for Bitlocker with Trusted Platform Module (TPM)

Step by Step guide

When a computer has a TPM chip, and BitLocker is enabled, the user is not required to enter a pre-OS password to authenticate and unlock the disk; instead, this occurs automatically using the encryption key from the TPM chip. Using the process below, the computer's recovery key will be securely transferred to ITS's Microsoft BitLocker Administration & Management server. If we need to obtain a recovery key, we must call the ITS Helpdesk with the user present to obtain it.

If you encounter problems with the TPM chip, see Troubleshooting BitLocker with TPM

1. Verify the computer has a TPM chip and verify in the BIOS that it is On and Active.
2. Ensure the computer is on the SOM domain.
3. Install MBAMClient on the user's computer.
   1. You can retrieve it from \polaris\Software\MDOP
   2. Use all default options during installation.
4. Create a sub-task for the SOM IT Systems team to move the computer object to be encrypted to the following organizational unit. Be sure to provide the exact computer name. Double check this!

   OU
   OU=SOM MBAM Workstations,OU=SOM Workstations,OU=SOM Global Computers,DC=som,DC=yale,DC=edu

5. Once systems has completed the sub-task from step 4, while on the Yale network, restart the user's computer. Within 5 minutes after logon with network connectivity, you should be prompted to begin encryption. Click "Start"

   If you do not see the prompt after 5 minutes, see: Troubleshooting BitLocker with TPM

   BitLocker drive encryption is required to help secure the data on drive C:

   • You can work as usual while this runs in the background.
   • Encryption can take several hours, depending on the disk size.
   • We will require some information from you, which will take only a few minutes.
   • A computer restart will be required.

   To begin, click Start.
   To delay, click Postpone. (We will remind you later.)
6. At this point, the screens you see can differ if the TPM chip is not enabled, not activated, or other requirements are not met. Please read and understand each screen carefully before proceeding. The expected screen will ask you to restart your computer, do so.

7. After logon, the system should begin encrypting, you may see the screen below. The user may use his or her computer while this proceeds.
If you do not see the screen below you can check encryption status in two ways:
Control Panel > System and Security > BitLocker Encryption Options
This should report either “Encrypting” or “Encryption On”

OR

Start cmd.exe with elevated permissions. Type `manage-bde - status` then hit enter. It should return either a percentage complete or “Fully Encrypted”
8. If you see the progress window, you will see completion message, click Exit.

- Your password is confidential. Keep your password in a safe place away from your computer.
- If you lose your password, contact your company help desk.
- To reset your password, open Control Panel, select System and Security, and then click BitLocker Encryption Options.
9. Launch an elevated command prompt and type: \texttt{manage-bde \textasciitilde status} then hit enter. The result should show that the disk(s) is Fully Encrypted at 100%.

![Command Prompt Output]

Software Updates

Software can be loaded by first having the user login to the computer using their credentials and then using administrative privileges to install the software.