Manually Encrypting a Windows computer with MBAM 2.5 SP1

Below are the requirements for MBAM 2.5 to function properly on a Windows system and information about how to perform the process.

If the computer(s) are in the Managed Workstation service, these steps are all handled automatically.

- The group policy "MW_MBAM_Policy" needs to be linked (or a policy created with the required settings) to add the required MBAM information to the Windows registry (e.g. the server name, the cipher strength (AES-256), etc.). If your computer(s) are in the Managed Workstation OU, they already have this policy linked.
- The MBAM 2.5 client needs to be installed: \configmgr_dsl.grove.ad.uconn.edu\MBAM\2.5 Choose the installer for the architecture of your system (e.g., x86/x64), as well as the servicing update for May 2019. Choose MBAM2.5_Client_x64_KB4505175.exe or MBAM2.5_Client_x86_KB4505175.exe to patch a bug introduced by Windows 10 1903.
- A TPM (Trusted Platform Module) needs to be present in BIOS, enabled, and ownership taken by MBAM.
- The disk also needs to have a Bitlocker partition (Windows 10 is normally ready out of box). You can use the following tool in Windows to create the partition: Open an elevated command window and run "BdeHdCfg.exe -target default". It will respond by creating the partition or notifying you that the computer's hard drive is already properly configured.
- Once all these requirements are met, MBAM will start encryption within 30 minutes. Note: You can force the process immediately by running the following file: C:\Program Files\Microsoft\MDOP MBAM\MBAMClientUI.exe
  - The encryption key is escrowed to the MBAM 2.5 server, which technicians can access at with NetIDadmin credentials: https://mbam-2-primary.grove.ad.uconn.edu/Helpdesk/
  - The reporting node also allows you to check machine compliance, last check-in, etc.
  - When recovery key(s) are used, they are changed after MBAM client does its check in.
- Individual customers can access their recovery key at the self-help portal: https://bitlocker.uconn.edu/selfservice/. Access to a key is determined by logon to the computer. If a customer has signed on to Windows and MBAM has registered it (on client sync), then that customer can request the recovery key from the self-help portal.
- If a computer is currently encrypted with standalone Bitlocker, it will need to de-crypt and re-encrypt with AES-256 for key escrow and to register as compliant in the console.

Related Articles

- Manually Encrypting a Windows computer with MBAM 2.5 SP1