Installing MBAM 2.5 May 2019 Hotfix & Confirming Encryption Key in MBAM

The Microsoft Windows 10 1903 release broke the Microsoft Bitlocker Administration and Monitoring (MBAM) agent. Below are instructions on how install the hotfix.

If your computers are in the Managed Workstation service, they will be patched automatically.

1. **Install the Hotfix (command line options below)**
   - “MBAM2.5_Client_x64_KB4505175.exe /qn /AcceptEula=Yes”
   - “MBAM2.5_Client_x86_KB4505175.exe /qn /AcceptEula=Yes”

2. **Force a MBAM patched computer to escrow its recovery key to MBAM**
   - PowerShell script located at: `\configmgr_dsl.grove.ad.uconn.edu\MBAM\2.5\configmgr.dsl.grove.ad.uconn.edu\MBAM\2.5`
   - Script must be run with argument provided

   ```
   ```

   Script creates a file “MBAMKickSuccess.txt” at C:\ as a detection method to verify successfully execution

3. **Confirming Recovery Key has been created and sent to MBAM database**
   - On a computer, obtain the challenge code by opening an elevated command or PowerShell prompt and running the following: C:\windows\system32\manage-bde.exe -protectors c: -get
   - This will return one of the following:
     a. **Numerical Password ID & Password**
        i. The first 8 digits of the "ID" are the challenge code (what a customer would be presented in Bitlocker Recovery Mode)
        ii. Password: is the 48 digit recovery key

   ```
   C:\WINDOWS\system32> .\manage-bde.exe -protectors c: -get
   Bitlocker Drive Encryption: Configuration Tool version 10.6.1713
   Copyright (C) 2013 Microsoft Corporation. All rights reserved.
   Volume C: [W indows]
   All Key Protectors
   Numerical Password:
   ID: \{5C7A831B-A871-4B15-94A0-E928CF63F0A5\}
   Password:
   811452-620456-304573-663256-664953-668256-4682372-236423
   TPM:
   ID: \{1A8AFCF9-4371-40F3-BB43-341761F110C0\}
   PCR Validation Profile:
   0, 2, 4, 11
   ```

   b. **There is no Numerical Password displayed, only TPM information**
      i. This means the computer is encrypted but not sending a recovery key to the MBAM database. Ensure all requirements are met and the hotfix installed. Run the PowerShell script "Invoke-MbamClientDeployment.ps1" to force key escrow and then re-run the manage-bde command.

   ```
   C:\Windows\system32> .\manage-bde.exe -protectors c: -get
   Bitlocker Drive Encryption: Configuration Tool version 10.6.1713
   Copyright (C) 2013 Microsoft Corporation. All rights reserved.
   Volume C: [W indows]
   All Key Protectors
   TPM:
   ID: \{90E437A-0925-4A51-B315-D868704B849A\}
   PCR Validation Profile:
   7, 11
   ```
c. No key protectors found
   i. Computer is not encrypted. Ensure that all requirements are met, the hot fix installed, and ensure encryption starts.

4. Accessing the recovery key on the MBAM server
   a. To test that the recovery key is present in the MBAM database as a technician, visit https://mbam-2-primary.grove.ad.uconn.edu/Helpdesk and logon with your NetIDadmin password.
      Note: If you do not have access, please put in a request.
   b. From the left-hand pane, choose “Drive Recovery.”
   c. In the right-hand pane, in the Key ID field, type the first 8 digits of the Numerical ID you obtained (example in the screenshot earlier is 5C7AB31B). Specify a reason for the drive unlock (this is a required field). Press “Submit” and the recovery key will appear in the console.

Related Articles

- Manually Encrypting a Windows computer with MBAM 2.5 SP1