

ESET Tech Center

Knowledgebase > ESET Endpoint Encryption > Resolve error 0xC00B004F—The disk specified is locked in ESET Endpoint Encryption

Resolve error 0xC00B004F—The disk specified is locked in ESET Endpoint Encryption

Steef | ESET Nederland - 2021-05-19 - Comments (0) - ESET Endpoint Encryption

Issue



ESET Endpoint Encryption (EEE) Client and EEE Server are separate products from ESET Full Disk Encryption (EFDE)

The article below applies only to the EEE Client or EEE Server and not EFDE. Visit [What's new in ESET Full Disk Encryption](#) to view EFDE content.

- "The disk specified is locked (0xC00B004F)" error message appears when SafeStart fails after an attempt to OPAL encrypt a system

Details

Windows and other software can automatically configure drives and take ownership of the drive. If a drive is already owned by another piece of software on the system, ESET Endpoint Encryption cannot configure the drive and take ownership of it when encryption is trying to start.

Solution

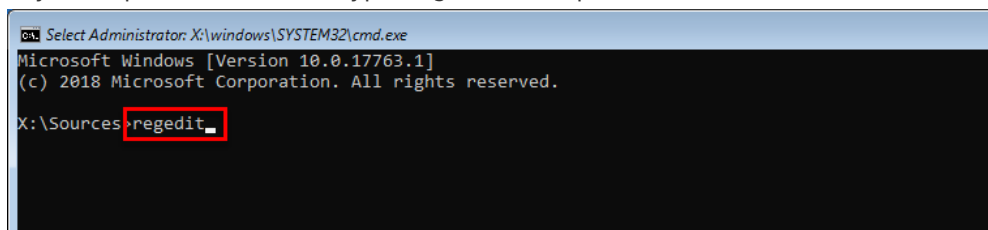


Performing a PSID revert

PSID revert process will erase all data on the disk and is irreversible. If Windows is accessible, ensure you back up all important data from the disk before performing a PSID revert.

To unlock the drive, you need to [perform a PSID revert](#). After the PSID revert, reinstall Windows. To stop Windows automatically locking the drive, perform the following steps in the Windows setup process:

1. Boot from the installation disk/USB flash drive with Windows setup. Wait for the first setup screen.
2. Open **Command Prompt** window and Launch **Registry Editor**. To do this, on your keyboard press **Shift+F10**, type **regedit**, and press **Enter**.

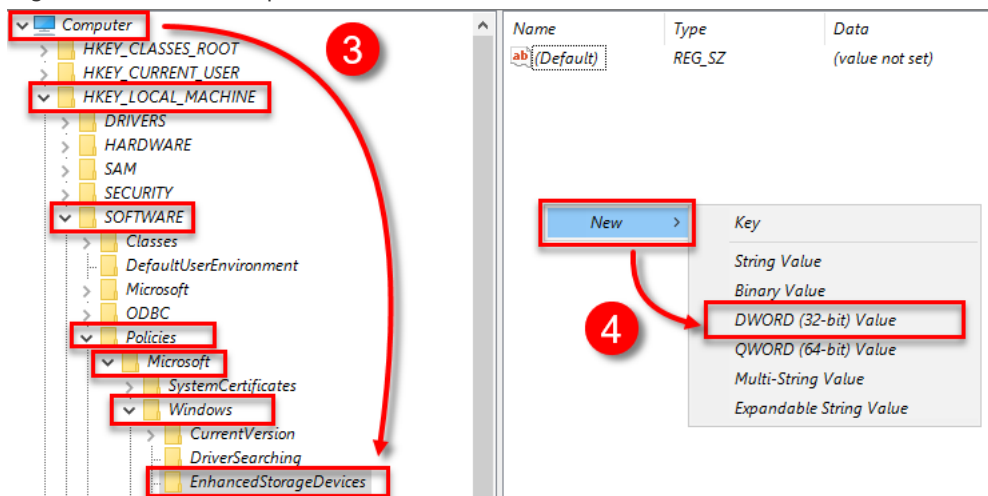


```
cmd: Select Administrator: X:\windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.17763.1]
(c) 2018 Microsoft Corporation. All rights reserved.

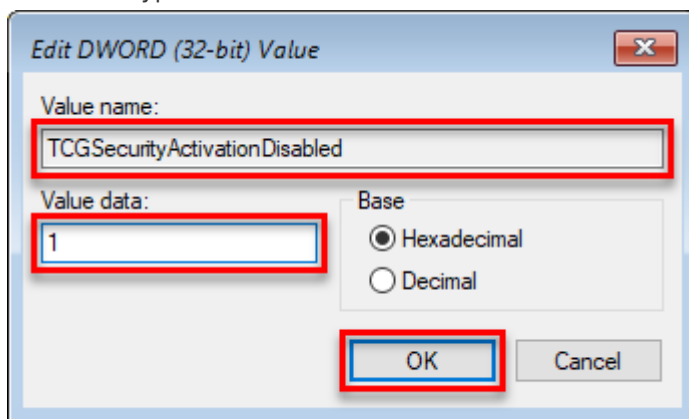
X:\Sources>regedit
```

3. Navigate to the registry path:
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EnhancedStorageDevices.

4. Right-click the blank space and click **New → DWORD (32-bit) Value**.



5. In the **Value name** box, type TCGSecurityActivationDisabled. In the **Value data** box, type 1 and click **OK**.



6. Proceed with the Windows installation process as normal.

Alternatively, you can set up an unattended file that disables this feature on Windows installation. Read more in Microsoft Documentation about [TCGSecurityActivationDisabled](#) and [DisableEncryptedDiskProvisioning](#).