MECM - SCCM - Updating TPM Validation Profile for BitLocker

Q: Why does BitLocker keep triggering?

Answer

BitLocker occasionally triggers a recovery scenario when you're not expecting it. This is often due to changes in the hardware configuration. Microsoft uses a set of criteria made up of PCRs (Platform Configuration Registers). The state of the hardware configuration at the time of encryption is used to create a baseline for BitLocker. If the hardware changes at anytime in the future, Windows will assume malicious hardware tampering such as a key logger. While this is a possible scenario, the far more likely scenario is simply innocuous hardware changes.

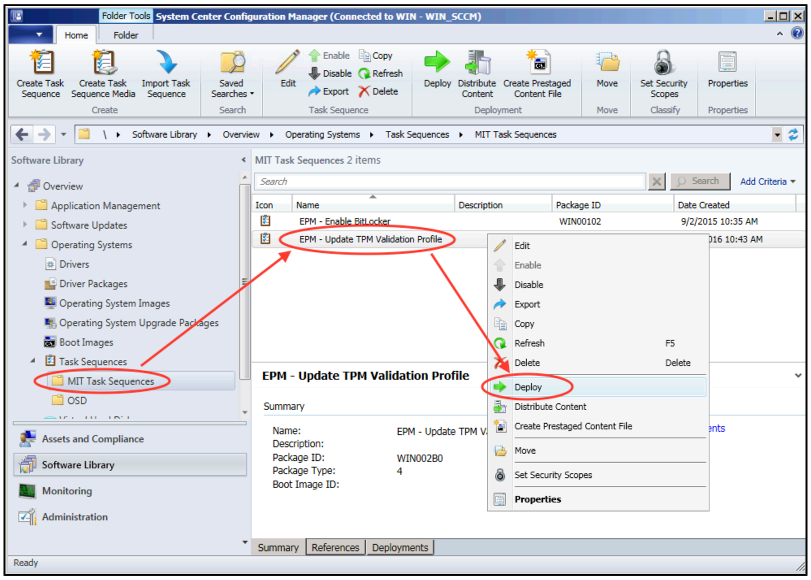
For instance, enabling BitLocker while using the built-in video card and then later switching to a discrete video card will cause BIOS to disable the built-in video hardware. Windows will detect the missing video card as a hardware change and trigger BitLocker. Leaving a bootable USB drive plugged into a USB port and then rebooting can change the available boot devices and trigger BitLocker recovery. Also, using a Thunderbolt dock with a computer can be detected as adding hardware and can trigger BitLocker recovery.

In order eliminate these BitLocker recovery triggers, we've made some changes to Microsoft's default TPM validation profile (set of PCRs). We've removed PCRs 0 and 2 that deal with these types of hardware changes. This change is implemented via GPO at the domain level and is also implemented via EPM Lite Touch so it'll apply to both domain and non-domain machines.

All computers in the domain that have enabled BitLocker after August 21st, 2016 are encrypted using the modified TPM validation profile. Those enabled prior to this date likely have the default Microsoft TPM validation profile. In order to fix older machines to use the updated TPM validation profile you'll need to suspend BitLocker (you don't have to decrypt), run a `gpudpate` command, and then resume BitLocker. We have created a task sequence in SCCM to automatically do these steps for you.

Deploying the TPM Validation Profile Fix Task Sequence

You'll find the task sequence to fix the TPM validation profile located at **Software Library > Operating Systems > Task Sequences > MIT Task Sequences > EPM - Update TPM Validation Profile**. Deploy the task sequence to your target collection. You'll want to create a collection based on the query called "MDOP MBAM Installed" located under **Queries > MIT Queries**. The task sequence takes about 10 seconds to run and is transparent to end users.



Icon	Name	Description	Package ID	Date Created
	EPM - Enable BitLocker		WIN00102	9/2/2015 10:35 AM
	EPM - Update TPM Validation Profile			016 10:43 AM

EPM - Update TPM Validation Profile

Summary

Name:	EPM - Update TPM V
Description:	
Package ID:	WIN002B0
Package Type:	4
Boot Image ID:	

See Also

- Microsoft Endpoint Configuration Manager (MECM) Landing Page