Windows 11 adds a policy to exclude USB from BitLocker encryption

Microsoft has just released another build for Windows 11 with a series of changes, improvements and bug fixes. This build number 22579 has now been pushed to the Dev Channel for Insider Preview users.

However, the most striking thing about this build is a new policy that allows Windows admins to exclude USB drives from BitLocker encryption.

"This will prevent the problem of automatic or random storage encryption being built into specialized equipment such as camcorders, recorders, conference systems, medical equipment.", Windows Insider team shared.

"When this policy is enabled, you will not be able to encrypt memory that is on the exclusion list, and you will not receive an encryption prompt when you connect it to a device while the "Deny" policy write permission to removable drives not protected by BitLocker" is enabled on it".

Currently, the new policy can only be configured by IT admins via mobile device manager (MDM) and custom configured Windows clients using the OMA-URI (Open Mobile Alliance Uniform Resource) setting. Indentifiers).

To perform hardware removal from BitLocker, the IT admin will have to collect the hardware ID and configure the BitLocker Exclusion list Policy in Intune.

Microsoft wants Insider users to try out the new policy and then respond to them with issues (if any) through the Feedback Hub.

The new build also comes with a bunch of changes and improvements to the Start menu and Started app including the ability to name application folders in the Start menu and site suggestions in the Get Started app that can be pinned to. taskbar.