ESET Tech Center

Acer Laptop Full Disk Encryption compatibility

Anish | ESET Nederland - 2018-02-12 - Comments (0) - ESET Endpoint Encryption

When starting Full Disk Encryption on an Acer machine you may find that the DESlock+ Safe Start process is unable to complete and reports that a problem was detected.

In order to use DESlock+ Full Disk Encryption with GPT partitioned disks the system must be configured to use UEFI boot mode.

Some Acer systems come configured from the factory to use Legacy boot mode. This is in order to allow downgrades from Windows 8 to be performed. This is detailed in the Windows 8 Disclaimer section on the Acer website:

"*To enable downgrade to Windows 7 on this system the BIOS settings on this system were changed to boot into legacy BIOS mode.*"

More detail can be found on the Acer website here: http://www.acer.com/disclaimer-downgrade-windows8/en/index.html

In order to resolve this the Boot Mode of the system will need to be changed.

The following steps apply to Acer machines that are using **Windows 7 x64** and **GPT** formatted disks.

Checking System Configuration

Firstly check if the drive is formatted using GPT:

From the Windows Start menu click the **Control Panel** shortcut.
Click **System and Security**.
Click **Administrative Tools**.
Double click on **Computer Management**.
Click on **Disk Management** in the left hand tree.
Right click on the **Disk 0** box (or appropriate disk) in the pictorial display of disks then click the **Properties** item.
Click the **Volumes** tab.
If the disk is using GPT the value for **Partition style** will be **GUID Partition Table (GPT)** as shown in the example below.

Adjusting BIOS Settings

If the disk is partitioned using **GPT** then the following steps can be attempted on the system.

Note: It is important that a full system backup is taken before using the following process.

Restart the machine.
The ACER splash screen will be displayed, press the **F2** key once this displays to display the BIOS.
You will see the **Information** section of the BIOS selected when it first loads.

Press the **Right Arrow** key **three** times to select the **Boot** section.
Within the **Boot** section is a setting for **Boot Mode**. If this is set to **Legacy** it might be the cause of the problem being experienced.

Press **Enter** to change the **Boot Mode**.
Press the **Up Arrow** to select **UEFI**, then press **Enter**.

The setting of **Boot Mode** will now show as **UEFI**.

We now need to disable the **Secure Boot** setting. This can only be done once a password has been specified on the BIOS.
Press the **Left Arrow** key to select the **Security** section.
Ensure the **Set Supervisor Password** option is selected and press **Enter**.

Enter and confirm a **password** to use for the BIOS, then press **enter**.
You should **make a record of the password** you specified for future use.
It will need to be entered when using the BIOS in the future.

Press the **Right Arrow** key to select the **Boot** section again.
Press the **Down Arrow** Key once to select the **Secure Boot** entry.
Press the **Enter** key, press the **Down Arrow** key to select

the **Disabled** option then press **Enter**.

The **Boot** section should now look as pictured below with **Boot Mode** set to **UEFI** and **Secure Boot** set to **Disabled**.

Press the **F10** key.
Press the **Left Arrow** key to select **Yes** to the confirmation to save changes then press **Enter**.
The system will now restart and boot into Windows.

System starts Windows

If with the settings above in place the machine is able start and load Windows correctly then you should be able to perform full disk encryption as normal. You should have a current backup of the disk before commencing the encryption operation.

System does NOT start Windows

If with the settings above in place the machine is **not** able to start Windows, then you will need to revert the changes made to allow Windows to load again. Set Boot Mode back to Legacy and enable Secure Boot. Please note you will need to supply the BIOS password you specified earlier in order to enter the BIOS to modify the settings.

In order to encrypt a system that is not able to start with the Boot Mode setting set to UEFI there are two possible options:

1. Upgrade the system to Windows 8, setting the Boot Mode setting to UEFI once installation is complete. You should ensure you have made a copy of your data and applications from the system before upgrading so that you can restore them after reinstallation.

2. Reinstall Windows 7 from Windows 7 media with the Boot Mode set to UEFI and Secure Boot set to Enabled (optional but recommended). You should ensure you have made a copy of your data and applications from the system before reinstalling Windows so that you can restore them after reinstallation.

Keywords: acer, travelmate, pm256, m385y, z5wbh, travel, mate, p265, p256m, p256-m