Microsoft

Enabling Support for the Microsoft UEFI Driver Signing CA on Surface Pro and Surface Pro 2

OVERVIEW AND AUDIENCE

Surface Pro and Surface Pro 2 systems currently do not include the Microsoft UEFI Certification Authority certificate in the systems' UEFI Secure Boot database. If present, this certificate would be in the Allowed Database (also referred to as "db"), enabling the execution of 3rd party UEFI applications and drivers that have been signed by the Microsoft UEFI CA. The tool bundled with this document enables the addition of the Microsoft UEFI Certification Authority certificate to the db. This tool is intended for use by IT professionals and advanced users who require the execution of 3rd party UEFI applications and drivers on a Secure Boot enabled system. Users of the tool should be familiar with the concepts of UEFI, Secure Boot, and BitLocker.

ABOUT THE TOOL

This tool performs the following operations on the system:

1. Adds the Microsoft UEFI Certification Authority certificate to the Allowed Database 'db'. Keys that are currently provisioned in the db will not be affected by this step.
2. Updates the Revoked Signatures Database 'dbx' with the most recent UEFI revoked signatures list. This step enhances the security of the system by denying Secure Boot to components which are signed with a compromised certificate.

BEFORE YOU BEGIN

This tool modifies the contents of the Surface Pro UEFI Secure Boot databases. <u>Improper use of this tool without taking the following precautions could render all data on the system unreadable and unrecoverable</u>. Before continuing, it is recommended that you do the following:

1. Backup all essential user data to an external storage device.
2. If BitLocker is enabled on the system:
    a. Backup the BitLocker Recovery Key.
    b. Turn off BitLocker and decrypt all BitLocker protected drives from the BitLocker Drive Encryption Control Panel applet. Ensure that all drives have been completely decrypted before proceeding.

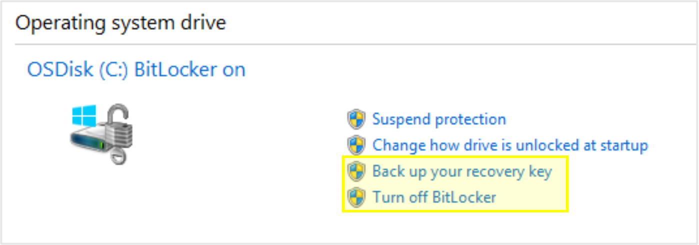
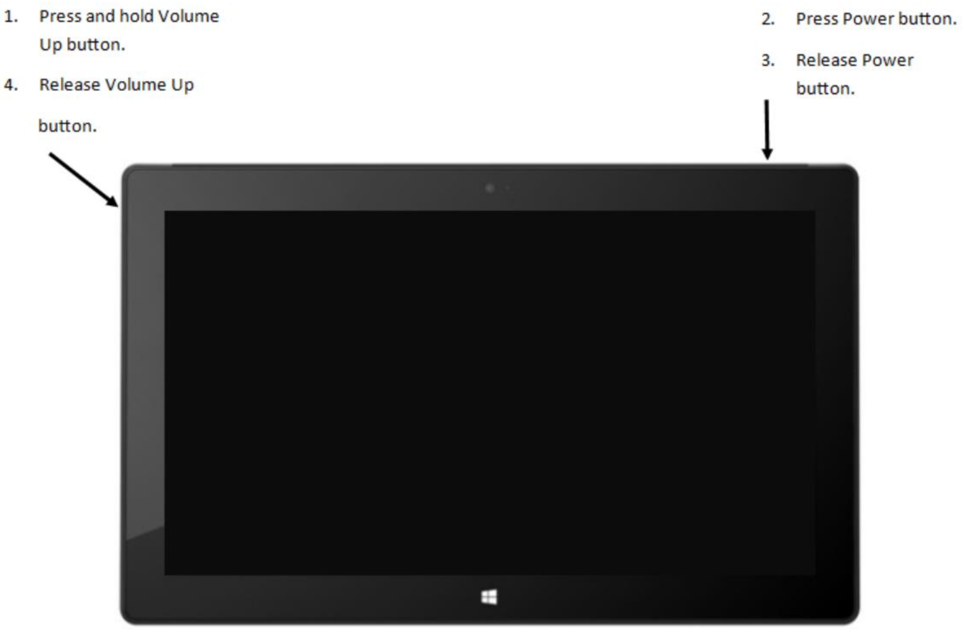


Figure 1: BitLocker options to back up the recovery key and turn off BitLocker

If you intend to create a new OS image containing your early boot UEFI components, do not delete the existing EFI System Partition on the Surface Pro device. The EFI System Partition is used for staging firmware updates to the Surface Pro device. If you delete the EFI System Partition, the Surface Pro device will no longer be able to receive firmware updates from Windows Update.

UPDATE PROCEDURE

1. Save Platform Key (Make sure that secure boot is not turned off and secure boot keys are not deleted. By default secure boot will be on)
   a. Copy folder containing this download package to Surface Pro or Surface Pro 2 device
   b. Launch admin command prompt and change to the directory containing this download package
   c. Run command **SavePlatformKey.cmd** and make sure there are no error messages displayed. This step should create two new files (**OEM_PK_SigList.bin** & **Existing_dbx_SigList.bin**) which will be used in step 5.
2. Boot to the UEFI menu.
   a. Shut down the Surface Pro device from within Windows. This can be done by going to **Settings > Power > Shut down** from the Charms Bar. The device must be shut down in order to boot to the UEFI settings menu.
   b. Perform the following key sequence: press and hold Volume Up button, press the Power button, release the Power Button, and release the Volume Up button.


1. Press and hold Volume Up button.
4. Release Volume Up button.
2. Press Power button.
3. Release Power button.

3. Delete the Secure Boot keys. (**Make sure steps 1 and 2 are successfully completed before following this step**)
   a. Click on **Delete All Secure Boot keys**.
   b. Click **Yes** when prompted “Delete all secure boot keys and databases to reset Platform to Setup Mode?”.
   c. Click **Exit Setup**.

   d. Click **Yes** when prompted “Save configuration and reset”.

4. Reboot to Windows.
5. Run the Secure Boot provisioning script.
   a. Login to Windows.
   b. Open a Command Prompt or Windows PowerShell instance with Administrator privileges.
   c. Navigate to the directory containing this download package.
   d. Run **InstallSecureBootWithMsftUefiCertAuthToDB.cmd** which will install secure boot keys with Microsoft UEFI Certificate Authority in DB.

The system is now provisioned with the default Secure Boot keys and the Microsoft UEFI Certification Authority. At this point you should be able to run 3rd Party UEFI drivers and applications that have been signed with the Microsoft UEFI Certification Authority.

Troubleshoot

If accidentally secure boot keys are deleted (step 3) before saving platform key (step 1)

a) Surface Pro device

   Rename file OEM_PK_SigList_SurfacePro.bin to OEM_PK_SigList.bin and follow step 5

b) Surface Pro 2 device

   Rename file OEM_PK_SigList_SurfacePro**_2**.bin to OEM_PK_SigList.bin and follow step 5