The Secure Boot Certificates are coming... The Secure Boot Certificates are coming...

Heads Up !!!

Secure Boot Certificates 2011 are EXPIRING Late June 2026 – Windows 8 era

Secure Boot Certificates 2023 are available from Windows Updates April 2026

Secure Boot certificates are crucial because they help ensure that only trusted, digitally signed software can run during the startup process of a device, preventing malware from loading.

This security feature protects the system from sophisticated threats right from the moment it powers on.

Checking Secure Boot Certificate Status

To determine if your Secure Boot certificates are up to date, you can use PowerShell commands and the Windows Security app.

Using PowerShell

1. Open PowerShell as Administrator.

2. Run the following commands:

Command Purpose

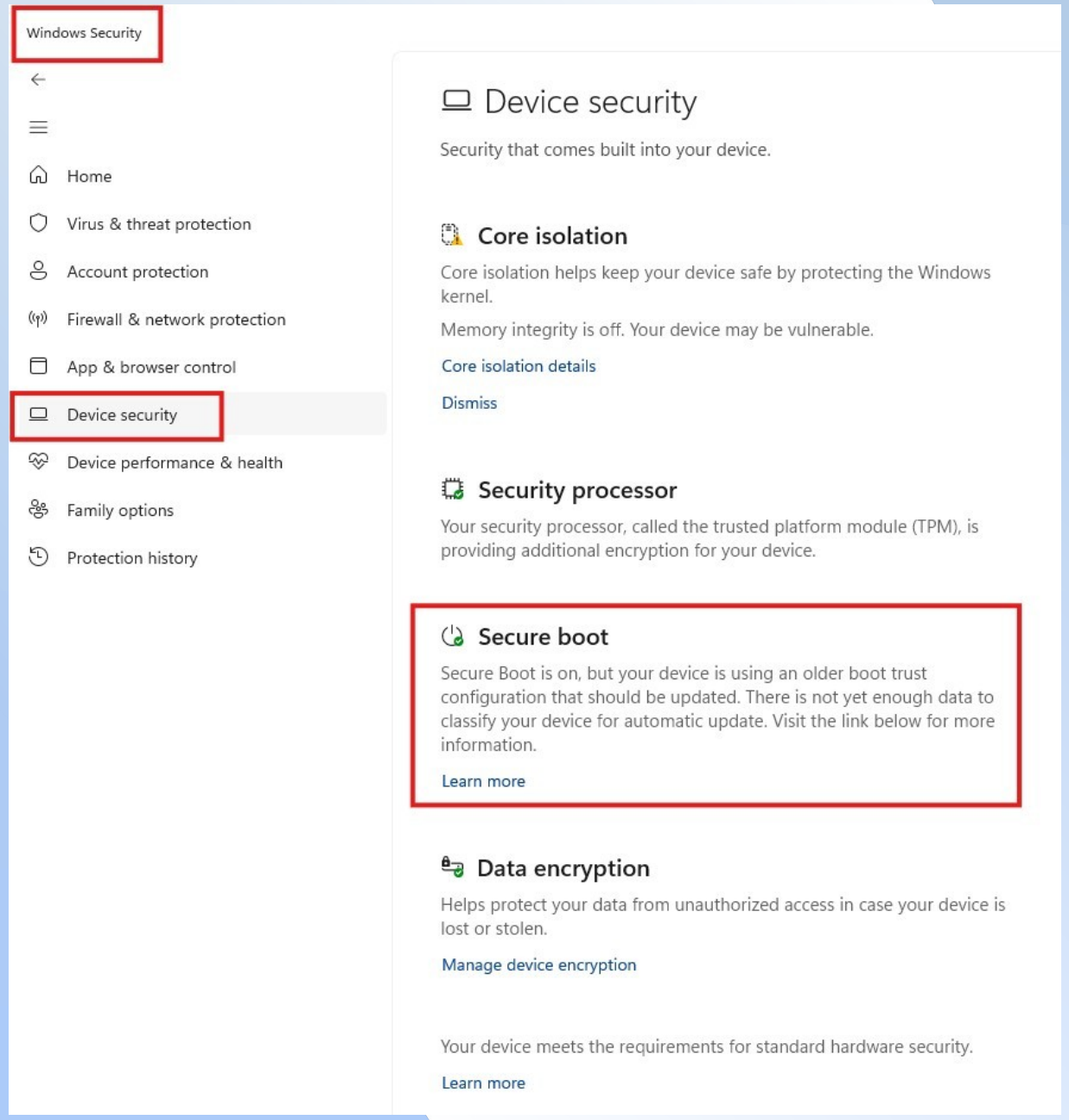
Confirm-SecureBootUEFI Checks if Secure Boot is enabled and functioning properly. It should return True.

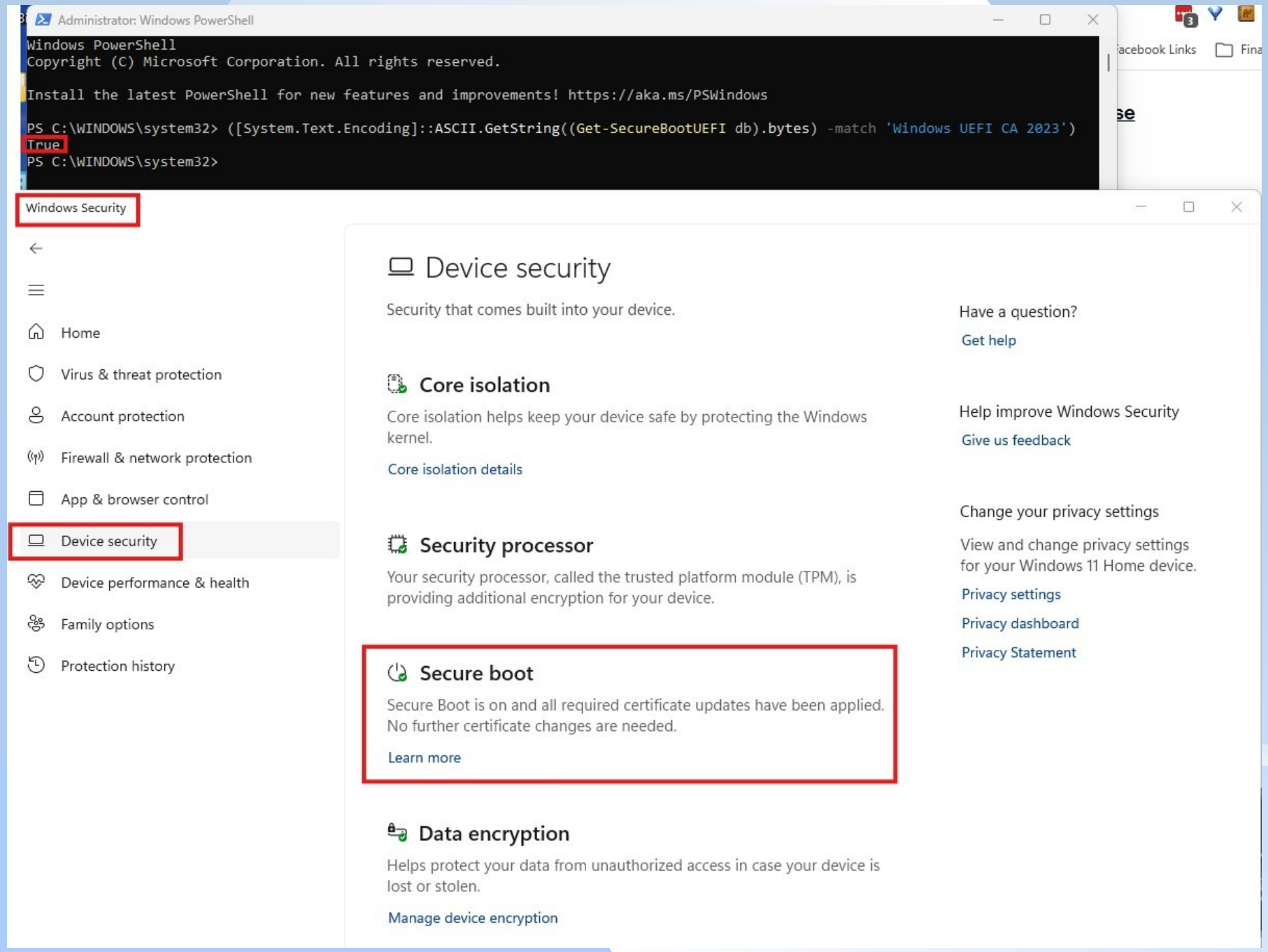
Command	Purpose
Get-SecureBootPolicy	Displays the current Secure Boot policy. Ensure there are no expired or invalid entries.
[System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI db).bytes) -match 'Windows UEFI CA 2023’	Verifies if the 2023 Secure Boot certificate is present in the Active Database.

Using Windows Security App

1. Open the **Windows Security app**.
2. Navigate to **Device security**.
3. Look for the **Secure Boot** section, which will indicate if Secure Boot is enabled and if the certificates are up to date.

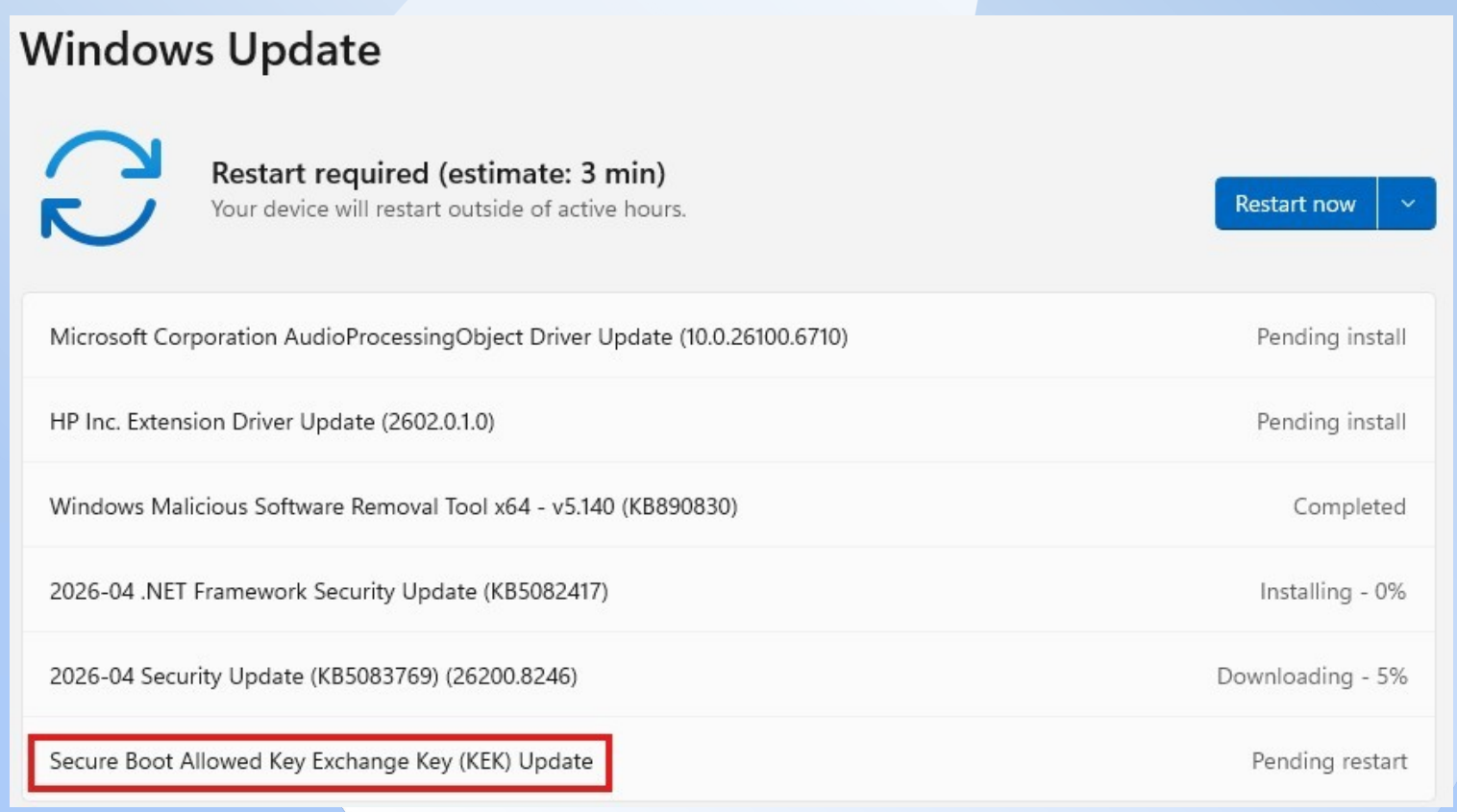
Windows Security App




Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\WINDOWS\system32> ([System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI db).bytes) -match 'Windows UEFI CA 2023')
True
PS C:\WINDOWS\system32>
Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Protection history
Device security
Security that comes built into your device.
Core isolation
Core isolation helps keep your device safe by protecting the Windows kernel.
Core isolation details
Security processor
Your security processor, called the trusted platform module (TPM), is providing additional encryption for your device.
Secure boot
Secure Boot is on and all required certificate updates have been applied. No further certificate changes are needed.
Learn more
Data encryption
Helps protect your data from unauthorized access in case your device is lost or stolen.
Manage device encryption
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 11 Home device.
Privacy settings
Privacy dashboard
Privacy Statement

How to Obtain Secure Boot Certificates via Windows Update

To obtain the latest Secure Boot certificates, ensure that Windows Update is enabled and install all available cumulative updates for Windows 11. This will automatically download and apply the new certificates to your device.



Most Windows computers will automatically receive Secure Boot certificate updates through Windows Update

The following conditions must be met for automatic updates to occur:

Secure Boot Enabled: The Secure Boot feature must be activated in the system's firmware settings.

Supported Windows Versions: The device must be running a supported version of Windows, such as Windows 11.

Windows 10 with Extended Security Updates (EDU) probably will

However, some older devices may not receive these updates if their firmware does not support them.

Using PowerShell to Retrieve Secure Boot Certificates

Expected Output will display details about the certificates, including their names and attributes. This information helps verify that the correct Secure Boot certificates are installed on your system.

1. Open PowerShell as Administrator:

- Search for PowerShell in the Start menu.
- Right-click on Windows PowerShell and select "Run as administrator."

2. Run the Commands in Powershell:

- Type the following command to check the Secure Boot database:

```
Get-SecureBootUEFI -Name db
```

- Then, check the Key Exchange Key with:

```
Get-SecureBootUEFI -Name KEK
```

Obtain and Save the BitLocker Key

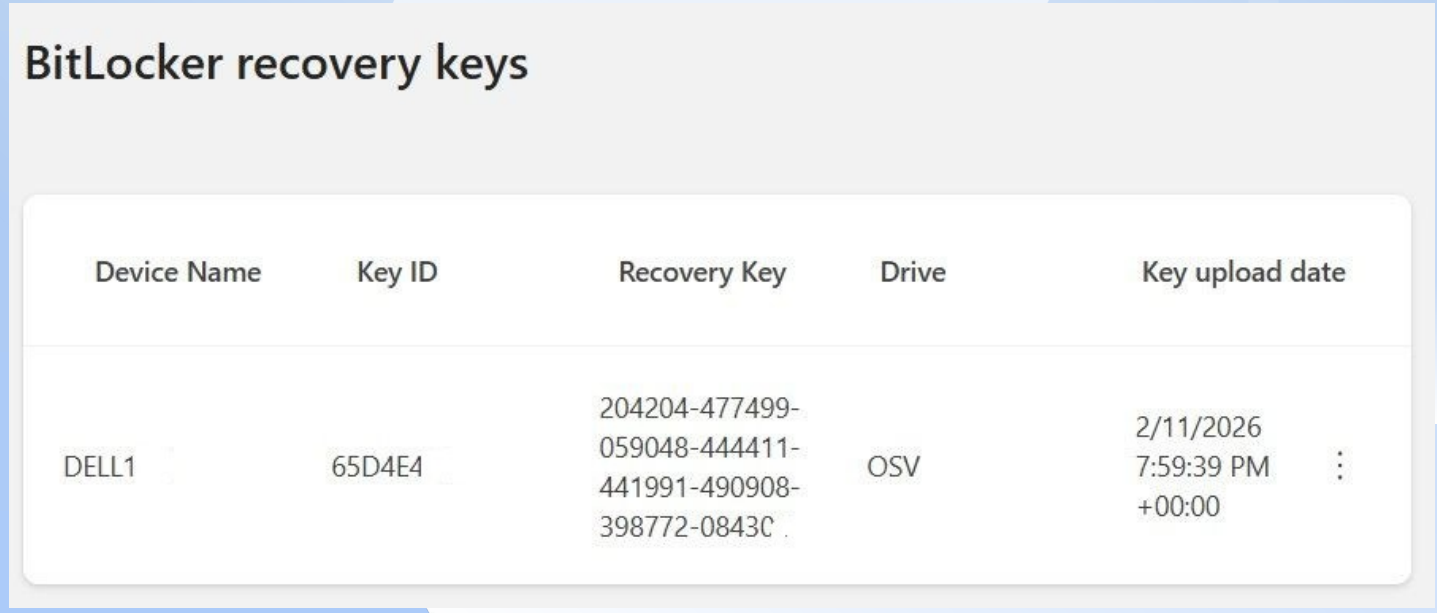
If there is a problem with the Secure Boot Certificates and BitLocker is active on Windows Pro, Enterprise or Education editions there could be a problem even accessing an encrypted drive without the BitLocker Key.

BitLocker Keys can generally be seen in your Microsoft Account associated with the computer.

Also in Windows Security

Data Encryption

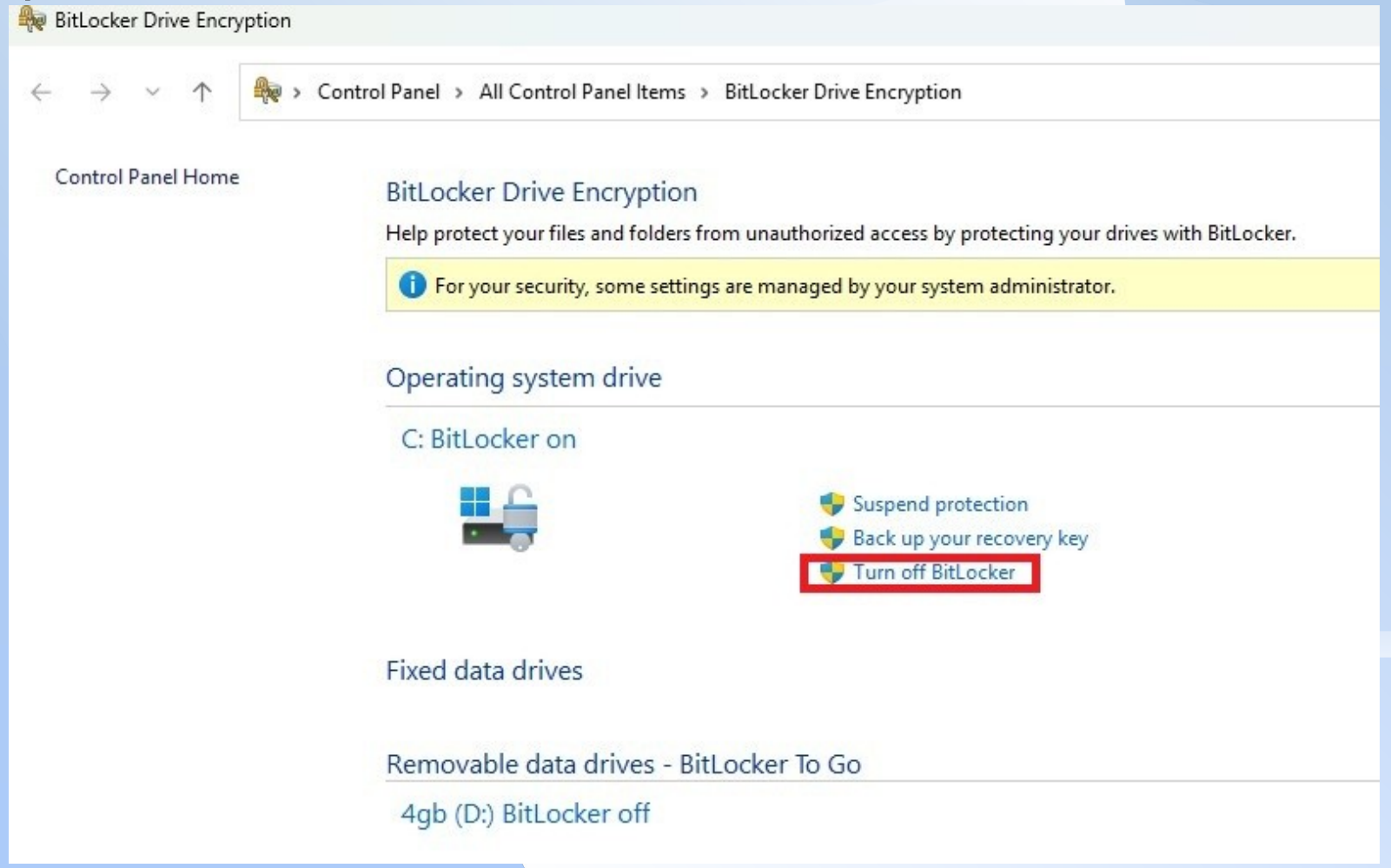
Print or Save a Snip



Obtain and Save the BitLocker Key

BitLocker can be Suspended or even Turned Off in Control Panel

Back Up Key option



To force the installation of the Windows UEFI CA 2023 Secure Boot certificates via PowerShell

1. Suspend BitLocker (if enabled) If your drive is encrypted, suspend protection for the required reboot cycles:

manage-bde -Protectors -Disable C: -RebootCount 1

Note: Some scripts recommend -RebootCount 2 to ensure the update completes fully.

Note: Windows Home does not have BitLocker but it can have Device Encryption found in Windows Security App

2. Set the Registry Key Open PowerShell as Administrator and run the following command to trigger the deployment of all necessary certificates (including the new CA 2023 and boot manager):

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Secureboot /v AvailableUpdates /t REG_DWORD /d 0x5944 /f
```

0x5944: Deploys all certificates and updates the boot manager.

0x5be6: Deploys certificates and revokes the old PCA 2011 cert (use with caution).

0x40: Deploys only the Windows UEFI CA 2023 to the DB.

3. Trigger the Update Task Start the secure boot update scheduled task:

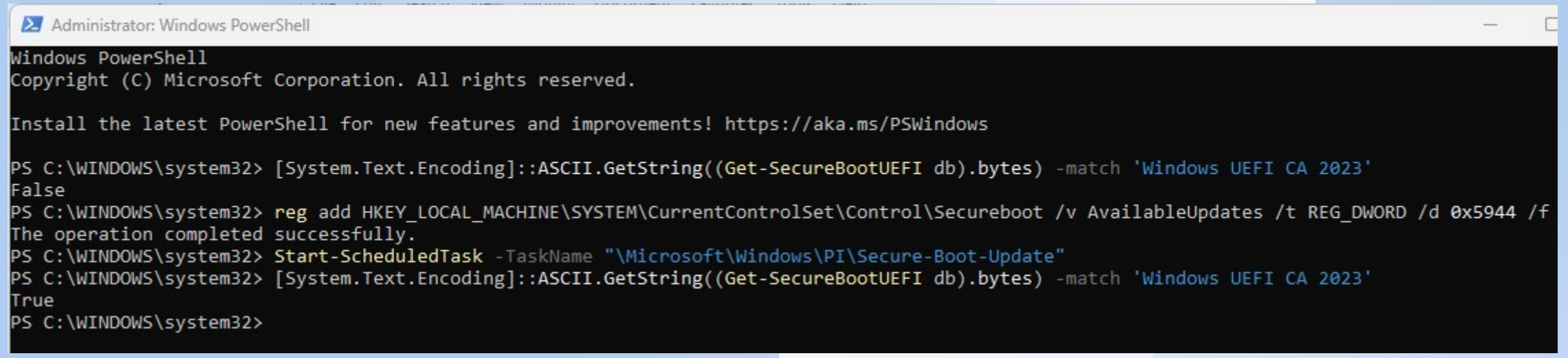
Start-ScheduledTask -TaskName "\Microsoft\Windows\PI\Secure-Boot-Update"

4. Reboot and Verify Restart your computer. The process may require two reboots to fully write the firmware changes. Afterward, verify the installation with:

[System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI db).bytes) -match 'Windows UEFI CA 2023'

If the output is True, the new certificate is installed.

If you suspended BitLocker, resume it with Resume-BitLocker -MountPoint "C:".


Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\WINDOWS\system32> [System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI db).bytes) -match 'Windows UEFI CA 2023'
False
PS C:\WINDOWS\system32> reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Secureboot /v AvailableUpdates /t REG_DWORD /d 0x5944 /f
The operation completed successfully.
PS C:\WINDOWS\system32> Start-ScheduledTask -TaskName "\Microsoft\Windows\PI\Secure-Boot-Update"
PS C:\WINDOWS\system32> [System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI db).bytes) -match 'Windows UEFI CA 2023'
True
PS C:\WINDOWS\system32>

For enterprise environments, you can also deploy this via Group Policy by enabling Computer Configuration > Administrative Templates > Windows Components > Secure Boot > Enable Secure Boot certificate deployment policy.

To install Secure Boot certificates via an OEM BIOS update, ensure your device's BIOS is updated to a version that includes the new Secure Boot certificates.

This typically involves downloading the appropriate BIOS update from the OEM's website and following their specific installation instructions.

Important Note : Most devices manufactured since 2024 should already have the updated Secure Boot certificates.

To obtain motherboard information using System Information, press

Windows + R, type msinfo32, and hit Enter.

In the System Summary, look for BaseBoard Manufacturer, BaseBoard Product, and BaseBoard Version to find your motherboard details.

- BaseBoard Manufacturer: This shows the manufacturer of your motherboard.
- BaseBoard Product: This indicates the model of your motherboard.
- BaseBoard Version: This provides the version number of your motherboard.

Note: This is a good article on Secure Boot 2023 Certificate Updates

Written by Ed Bott, Senior Contributing Editor March 12, 2026 at 5:53 a.m. PT

https://www.zdnet.com/article/secure-boot-certificate-updates-2026/

“How to check your Windows PC for expiring security certificates - a big one is ending soon”

To see whether your PC has the updated certificates, open a PowerShell window using administrator credentials and then copy the following command and paste it at the PowerShell command line:

([System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI db).bytes) -match 'Windows UEFI CA 2023')

Thank you

Don Beach

President PCBUG

https://pcbug.org

don@naplestechguy.com