Title: **How to handle Windows Secure Boot certificate expiration / Minimum Dell Firmware (BIOS) version with new 2023 certificates**
May 5, 2026

Key words:
Windows Operating System, Prinect Qualified Dell Systems, Dell Deployment

Objective:
Secure Boot is a security feature in Unified Extensible Firmware Interface (UEFI) based firmware that helps ensure that only trusted software runs during a device's boot (start) sequence. It works by verifying the digital signature of pre-boot software against a set of trusted digital certificates (also known as certificate authority or CA) stored in the device's firmware. Microsoft is updating the Secure Boot certificates originally issued in 2011 to ensure Windows devices continue to verify trusted boot software. These older certificates begin expiring in June 2026 and must be updated with their according successor:

Expiring Certificate	Expiration date	New Certificate	Purpose
Microsoft Corporation KEK CA 2011	June 2026	**Microsoft Corporation KEK 2K CA 2023**	Signs updates to DB and DBX.
Microsoft Windows Production PCA 2011	Oct 2026	**Windows UEFI CA 2023**	Used for signing the Windows boot loader.
Microsoft UEFI CA 2011	June 2026	**Microsoft UEFI CA 2023**	Signs third-party boot loaders and EFI applications.
		Microsoft Option ROM UEFI CA 2023	Signs third-party option ROMs

The impact of Secure Boot certificate expiration
Devices that haven't received the newer 2023 certificates will continue to start and operate normally, and standard Windows updates will continue to be installed. However, these devices will no longer be able to receive new security protections for the early boot process, including updates to Windows Boot Manager, Secure Boot databases, revocation lists, or mitigations for newly discovered boot level vulnerabilities. Over time, this limits the device's protection against emerging threats and may affect scenarios that rely on Secure Boot trust.

Most Windows devices will receive the updated certificates automatically, and many OEMs provide firmware updates when needed. Keeping your device current with these updates helps ensure it can continue receiving the full set of security protections that Secure Boot is designed to provide.

There are two Secure Boot databases present on the system: While the **active** Secure Boot Database (i.e. the one that is currently used during system startup) is commonly updated from Windows Update, the **Default** Secure Boot Database is stored on the system firmware and needs to be updated by flashing the system's BIOS.

Note: The Default Secure Boot database is a backup set of original trusted keys that can be restored if needed, it will become effective after resetting the system BIOS to default values.

HEIDELBERG qualified DELL EMC Servers:

Below are the **minimum** BIOS versions released by Dell for each generation of Heidelberg qualified Dell PowerEdge servers that include the Microsoft Secure Boot 2023 certificates:

PowerEdge 16G Platform	**BIOS Version**
T360 / R360 / T160,	2.4.0
T560 / R660xs	2.8.2
R7625	1.15.3
PowerEdge 15G Platform	
T550 / R450	1.19.2
T350 / R350 / T150	1.13.0
PowerEdge 14G Platform	
T640 / R640	2.25.0
R940	2.25.0
T440 / R440	2.25.0
T340 / R340 / T140	2.21.0

HEIDELBERG qualified DELL Workstations:

Below are the **minimum** BIOS versions released by Dell for Heidelberg qualified Dell workstations that include the Microsoft Secure Boot 2023 certificates:

Precision Workstations	**BIOS Version**
Precision 3630 Tower	2.37.0
Precision 3640	1.41.0
Precision 3650 Tower	1.44.0
Precision 3660	2.30.1
Precision 3680 Tower	1.18.2
Dell Pro Max Tower T2 FCT2250	1.7.1
OptiPlex Workstations	
OptiPlex Small Form Factor 7010	1.30.0
OptiPlex SFF 7020	1.20.0
OptiPlex XE3	1.38.0
OptiPlex XE4 SFF	1.33.2
Dell Pro Slim Plus QBS1250 (XE5)	1.7.0

For older systems, there aren't any BIOS updates with Microsoft's 2023 Secure Boot certificates available. Dell started shipping both 2011 and 2023 certificates on newly launched platforms in late 2024 and, by the end of 2025, on all sustaining platforms shipping from Dell factories.

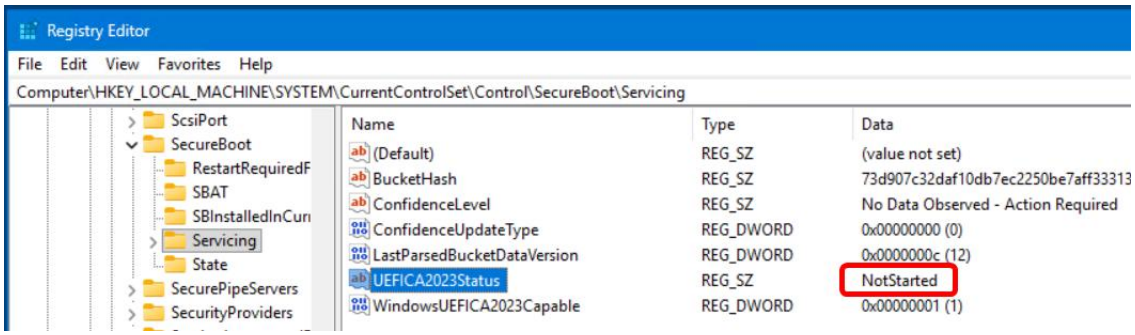
Implementation:

Please make sure that you update the Dell system BIOS (at least) to the version listed above. If this is not possible due to specific limitations, please follow the guidance as described in the article https://www.dell.com/support/kbdoc/en-us/000402373/poweredge-server-bios-update-guidelines-for-microsoft-secure-boot-certificates.

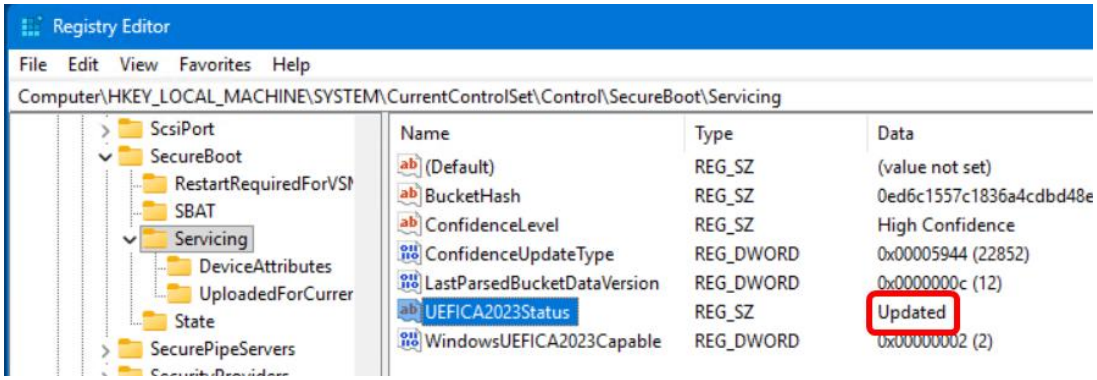
In addition, it is necessary to install the latest Microsoft updates to ensure that the new Secure Boot certificates are available on the system (note: It is always necessary to install Microsoft updates to ensure system security).

Check the certificate update status:

To verify the update status, you may look at the registry keys located in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing\` , you will find a value named "`UEFICA2023Status`" there. If the certificate update has not been started yet, it shows "`NotStarted`":



If the update has been (successfully) completed, it says "`Updated`":



You also may run the PowerShell command
`([System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI db).bytes) -match 'Windows UEFI CA 2023')`
to check for the new CA, it reports "True", if the string will be found in the database:

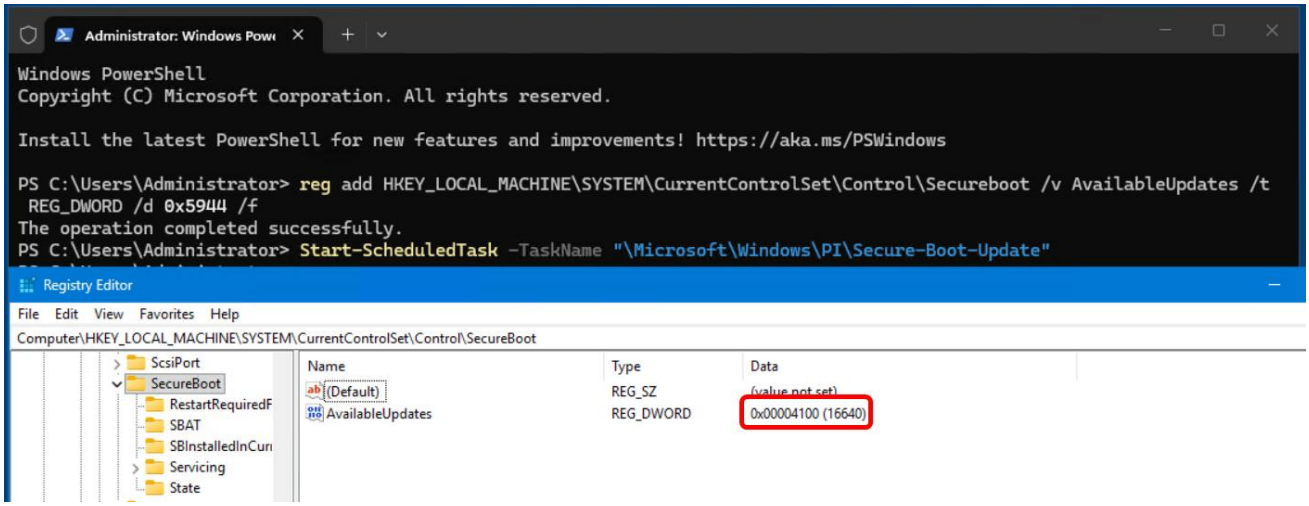
How to manually trigger the Secure Boot certificate update:

The manual certificate update can be triggered by setting the registry value `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\AvailableUpdates` to "`0x5944`" and trigger the update task.
Open an administrative PowerShell prompt and run the following command:

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

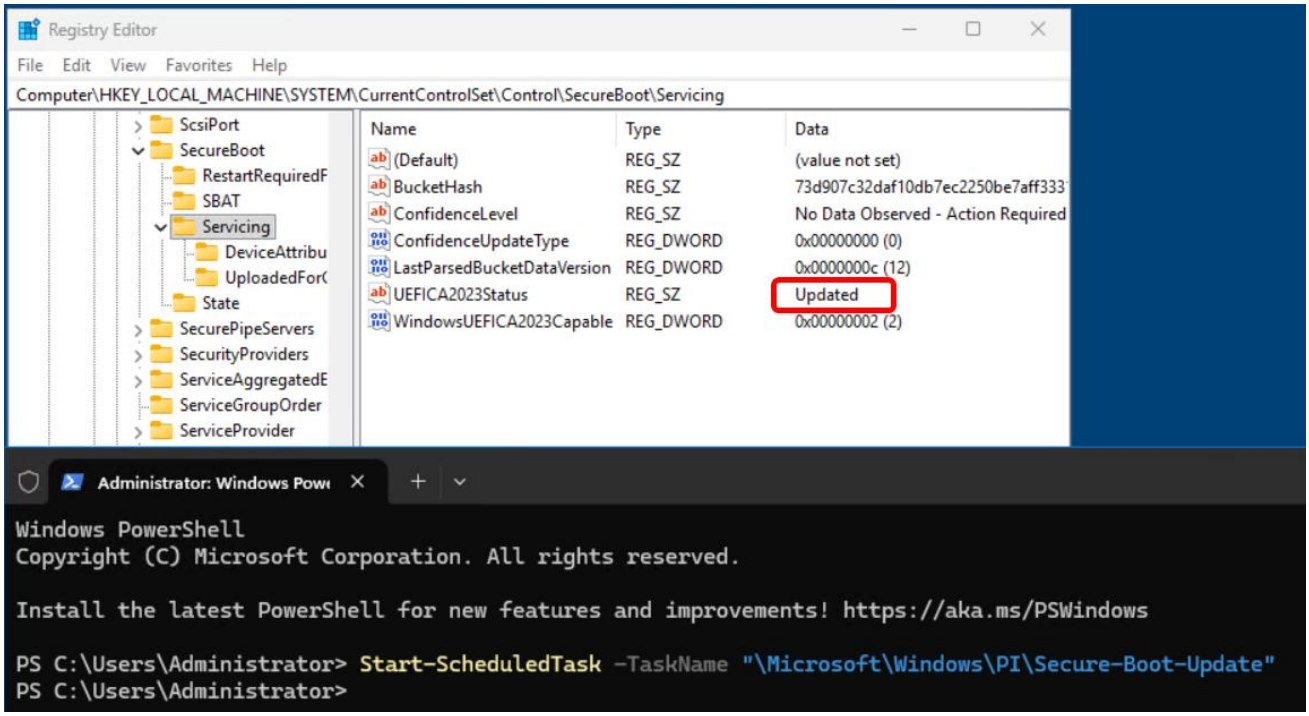
and afterwards run

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



Manually reboot the system when the "`AvailableUpdates`" value becomes "`0x4100`".
After the system is up again, open an administrative PowerShell prompt an again run

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



The "`UEFICA2023Status`" value becomes "`Updated`" now. For further details, please refer to the "Windows Server Secure Boot playbook" (see link below).

References:

Microsoft references:

“Windows Server Secure Boot playbook” for certificates expiring in 2026: https://techcommunity.microsoft.com/blog/windowsservernewsandbestpractices/windows-server-secure-boot-playbook-for-certificates-expiring-in-2026/4495789

Windows Secure Boot certificate expiration and CA updates: https://support.microsoft.com/en-us/topic/windows-secure-boot-certificate-expiration-and-ca-updates-7ff40d33-95dc-4c3c-8725-a9b95457578e

Registry key updates for Secure Boot: https://support.microsoft.com/en-us/topic/registry-key-updates-for-secure-boot-windows-devices-with-it-managed-updates-a7be69c9-4634-42e1-9ca1-df06f43f360d

Dell references:

Servers: https://www.dell.com/support/kbdoc/en-us/000402373/poweredge-server-bios-update-guidelines-for-microsoft-secure-boot-certificates

Workstations: https://www.dell.com/support/kbdoc/en-us/000347876/microsoft-2011-secure-boot-certificate-expiration

Secure Boot Transition FAQ: https://www.dell.com/support/kbdoc/en-us/000390990/secure-boot-transition-faq