UEFI-2026

UEFI-2026 - Readiness

TITLE	UEFI-2026
AUTHOR	Docusnap Consulting
DATE	9/18/2025
VERSION	1.0 | valid from 7/4/2016

CONTENTS

1. Introduction

In 2026, millions of systems worldwide will face a critical security issue: the Microsoft certificates previously used for UEFI Secure Boot will expire.

Secure Boot is a key security mechanism that prevents manipulated or unsigned software from being loaded during system startup. With the expiration of these certificates in June and October 2026, many devices will lose the ability to recognize new firmware or operating system updates as trustworthy.

Affected systems include:

- traditional Windows PCs and servers
- virtual machines
- dual-boot systems with Linux or macOS

Without timely action, for example installing new certificates or applying necessary firmware updates, systems may fail to boot or remain exposed to persistent security vulnerabilities.

Docusnap makes it possible to detect whether old certificates are still active or whether they have already been replaced with the new ones. This provides administrators with a reliable basis to identify the need for action and plan targeted measures.

1.1 Obtaining Current Certificates

Via Windows Update (automated)

- Systems that regularly receive Windows Updates and send telemetry are automatically included in the Managed Certificate Update.
- Starting in July 2025, preparatory updates will be distributed (e.g., KB5064489).
- New certificates (KEK 2K CA 2023, UEFI CA 2023, Option ROM UEFI CA 2023) will be entered into the UEFI certificate store via the update mechanism.

Via Firmware/BIOS Updates from the OEM

- Manufacturers such as HP, Dell, and Lenovo deliver the certificates through BIOS/UEFI updates.
- These must be applied manually or via vendor management tools if Windows Update is blocked or not in use.

1.2 Limitations Without Telemetry

Microsoft explicitly points out: Without telemetry, devices will not automatically be included in the rollout group.

Consequence:

- Systems without telemetry will not receive new certificates via Windows Update.
- They will retain the old 2011 certificates and thus directly run into the UEFI 2026 problem.

Impacts:

- Starting June 2026: Expiration of KEK and UEFI CA 2011 → no further installation of new boot drivers or firmware components possible.
- Starting October 2026: Expiration of Windows Production PCA 2011 → no further bootloader updates possible.

Result: Systems may become insecure (e.g., no protection against bootkits such as BlackLotus) or, in extreme cases, may fail to start.

2. Prerequisites

During Windows inventory, the trusted certificates must also be read. By default, however, these are not activated in the component selection. Reading the certificates requires administrative privileges on the system.

3. Analysis with Docusnap

To verify UEFI 2026 readiness, Docusnap checks for the existence of the following certificates:

- CN=Microsoft Corporation KEK 2K CA 2023
  Thumbprint: 459AB6FB5E284D272D5E3E6ABC8ED663829D632B
- CN=Microsoft Option ROM UEFI CA 2023
  Thumbprint: 3FB39E2B8BD183BF9E4594E72183CA60AFCD4277
- CN=Microsoft UEFI CA 2023
  Thumbprint: B5EEB4A6706048073F0ED296E7F580A790B59EAA

Identification is performed using the thumbprints.

Evaluation in Docusnap

Through the UEFI 2026 Readiness report (Path: Company → Infrastructure → Domain → Reports → Infrastructure HW → UEFI 2026 Readiness) and the corresponding Connect package (UEFI 2026 Readiness), it can be determined whether devices are already "UEFI 2026 Ready."

Status Evaluation

- Yes – Certificates with the thumbprints listed above are present
- No – Certificates are missing
- Can't be determined – Certificates could not be read

4. Note

Docusnap cannot provide recommendations for action if the required certificates are missing. The solution only indicates whether a device already has the new certificates and is therefore "UEFI 2026 Ready." For further information or necessary measures, administrators must refer to the guidance provided by the respective manufacturer.

Further information:
Microsoft Tech Community Blog – Act now: Secure Boot certificates expire in June 2026

VERSION HISTORY

Date	Description
26.08.2025	Document Created