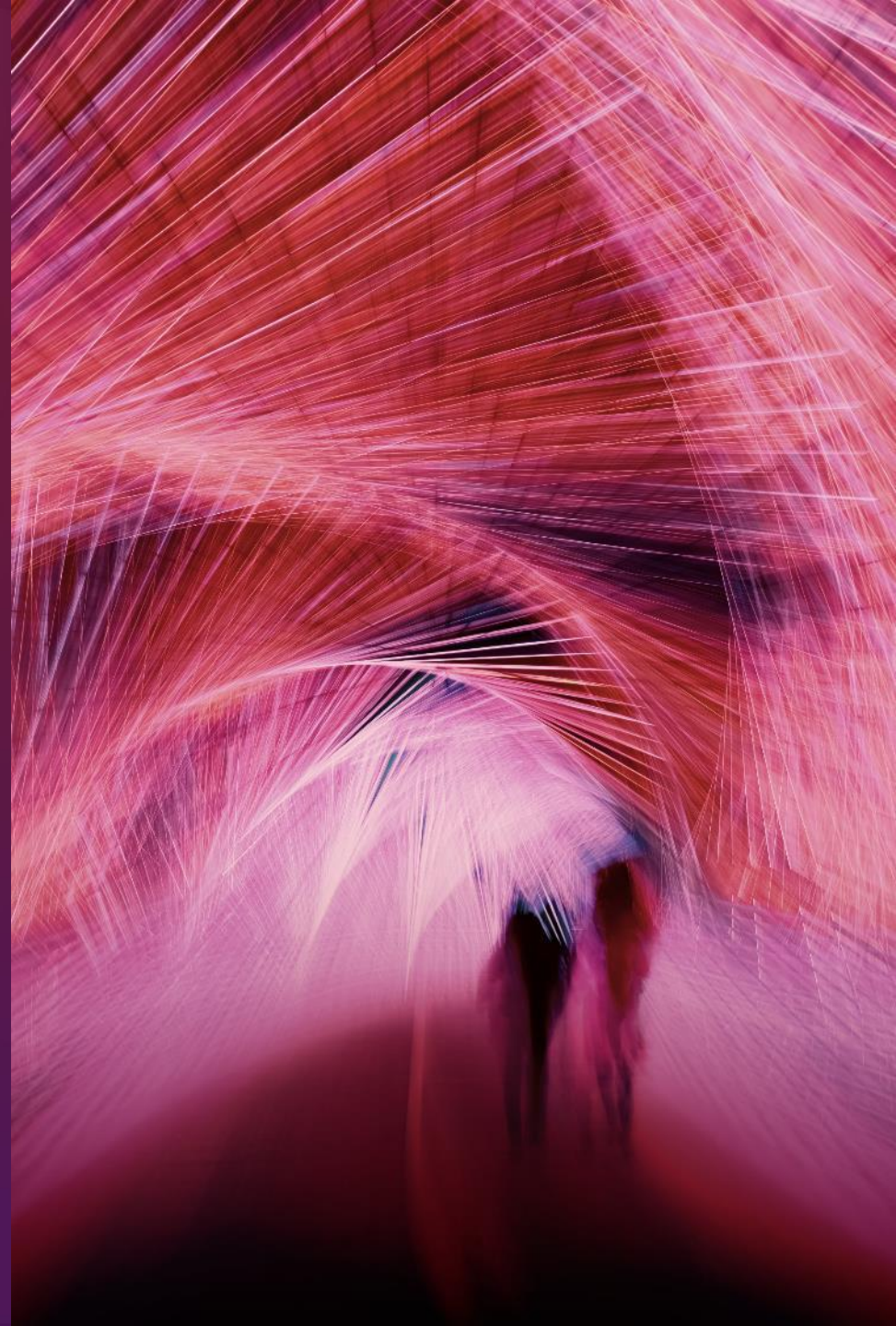
Smarter technology for all

Lenovo ThinkSmart Secure Boot Cert Expiry Analysis & Recommendations

Introduction

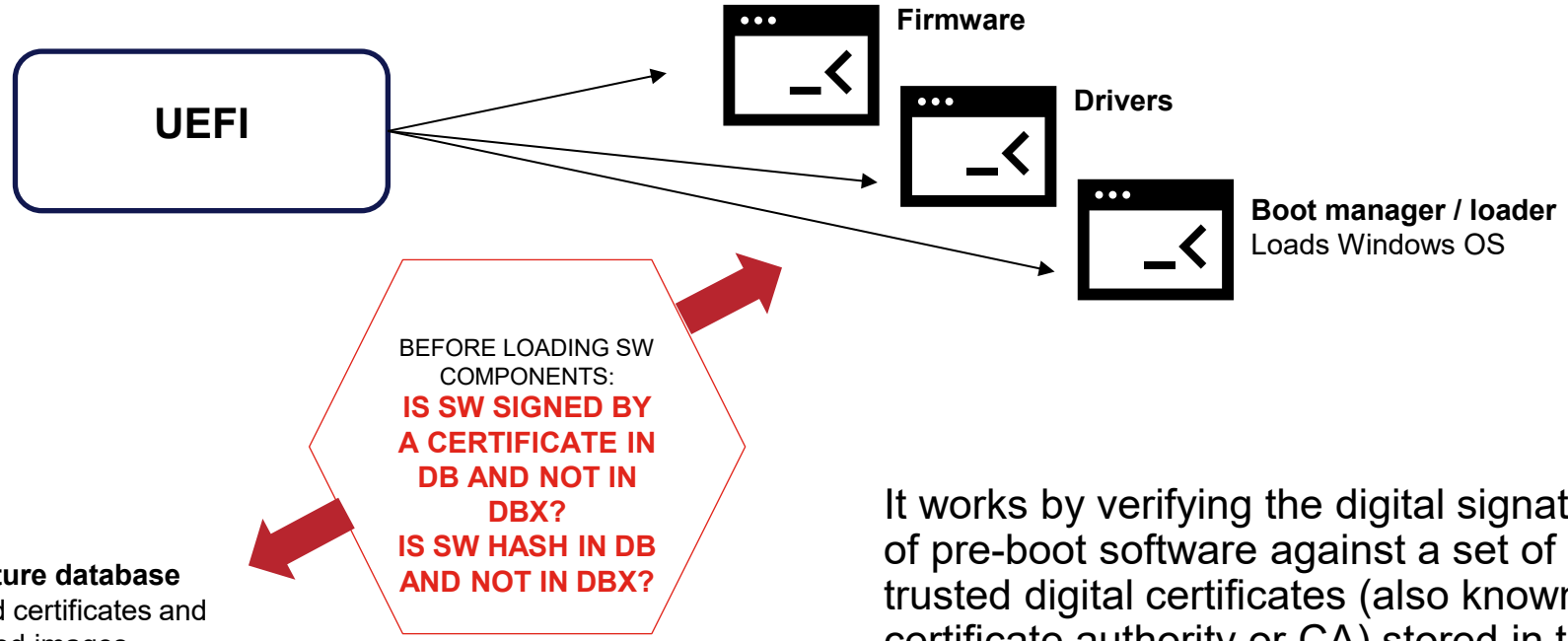


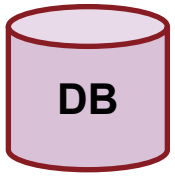
What is secure boot and why it's important

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

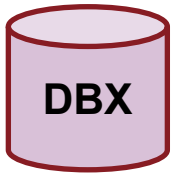
Why boot-level security is so important? An attacker with access to the boot chain can effectively own the entire system, and no amount of endpoint protection / antivirus running inside Windows can do anything about it.

You may remember the Black Lotus vulnerability a few years ago …





Allowed Signature database
Contains trusted certificates and hashes of allowed images

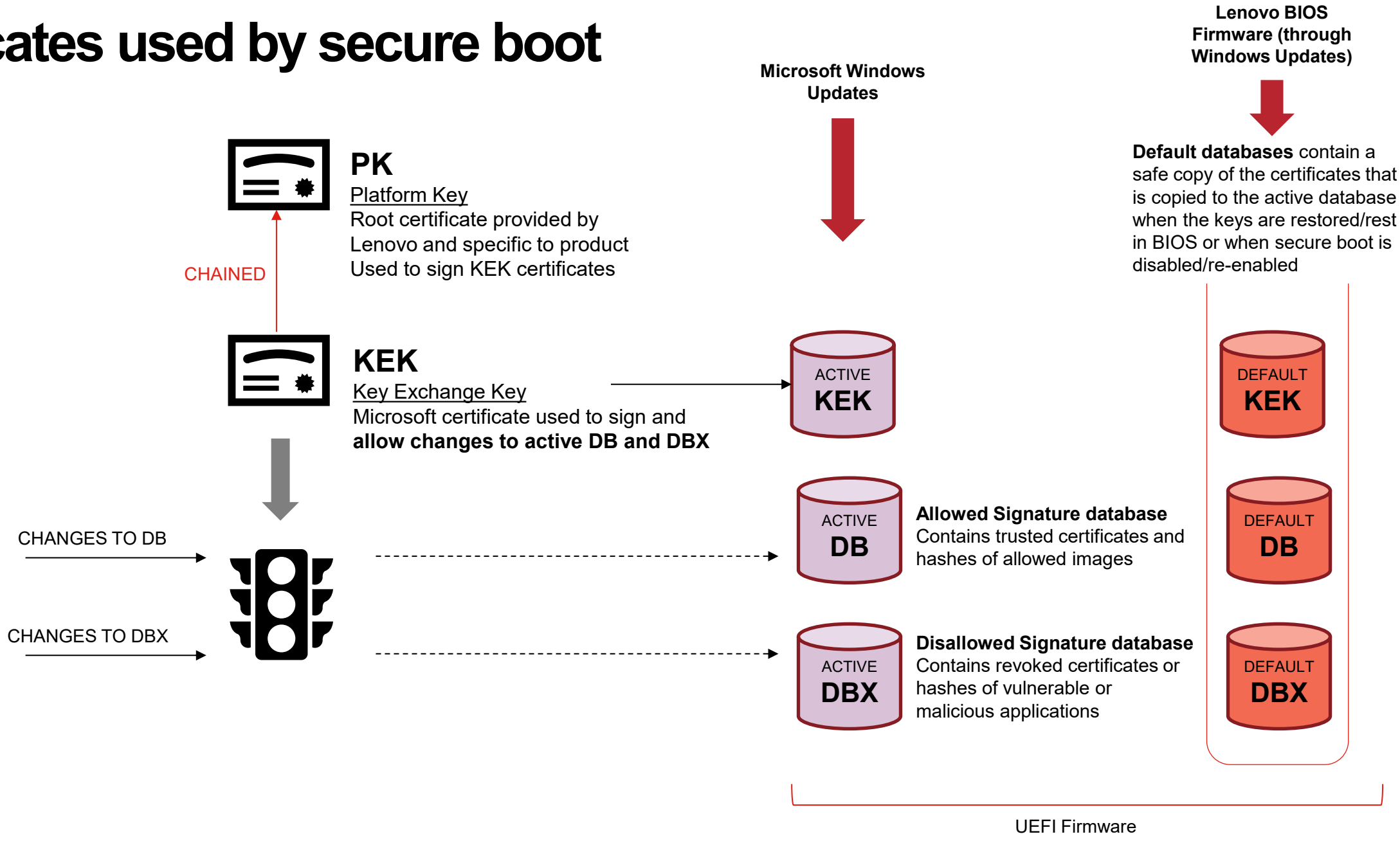


Disallowed Signature database
Contains revoked certificates or hashes of vulnerable or malicious applications

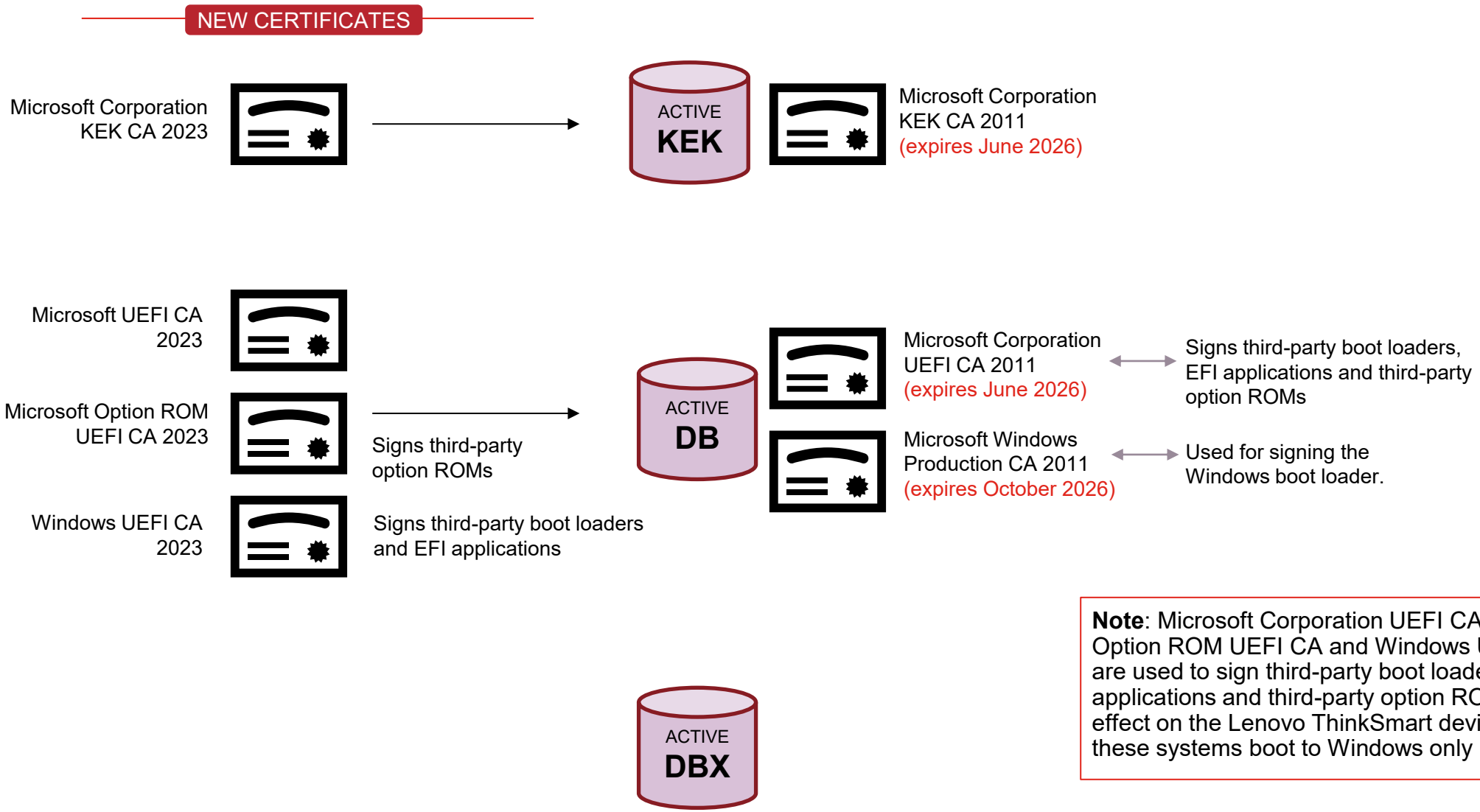
It works by verifying the digital signature of pre-boot software against a set of trusted digital certificates (also known as certificate authority or CA) stored in the device's firmware.

Note: Secure Boot is enabled by default in all ThinkSmart devices and must remain enabled to be compliant with Microsoft Teams Room on Windows rules

Certificates used by secure boot



Secure Boot Certificate Expiration and Update

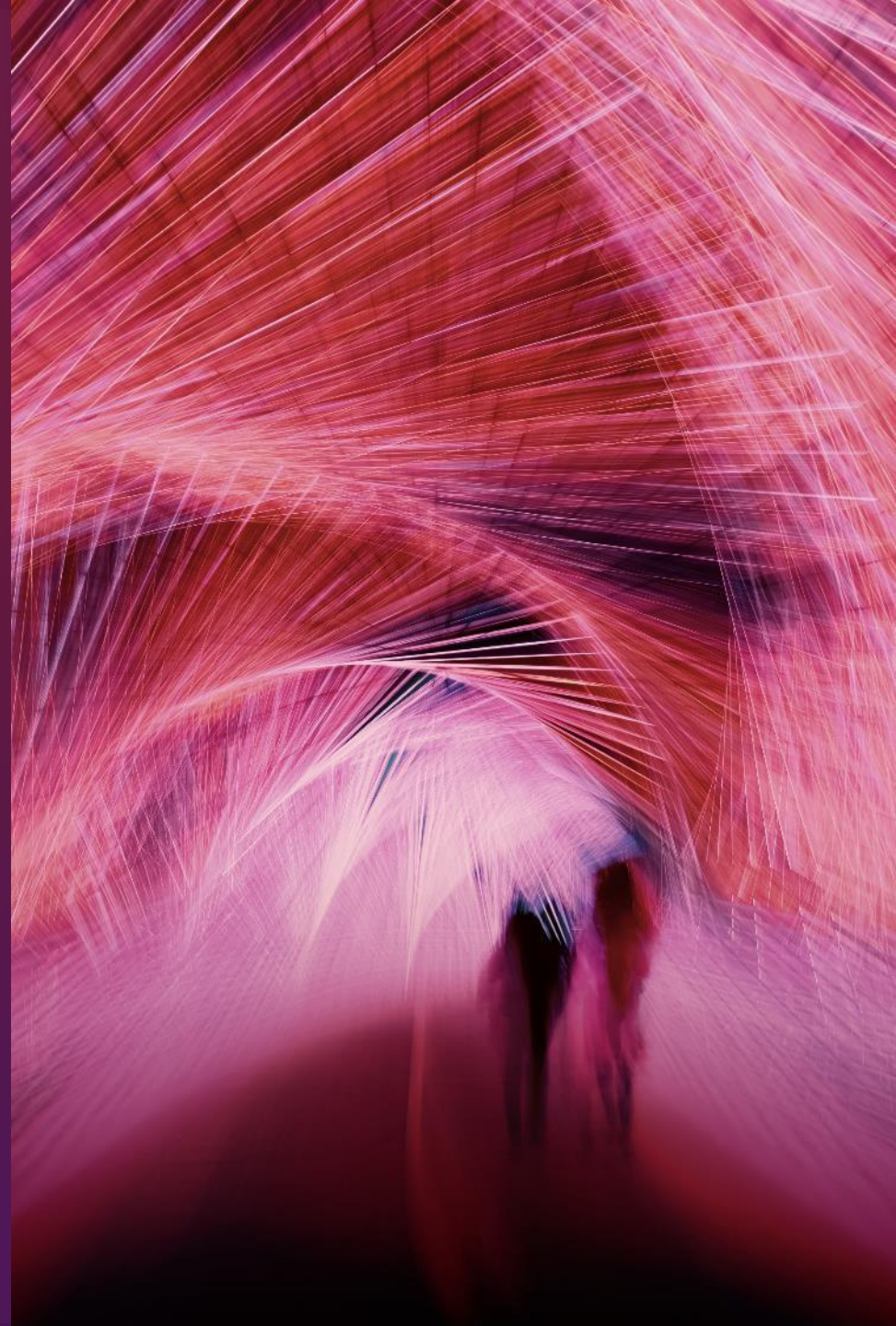


Note: Microsoft Corporation UEFI CA, Microsoft Option ROM UEFI CA and Windows UEFI CA that are used to sign third-party boot loaders, EFI applications and third-party option ROMs, have no effect on the Lenovo ThinkSmart devices since these systems boot to Windows only

Secure Boot Cert Expiry

Current Status

May 2026



Current status

- All deployed devices have received BIOS updates that have placed the new certificates in the KEKdefault and DBdefault databases.
  - For these devices, in case they have not received yet the new certificates in the Active DB/KEK, if bitlocker is enabled please note that resetting keys in BIOS or disabling/re-enabling Secure Boot will trigger the BitLocker recovery flows.
- Devices manufactured since October 2025 have the new certificates also in the KEK and DB active databases since they were added at the factory (without triggering bitlocker recovery).
- Please make sure your devices have received all latest BIOS updates through WU

What's in progress

2 further steps are occurring in the certificate update process:

1. **Microsoft is adding the new certificates to the KEK/DB active databases through Windows Updates** (without triggering a bitlocker recovery flow) and will keep DB/DBX servicing healthy
   - KEK 2023 will be delivered before June 2026

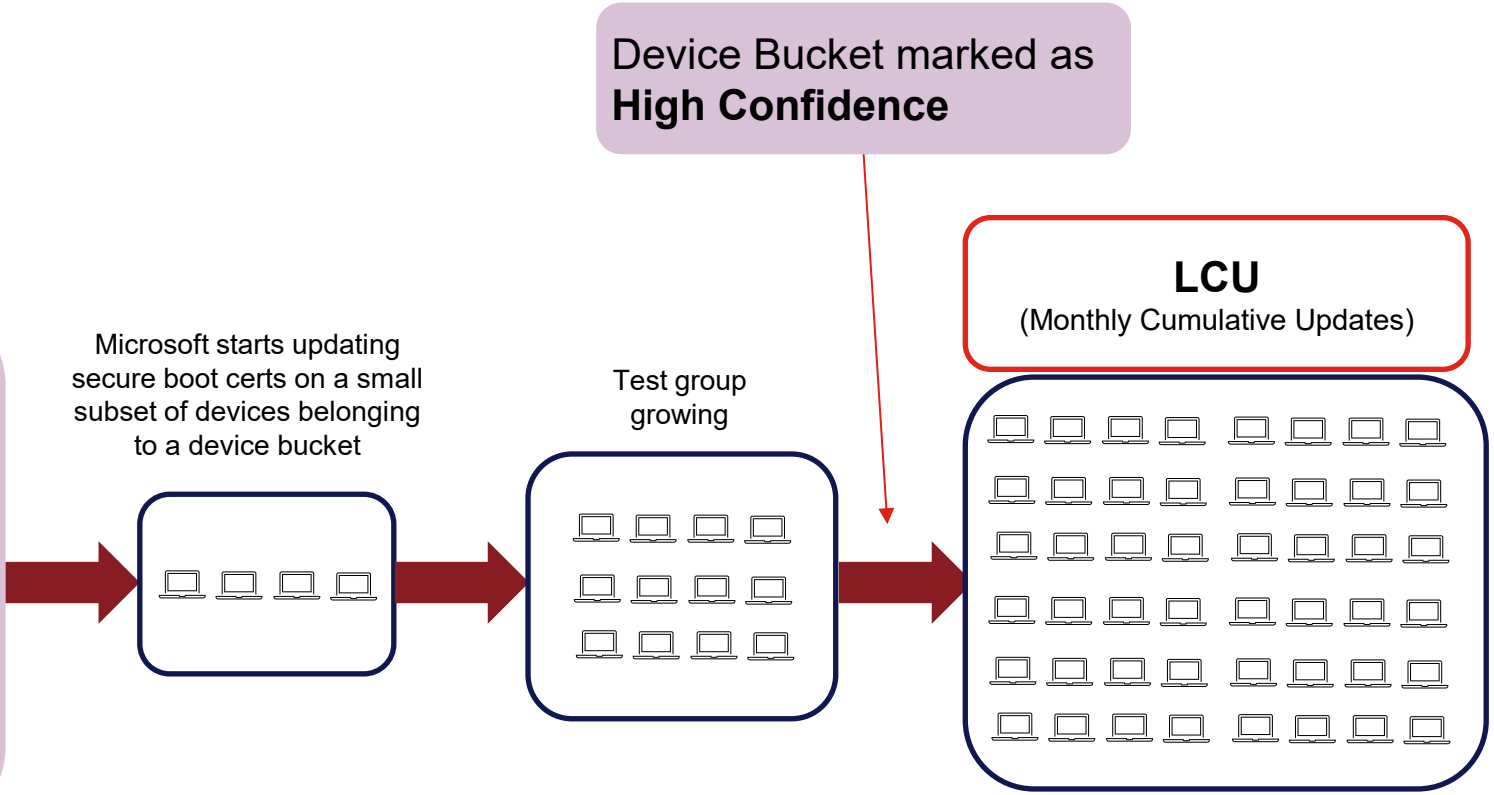
2. **Microsoft is delivering the new boot manager (signed by 2023 certs) via WU**
   - Microsoft started enabling the new 2023 boot manager in Dec 2026
   - The process will be complete by October 2026

Conservative approach by Microsoft: CFR Controlled Feature Rollout based on Windows telemetry

Microsoft has been compiling a full list of Device Buckets (unique hw/sw characterization of a device) based on data collected through telemetry

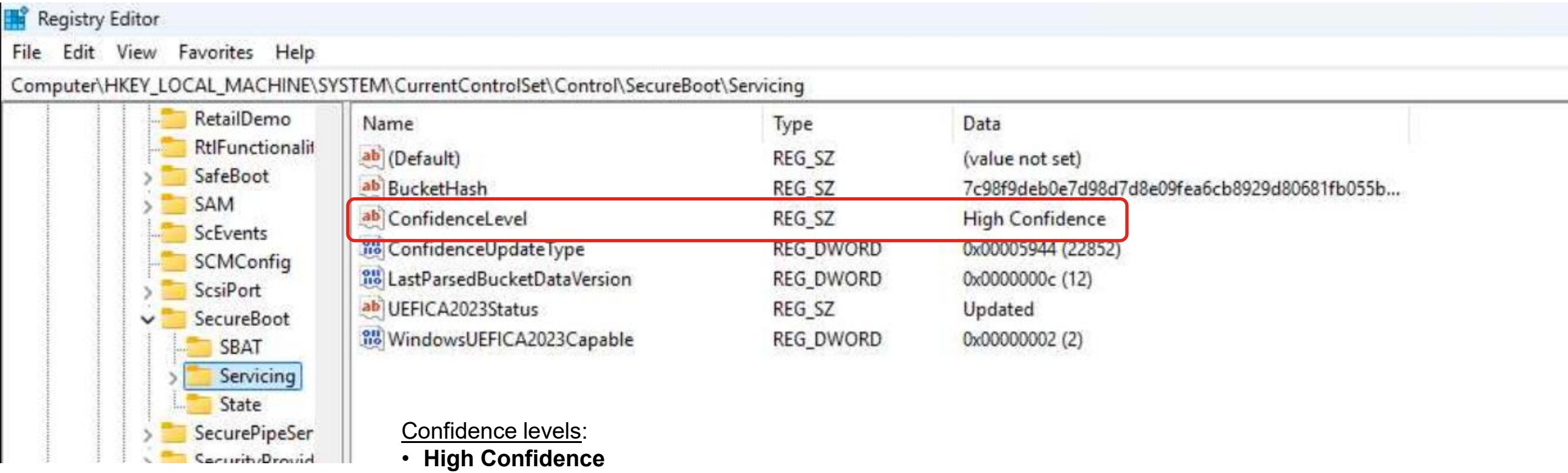
Device Bucket:

- OEMModelSystemFamily: ThinkSmart Core Gen 2
- OEMModelBaseBoard: 3360
- OEMModelBaseBoardVersion: SEK1H03537 IOT 4362202012478
- OEMModelSKU: LENOVO_MT_12WC_BU_Think_FM_ThinkSmart Core Gen 2
- OEMModelNumber: 12WC0001GR
- OEMModelSystemVersion: ThinkSmart Core Gen 2
- FirmwareVersion: M5JKT17A



- MTR on Windows have Windows Telemetry enabled by default (Required+Optional)
- Nevertheless, telemetry URLs may be blocked in enterprise environments
- So, despite the current High Confidence Buckets already contain several ThinkSmart devices, it's NOT guaranteed that ALL ThinkSmart devices will be placed in a High Confidence Bucket

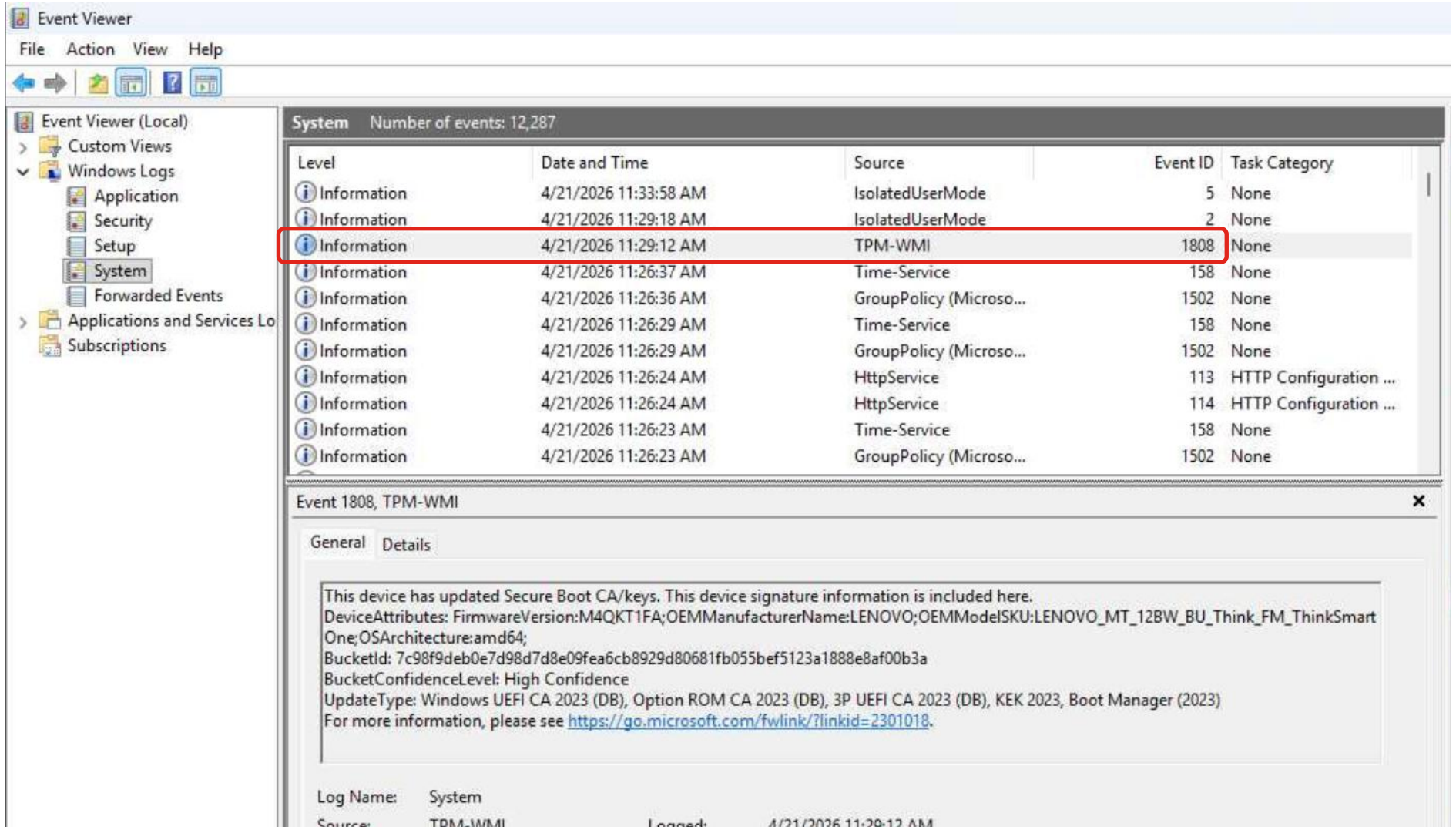
How to monitor High Confidence automatic updates



Confidence levels:

- **High Confidence**
- **Temporarily Paused**: affected by a known issue (Microsoft and partners working on a fix). This may require a firmware update.
- **Not Supported - Known Limitation**: no support for the automated Secure Boot certificate update path due to hardware or firmware limitations.
- **Under Observation - More Data Needed**: Secure Boot certificate updates may be deferred until sufficient data is available.
- **No Data Observed - Action Required**: administrator action is likely required.

How to monitor High Confidence automatic updates

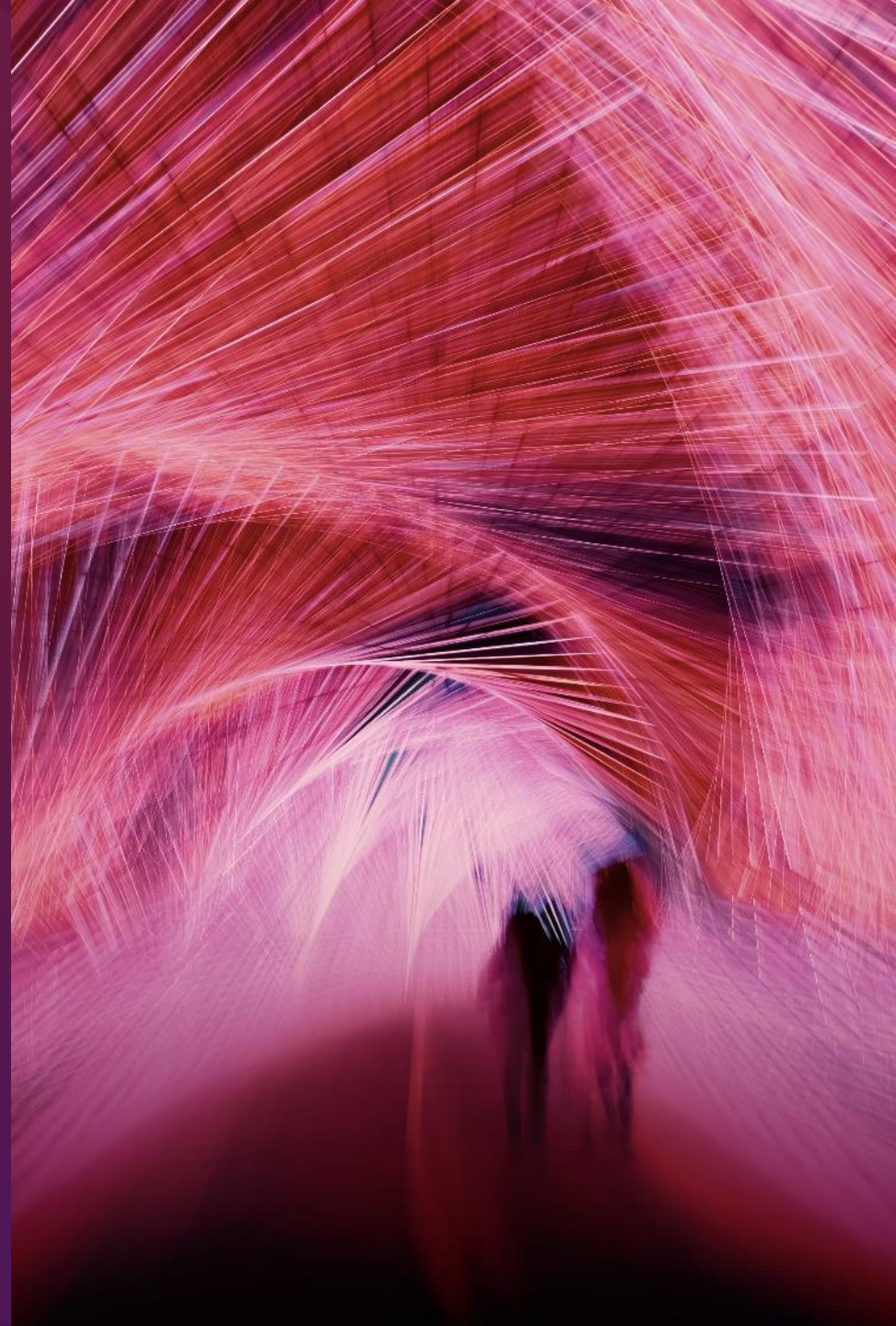


How to monitor updates

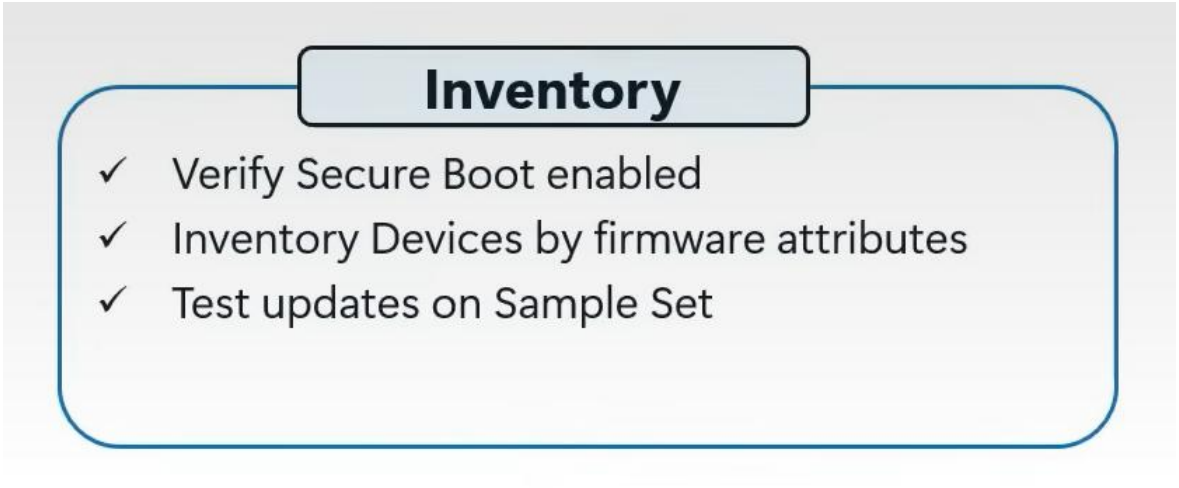
Windows Event Logs: Windows > System > TPM-WMI

Event ID	Description and Action
1801	**The device has not yet been updated with the Secure Boot certificates and/or the boot manager** ***Action:*** **begin deployment of the Secure Boot updates via one of the solution pathways**
1808	**The device has been updated with the Secure Boot certificates and the boot manager** ***Action:*** **no further action is required**
1795	Windows encountered an error applying the Secure Boot certificate updates or the CA2023-signed boot manager *Action:* organizations should check if firmware updates are available
1802	Windows has blocked the updates due to a known hardware or firmware issue preventing a safe update *Action:* organizations should check with the device manufacturer for the status of a KEK update.
1803	Windows does not have a KEK update for this device *Action:* organizations should check with the device manufacturer for the status of a KEK update.

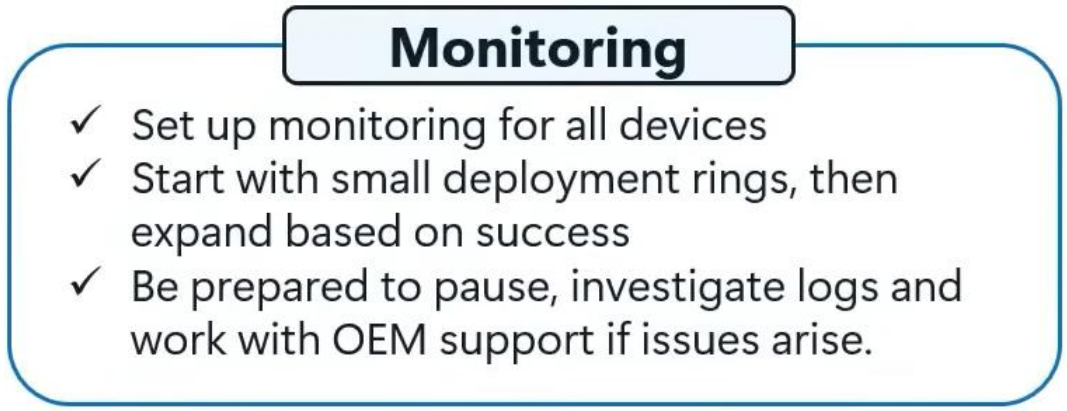
Call To Action



What if my ThinkSmart device is not in High Confidence Bucket?



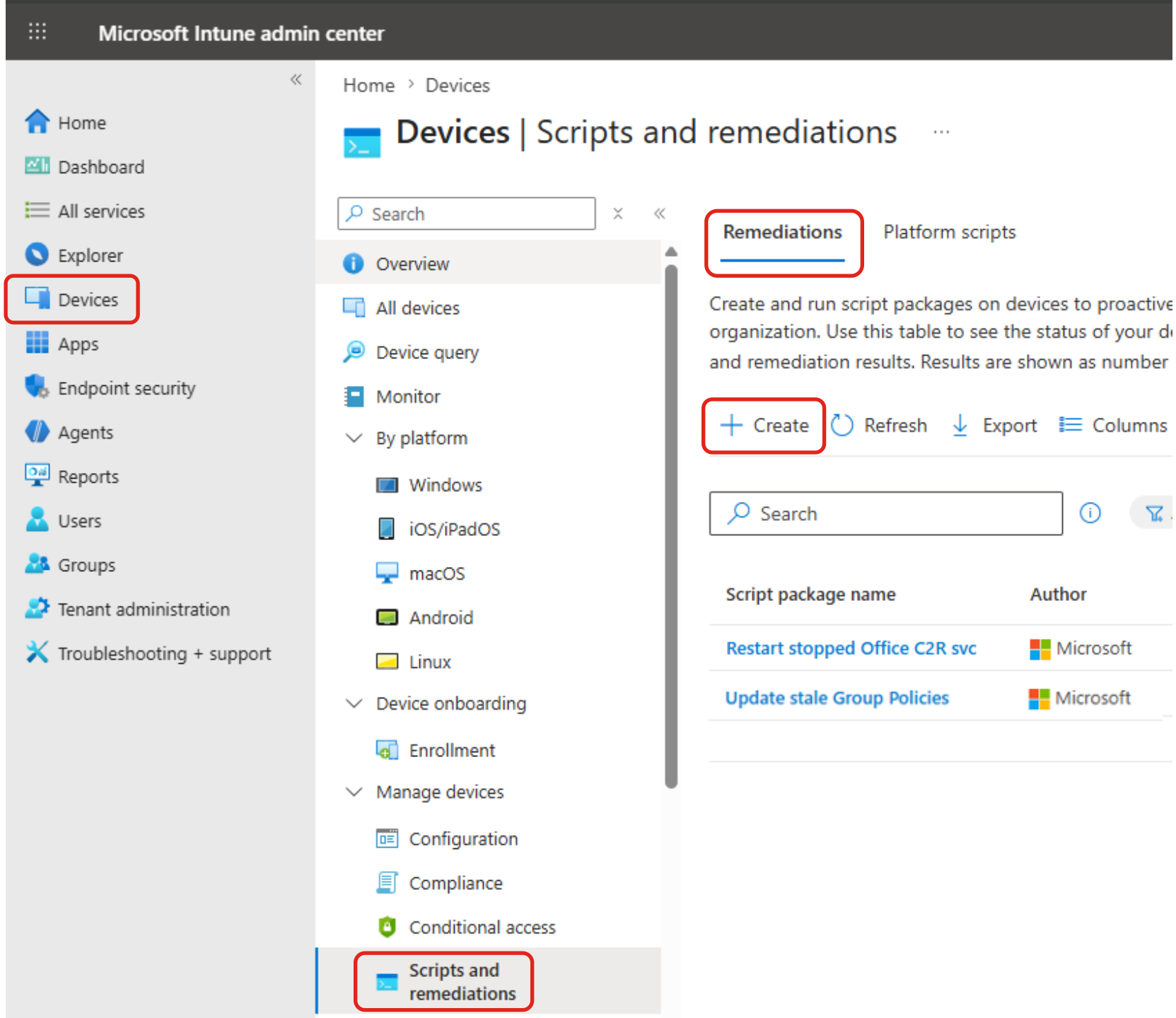
Microsoft Intune Remediation and other monitoring methods are described at aka.ms/getsecureboot



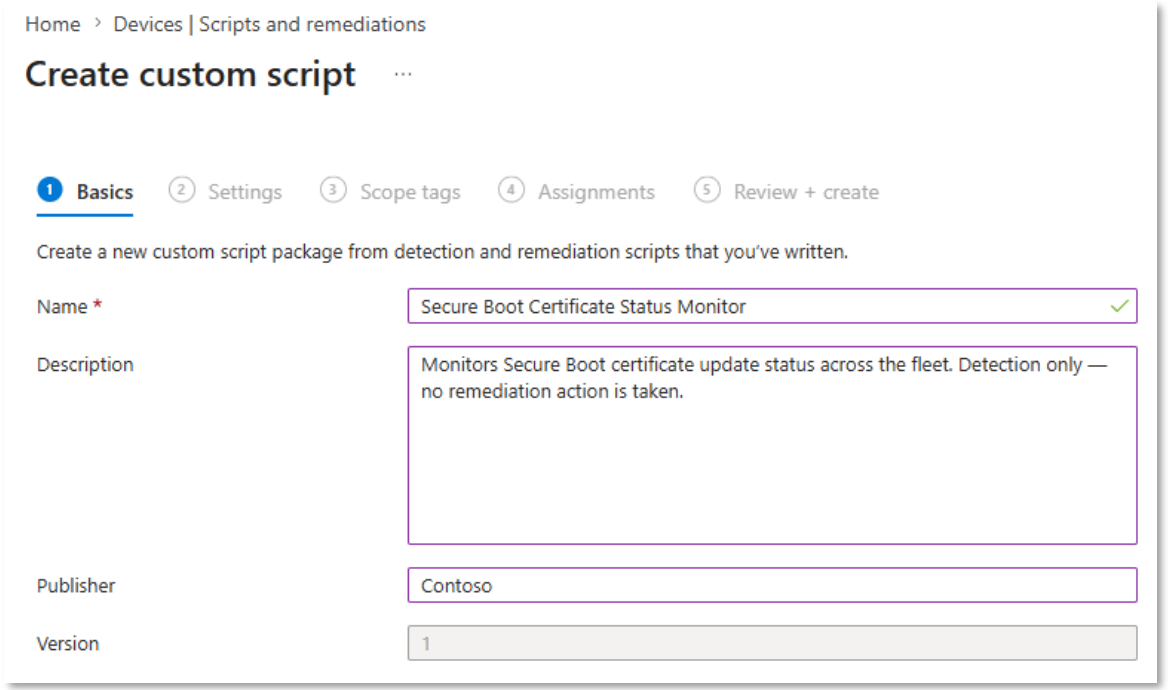
Inventory: Intune Remediation

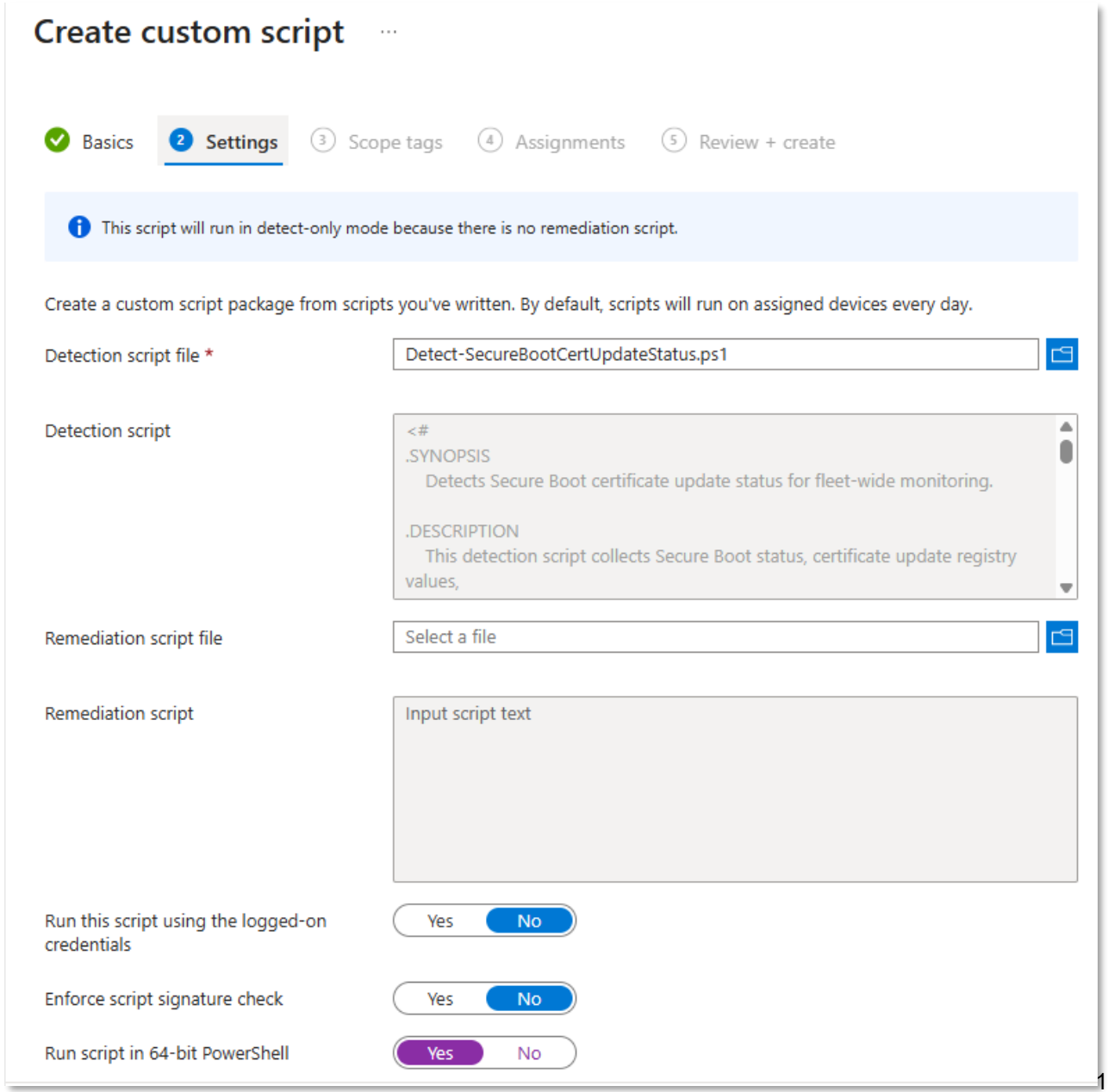
- Monitoring-only (no actual remediation action is taken on devices)
- Based on a detection script (powershell) that collects Secure Boot and certificate status from each device and reports it back to the Intune portal
- This gives administrators a centralized, exportable view of certificate update progress across their Intune enrolled Windows devices.
- Reference: https://support.microsoft.com/en-au/topic/monitoring-secure-boot-certificate-status-with-microsoft-intune-remediations-6696a27b-fa09-4570-b112-124965adc87f

Inventory: Intune Remediation

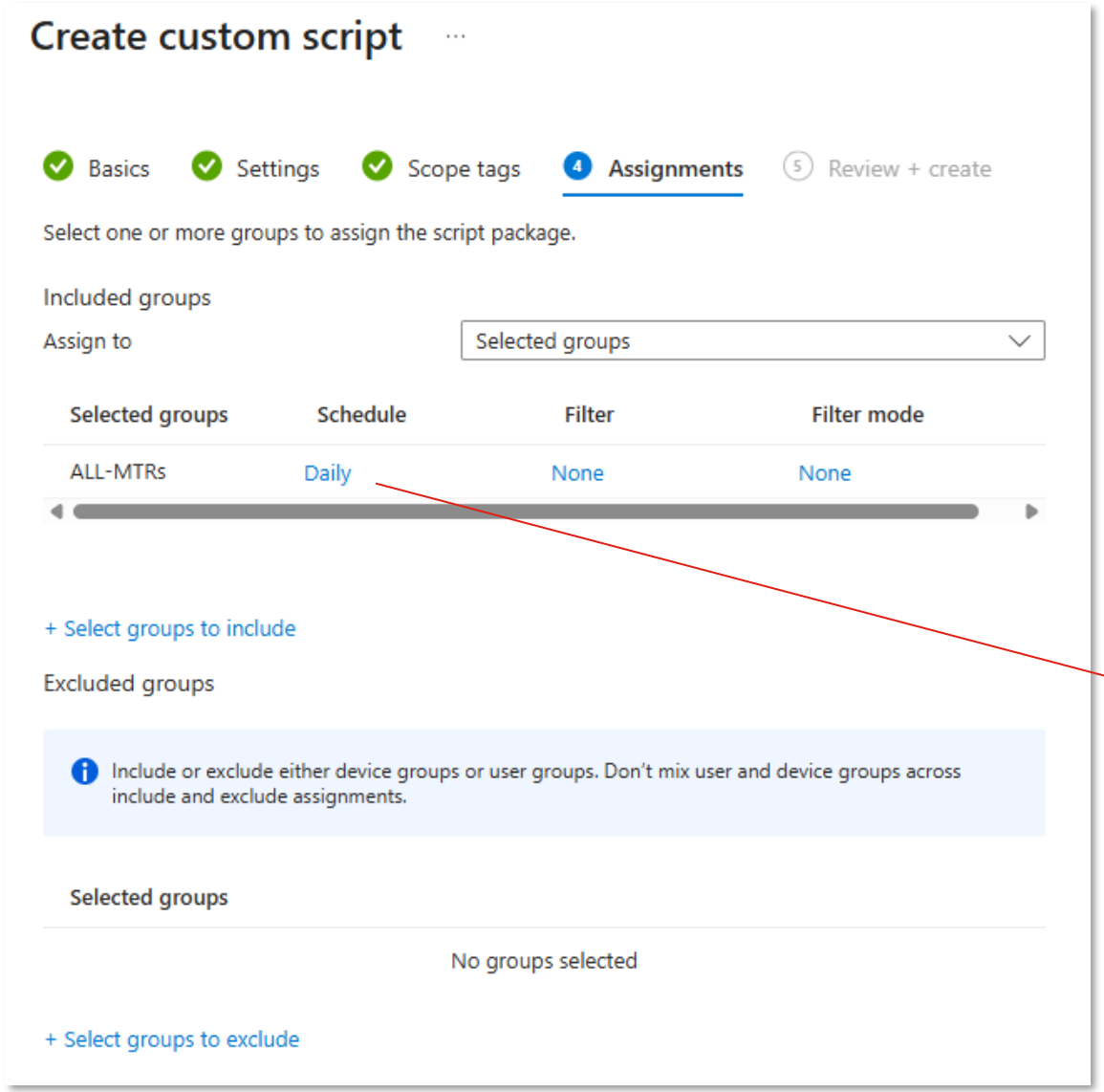


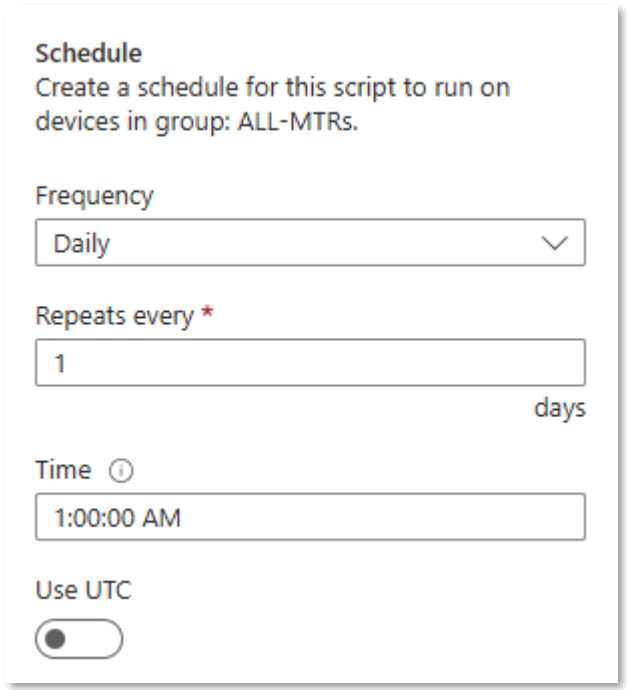
Inventory: Intune Remediation



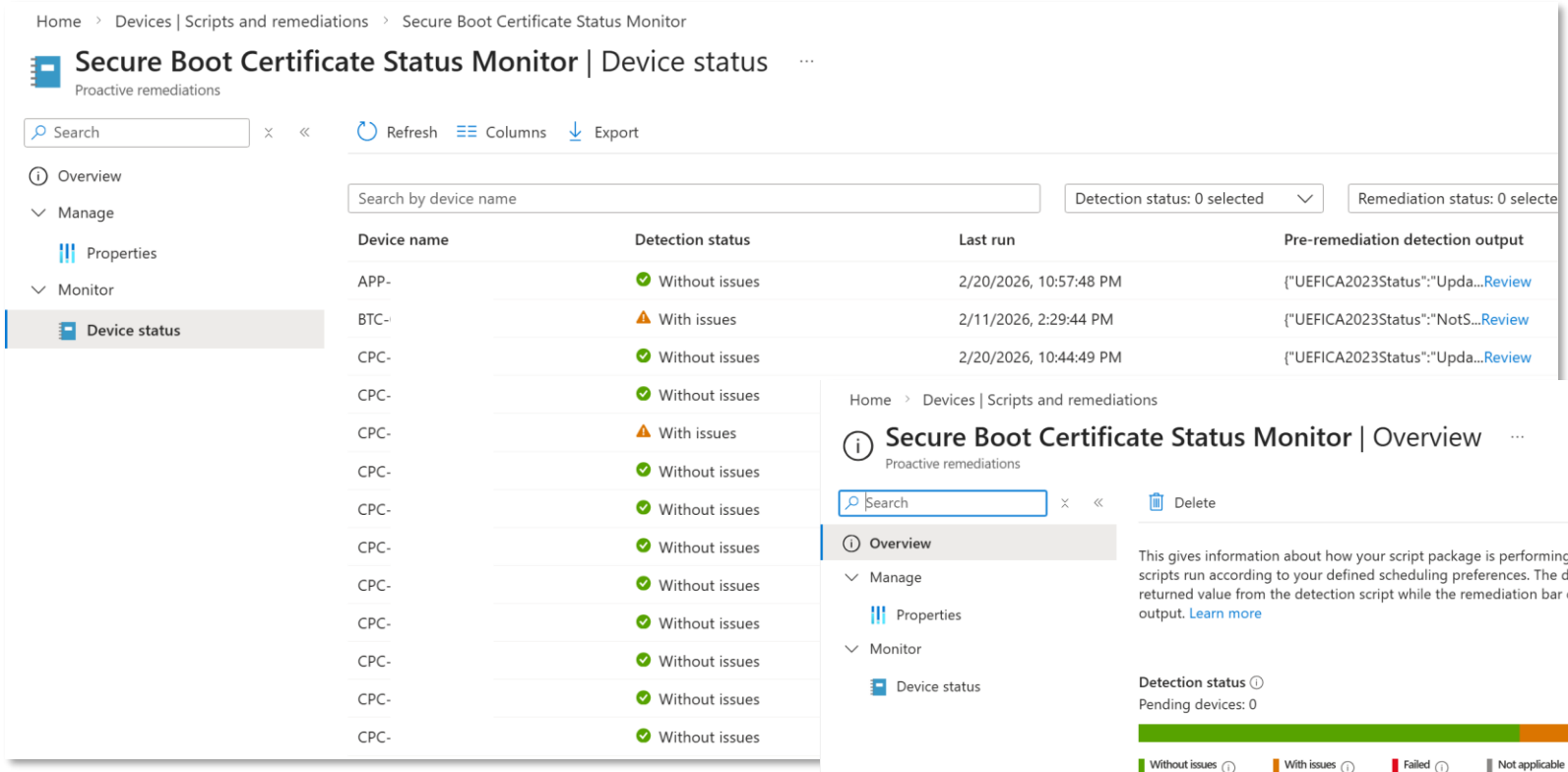


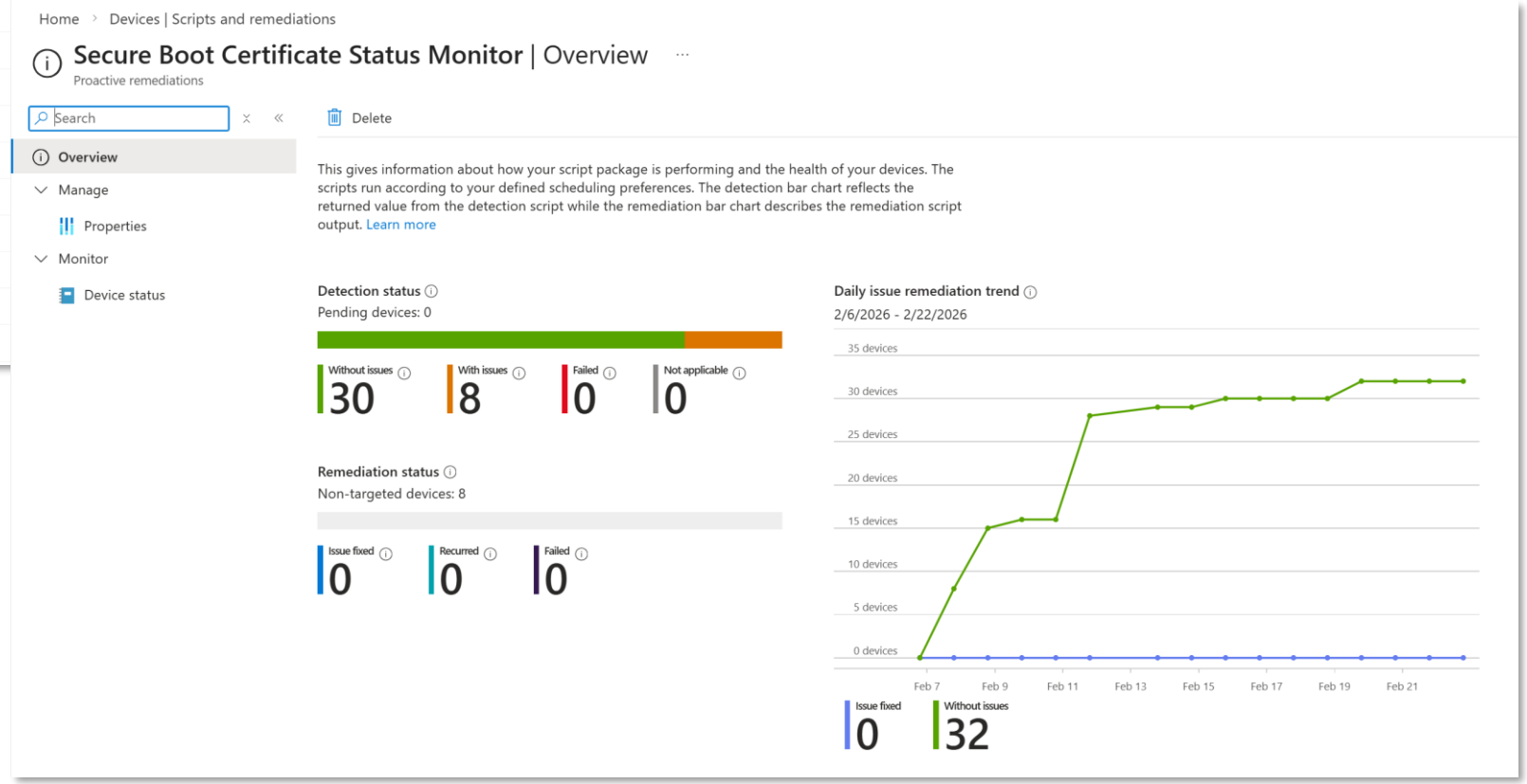
Inventory: Intune Remediation





Inventory: Intune Remediation





What if my ThinkSmart device is not in High Confidence Bucket?

olSet\Control\SecureBoot\Servicing

Name	Type	Data
(Default)	REG_SZ	(value not set)
BucketHash	REG_SZ	2c63ddd06abcbfe363694ccd7a88ca55ef177d75b5...
ConfidenceLevel	REG_SZ	Under Observation - More Data Needed

Microsoft is asking the customer (or managing partner) to test first

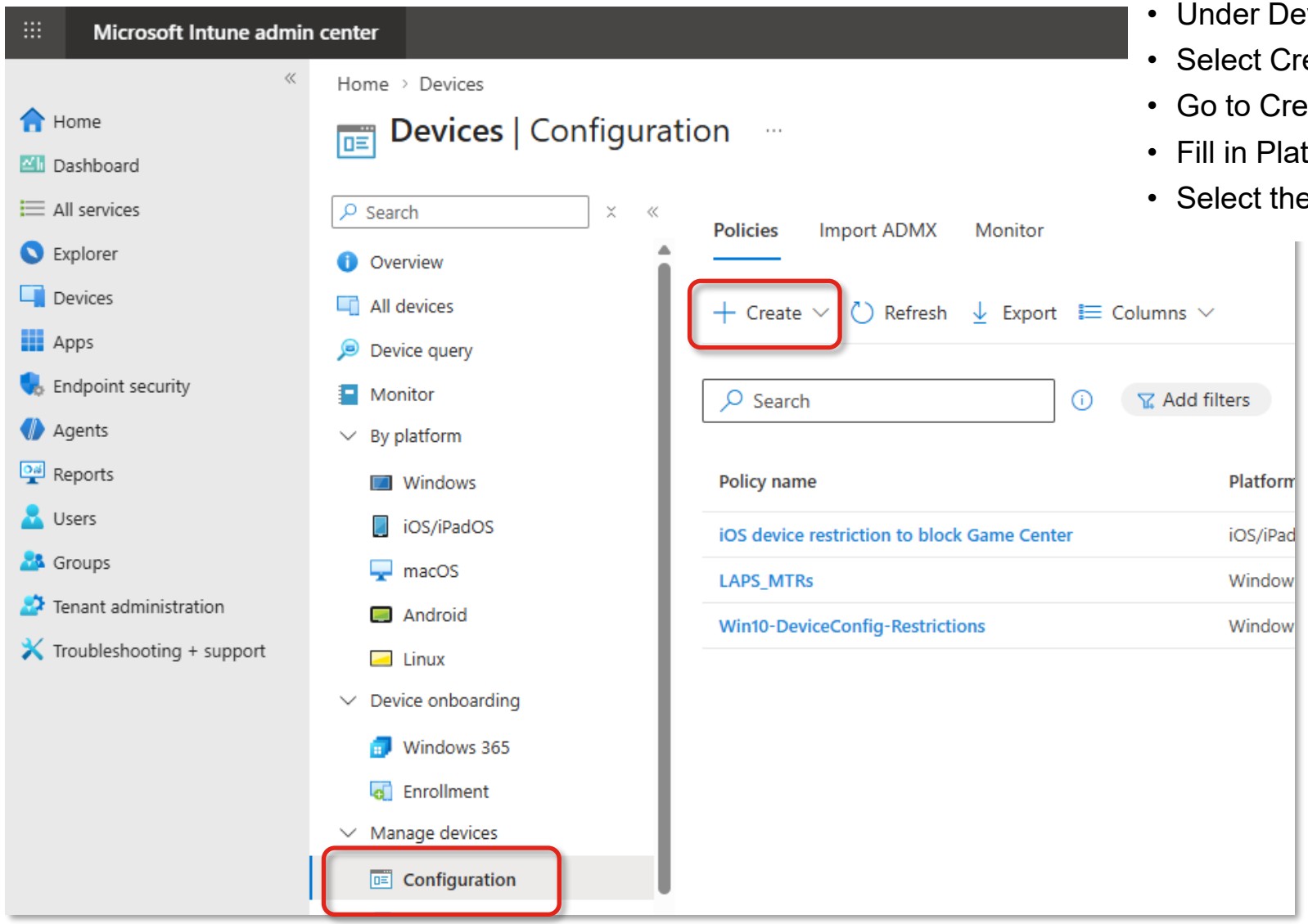
How to trigger updates on a selected device subgroup

This is the most typical scenario: a MTRoW is enrolled in Intune

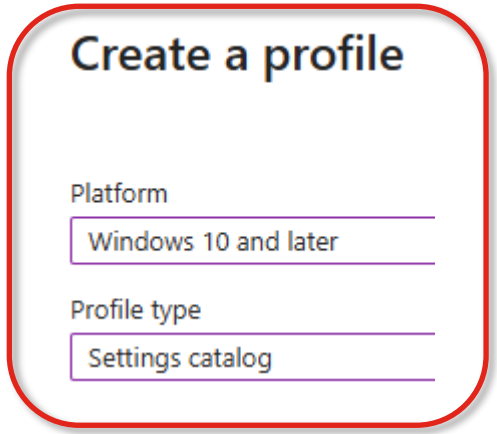
- Please note that devices deployed through MTR Autopilot with Autologin are always enrolled in Intune

Actions required are documented by Microsoft @ https://support.microsoft.com/en-us/topic/microsoft-intune-method-of-secure-boot-for-windows-devices-with-it-managed-updates-1c4cf9a3-8983-40c8-924f-44d9c959889d

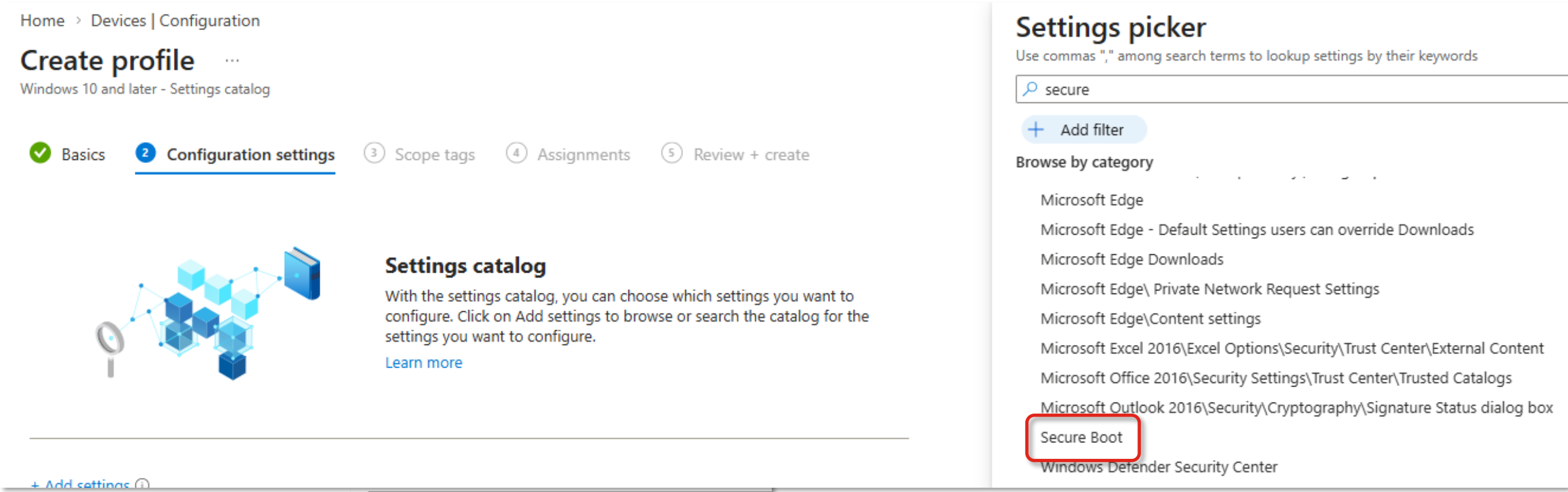
Required Intune Settings

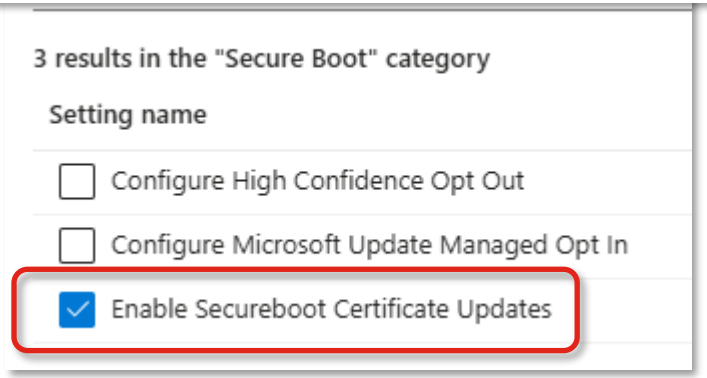


- Under Devices > Manage devices, select Configuration
- Select Create and select New Policy
- Go to Create a profile in the right-hand pane
- Fill in Platform with Windows 10 and later
- Select the Settings Catalog under the Profile Type



Required Intune Settings





- Begin creating a profile by giving the profile a name.
- Under Configuration settings, select Add settings and use the Settings picker to find the Secure Boot settings by searching for Secure Boot
- Select Enable Secureboot Certificate Updates
- **Assign to a subset of test MTRs**

IT-managed Windows devices: Alternative methods to trigger updates (other than Intune Settings)

Avoid mixing methods on the same device

1. **Registry keys:**

   There is one essential registry key available for triggering the deployment of the certificates:

   reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Secureboot /v AvailableUpdates /t REG_DWORD /d 0x**5944** /f

   The registry keys under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing can be used to monitor the deployment status based on the rules defined at https://support.microsoft.com/en-us/topic/registry-key-updates-for-secure-boot-windows-devices-with-it-managed-updates-a7be69c9-4634-42e1-9ca1-df06f43f360d#bkmk_registry_keys

2. **Group Policy Objects (GPO):**

   Microsoft will be providing support for managing the Secure Boot updates using Group Policy in a future update. Note that since Group Policy is for settings, monitoring the device status will need to be done using alternate methods including monitoring registry keys and event log entries.

   https://support.microsoft.com/en-us/topic/group-policy-objects-gpo-method-of-secure-boot-for-windows-devices-with-it-managed-updates-65f716aa-2109-4c78-8b1f-036198dd5ce7

3. **WinCS (Windows Configuration System) CLI (for domain-joined clients):**

   Domain administrators can alternatively use the Windows Configuration System (WinCS) included in Windows OS updates to deploy the Secure Boot updates across domain-joined Windows clients and servers. It consists of a series of command-line utilities (both a traditional executable and a PowerShell module) to query and apply Secure Boot configurations locally to a machine.

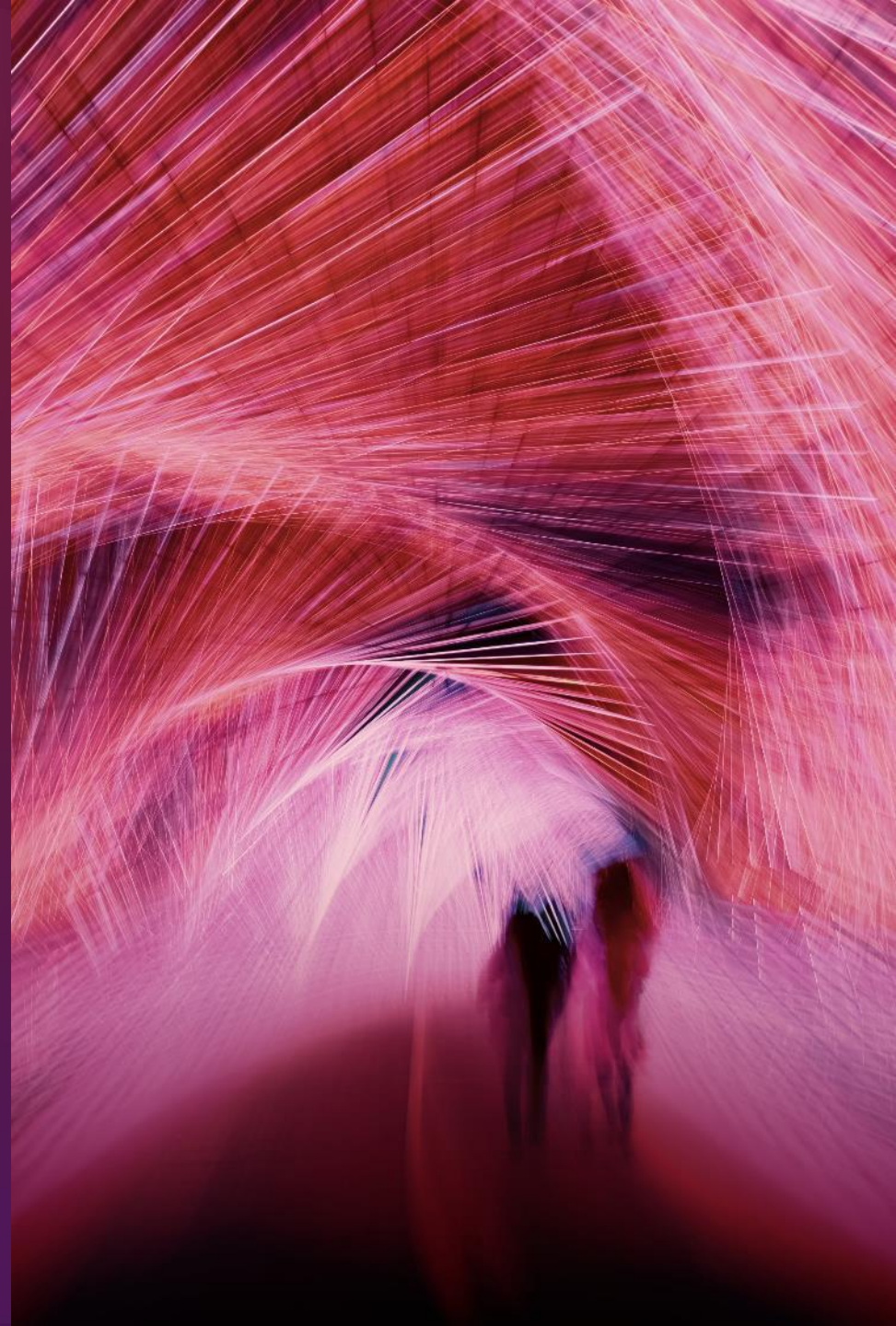
   https://support.microsoft.com/en-us/topic/windows-configuration-system-wincs-apis-for-secure-boot-d3e64aa0-6095-4f8a-b8e4-fbfda254a8fe

IT-managed Windows devices

- Organizations that have their own IT department managing Windows devices and updates
  - Organizations where any update rollout is controlled by IT who performs firmware testing, monitoring of updates, initiating deployment, and diagnosing issues
- In these cases, Microsoft expect IT department to initiate the update of the secure boot certificates. Customers should perform actions to explicitly trigger and activate the Secure Boot certificate and boot manager updates
- In practical terms, it means Microsoft Teams Room on Windows devices managed through IT management systems like **Intune, SCCM, WSUS, or similar**
  - Please note that in case organizations make use of the Microsoft Pro Management Portal (PMP) to control the roll out of updates through rings, by itself PMP is not enough to consider the MTRoW devices as “IT-managed”. Besides, PMP cannot be used to explicitly trigger and activate the Secure Boot certificate and boot manager updates

Secure Boot Cert Expiry

What If …



What If

In case the secure boot certificates are not updated:

- If the device reaches the expiration date without the new certificates, it will still start and operate normally. Device will still boot, because when UEFI validates a signature, it doesn't check the expiration date.
- In any case, for supported OS versions, the update could take place even after expiry (but pls be aware of security risks!)

However, there could be some scenarios where systems **will not boot**:

1
+ No new 2023 certificates (still 2011 certificates are active)
+ AND new Windows UEFI CA 2023 signed boot manager

This could happen with a recovery image which is using a 2023 boot manager

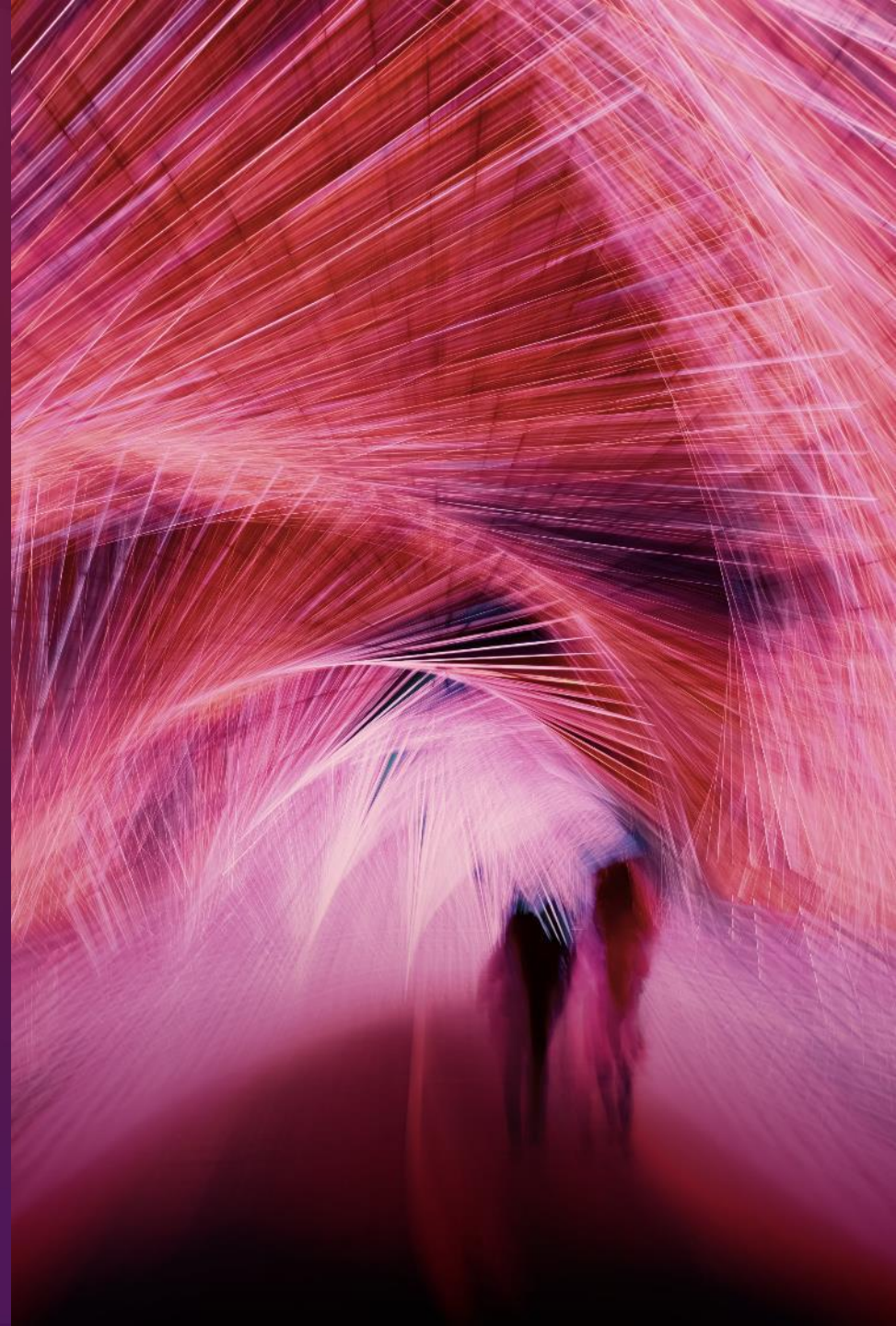
2
+ new 2023 certificates are active but no BIOS update to add 2023 certificates to default
+ AND new Windows UEFI CA 2023 signed boot manager
+ AND user resets the device (restored factory keys) or toggles secure boot off/on

Security and Compliance Risks

- Devices that haven’t received the newer 2023 certificates will continue to start and operate normally, and standard Windows updates will continue to install.
- 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, such as BitLocker hardening.

Note: Secure Boot should not be disabled to work around certificate expiration. Disabling Secure Boot significantly reduces device protection, removes safeguards against boot-level malware, and can create new security and compliance risks.

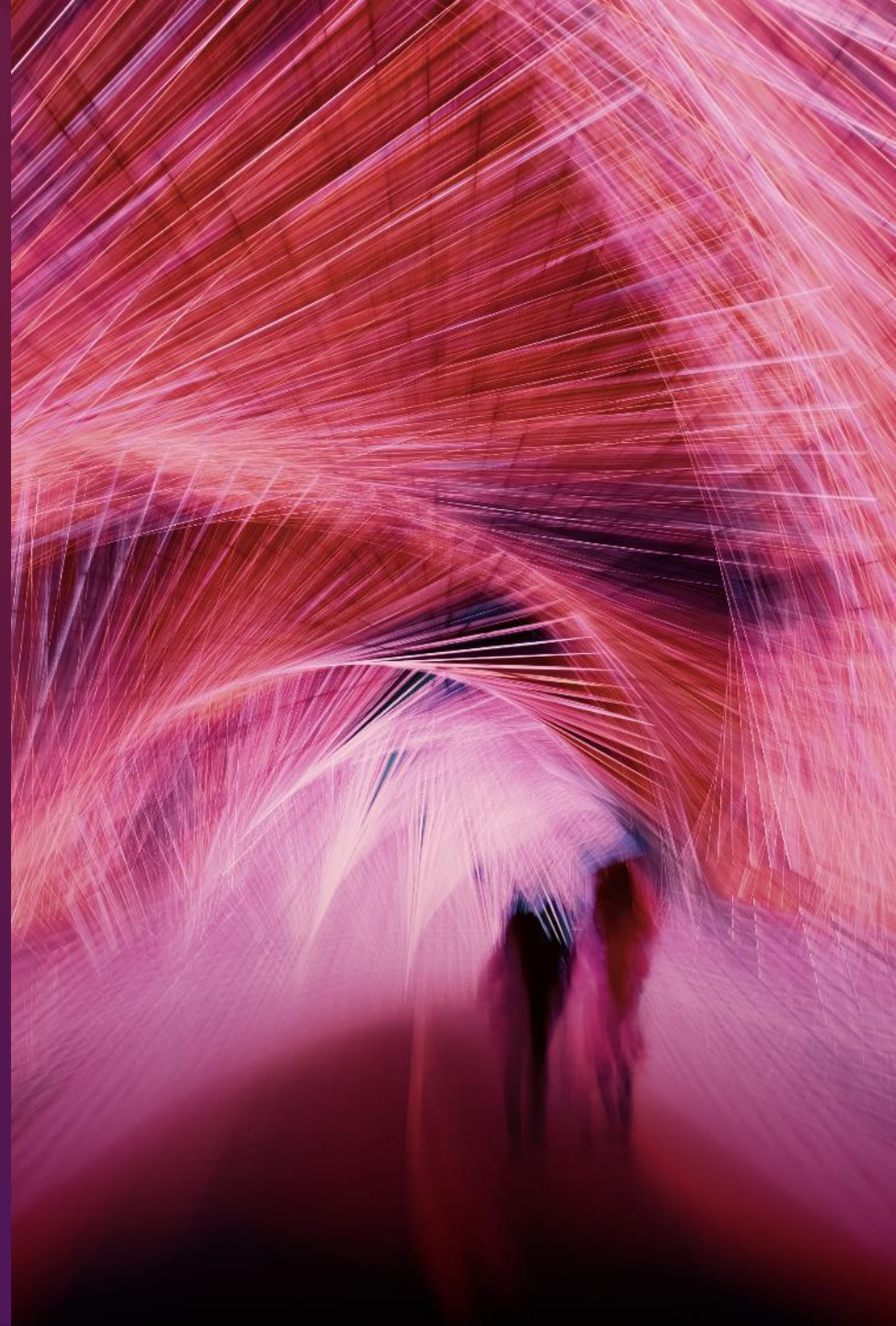
Revocation



Revocation of old certificates

- The final step of the overall process is the revocation of the old 2011 secure boot certificates.
- The revocation is performed by moving the 2011 certificates from the active DB to the DBX
- That move will be handled by Microsoft through Window Updates
- Microsoft has not yet indicated an exact date yet (for sure it will not be before end of 2026)
- Removal from default DB will be done by Lenovo via BIOS updates (through WU). Timing will depend on Microsoft revocation timing
- No customer action required

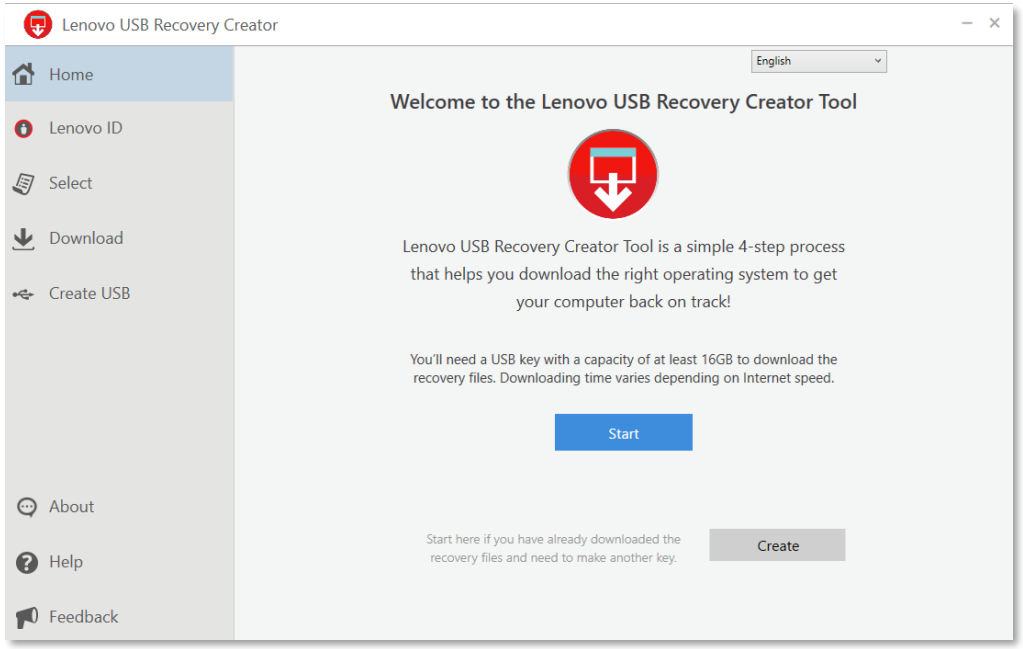
Recovery Images



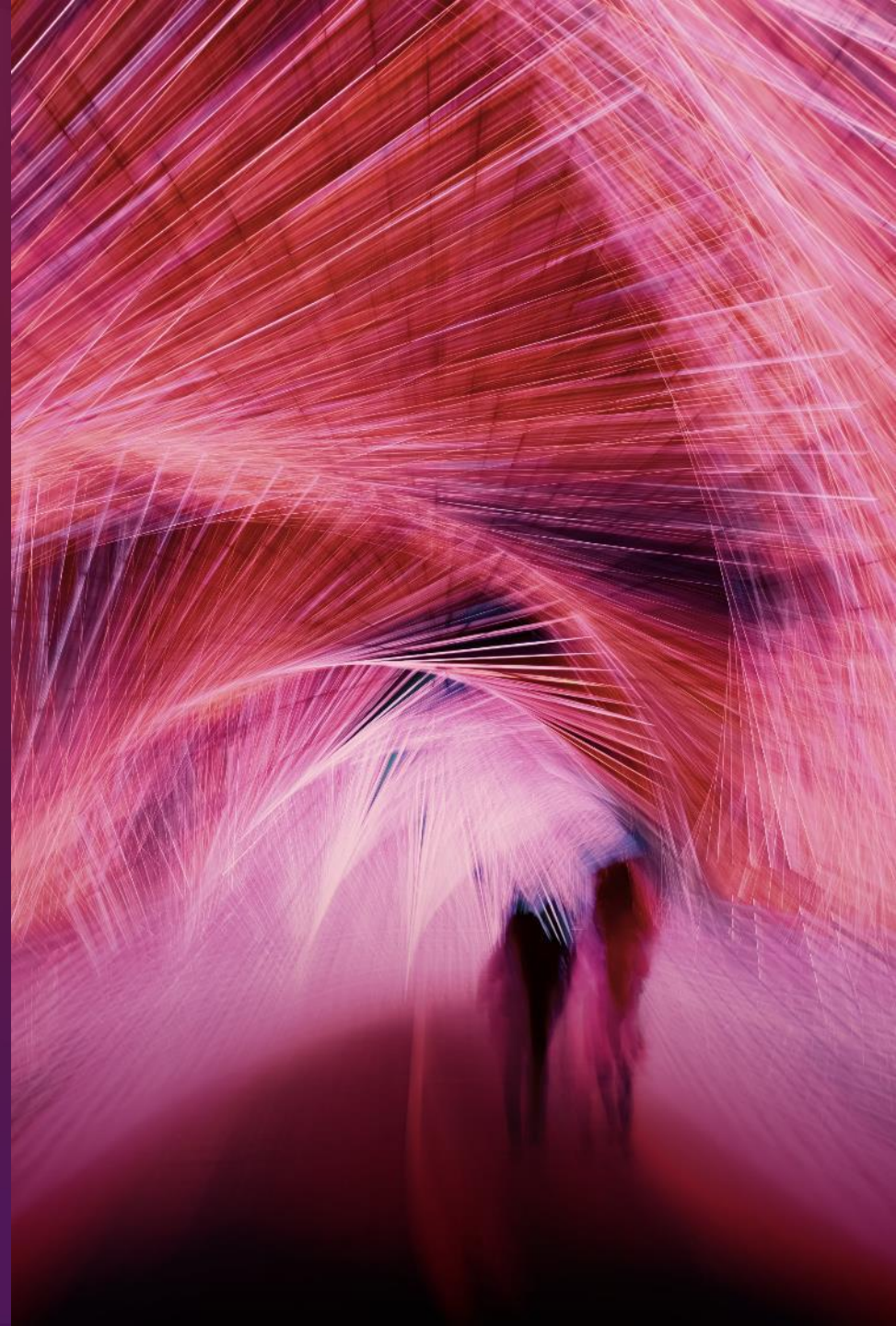
Recovery Images

- Nothing to worry about
- Until October all Lenovo recovery images (in either DDRS or LCD) will still have a boot loader signed by the 2011 certificates
- Those recovery images will stop working when Microsoft revokes the old certificates (move to DBX).
- Lenovo will start to replace the 2023 boot manager in all recovery images once Microsoft notifies timing of the revocation

- In parallel, Lenovo is preparing an update for the **USB Creator Tool** (available in the second half of 2026) that will allow the injection of the 2023 boot manager into the image (useful after the 2011 certs are revoked by Microsoft)



Special Cases



ThinkSmart Hub 500

- Remain on Windows 10 (not supported) and will not receive any certificate or boot manager update
- They will still boot but will run in a degraded protection status

ThinkSmart Edition Tiny M920q (Poly/Logitech)

- Despite they already reached End of Support, they will receive certificate and boot manager updates (on Windows 11)
- Lenovo has already delivered BIOS update with new certificates for default KEK/DB

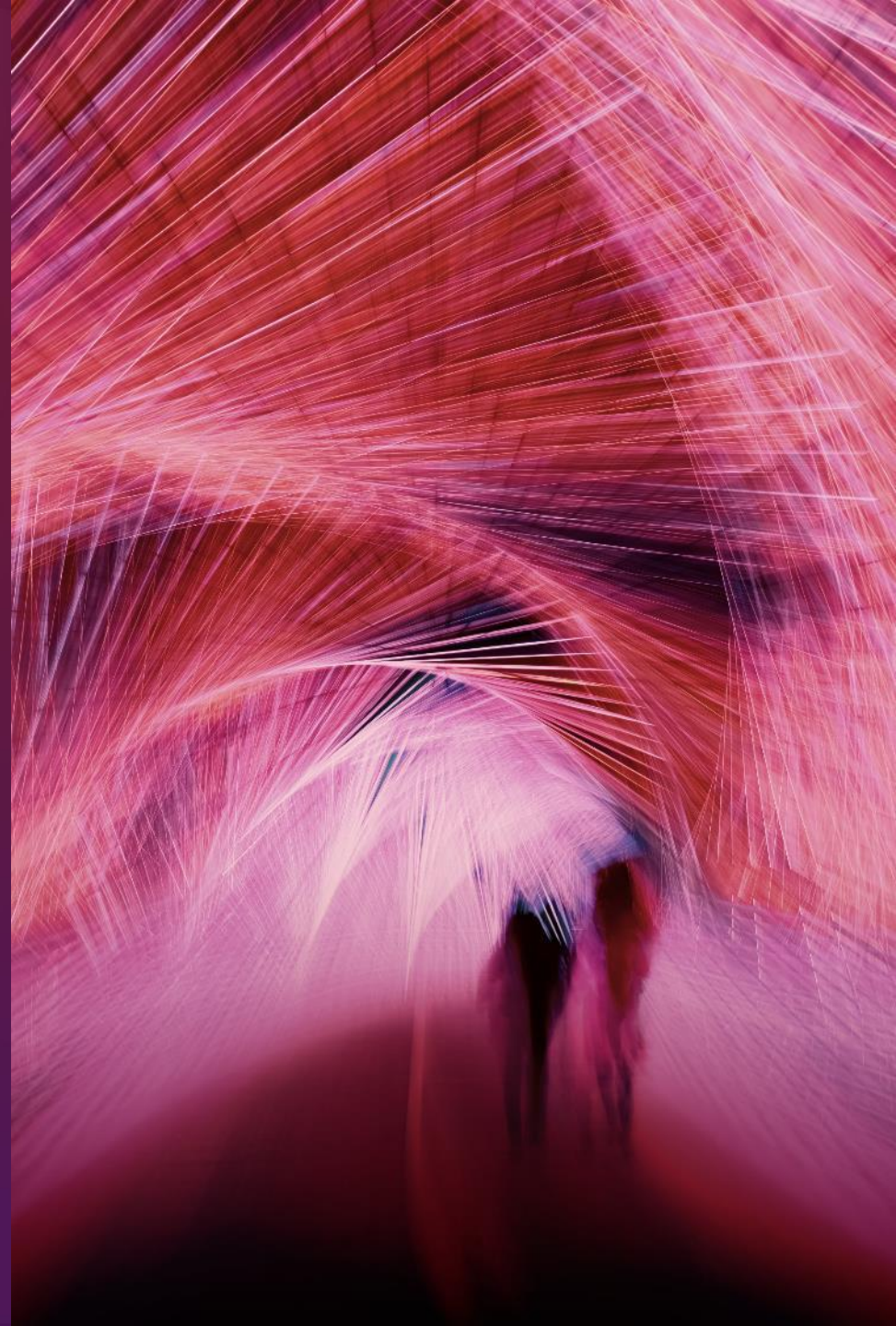
ThinkSmart Core for Logitech Out-Of-Warranty

- They will receive certificate and boot manager updates (on Windows 11) as per normal procedure
  - Remember that for Logi Core out-of-warranty, the official procedure for recovery is described at https://hub.sync.logitech.com/lenovo-thinksmart-teams?posts.view=lenovo+recovery (please note the post-install app at the bottom). Alternatively, the customer has the option to buy another 12 months of warranty for the Logi image at $10 per device. This will allow the access to Lenovo Cloud Deploy.

Secure Boot Cert Expiry

How to Monitor Update Progress

On a single device



How to verify installed secure boot certificates

Powershell as admin:

```
> Confirm-SecureBootUEFI
```

checking KEK

```
> [System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI
KEK).bytes) -match 'Microsoft Corporation KEK 2K CA 2023'
```

checking KEKdefault

```
> [System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI
KEKdefault).bytes) -match 'Microsoft Corporation KEK 2K CA 2023'
```

checking active db

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

checking default db

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

How to verify secure boot certificates: another method

Powershell as admin:

```
Install-Module -Name UEFIv2
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
Import-Module -Name UEFIv2
(Get-UEFISecureBootCerts KEK).signature
(Get-UEFISecureBootCerts db).signature

(Get-UEFISecureBootCerts KEKdefault).signature
(Get-UEFISecureBootCerts dbdefault).signature
```

ThinkSmart Hub (in-service): new certs in default KEK/DB

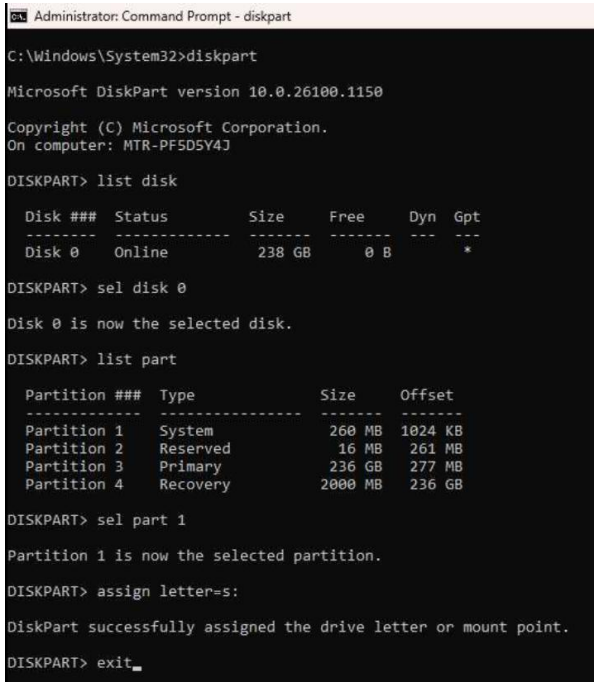
```
PS C:\WINDOWS\system32> (Get-UEFISecureBootCerts KEK).signature

Thumbprint                                Subject
----------                                -------
8393B27510558F5617CAA94F1D7F3C394F31958B  CN=LENOVO
31590BFD89C9D74ED087DFAC66334B3931254B30  CN=Microsoft Corporation KEK CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US


PS C:\WINDOWS\system32> (Get-UEFISecureBootCerts KEKdefault).signature

Thumbprint                                Subject
----------                                -------
8393B27510558F5617CAA94F1D7F3C394F31958B  CN=LENOVO
459AB6FB5E284D272D5E3E6ABC8ED663829D632B  CN=Microsoft Corporation KEK 2K CA 2023, O=Microsoft Corporation, C=US
31590BFD89C9D74ED087DFAC66334B3931254B30  CN=Microsoft Corporation KEK CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US


PS C:\WINDOWS\system32> (Get-UEFISecureBootCerts DB).signature

Thumbprint                                Subject
----------                                -------
CB0259714826C867D1422C310B88150160398F0B  CN=Lenovo UEFI CA 2014, O=Lenovo, S=North Carolina, C=US
D0B089CE2F5B4DFEFDA59940F7FD852B2CB2A6CB  CN=Trust - Lenovo Certificate
46DEF63B5CE61CF8BA0DE2E6639C1019D0ED14F3  CN=Microsoft Corporation UEFI CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
580A6F4CC4E4B669B9EBDC1B2B3E087B80D0678D  CN=Microsoft Windows Production PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US


PS C:\WINDOWS\system32> (Get-UEFISecureBootCerts DBdefault).signature

Thumbprint                                Subject
----------                                -------
CB0259714826C867D1422C310B88150160398F0B  CN=Lenovo UEFI CA 2014, O=Lenovo, S=North Carolina, C=US
D0B089CE2F5B4DFEFDA59940F7FD852B2CB2A6CB  CN=Trust - Lenovo Certificate
3FB39E2B8BD183BF9E4594E72183CA60AFCD4277  CN=Microsoft Option ROM UEFI CA 2023, O=Microsoft Corporation, C=US
B5EEB4A6706048073F0ED296E7F580A790B59EAA  CN=Microsoft UEFI CA 2023, O=Microsoft Corporation, C=US
45A0FA32604773C82433C3B7D59E7466B3AC0C67  CN=Windows UEFI CA 2023, O=Microsoft Corporation, C=US
46DEF63B5CE61CF8BA0DE2E6639C1019D0ED14F3  CN=Microsoft Corporation UEFI CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
580A6F4CC4E4B669B9EBDC1B2B3E087B80D0678D  CN=Microsoft Windows Production PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
```

ThinkSmart Core Gen2 (new): new certs in active KEK/DB

```
PS C:\WINDOWS\system32> (Get-UEFISecureBootCerts KEK).signature

Thumbprint                                Subject
----------                                -------
459AB6FB5E284D272D5E3E6ABC8ED663829D632B  CN=Microsoft Corporation KEK 2K CA 2023, O=Microsoft Corporation, C=US
8393B27510558F5617CAA94F1D7F3C394F31958B  CN=LENOVO
31590BFD89C9D74ED087DFAC66334B3931254B30  CN=Microsoft Corporation KEK CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US


PS C:\WINDOWS\system32> (Get-UEFISecureBootCerts KEKdefault).signature

Thumbprint                                Subject
----------                                -------
8393B27510558F5617CAA94F1D7F3C394F31958B  CN=LENOVO
31590BFD89C9D74ED087DFAC66334B3931254B30  CN=Microsoft Corporation KEK CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
459AB6FB5E284D272D5E3E6ABC8ED663829D632B  CN=Microsoft Corporation KEK 2K CA 2023, O=Microsoft Corporation, C=US


PS C:\WINDOWS\system32> (Get-UEFISecureBootCerts DB).signature

Thumbprint                                Subject
----------                                -------
45A0FA32604773C82433C3B7D59E7466B3AC0C67  CN=Windows UEFI CA 2023, O=Microsoft Corporation, C=US
CB0259714826C867D1422C310B88150160398F0B  CN=Lenovo UEFI CA 2014, O=Lenovo, S=North Carolina, C=US
D0B089CE2F5B4DFEFDA59940F7FD852B2CB2A6CB  CN=Trust - Lenovo Certificate
46DEF63B5CE61CF8BA0DE2E6639C1019D0ED14F3  CN=Microsoft Corporation UEFI CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
580A6F4CC4E4B669B9EBDC1B2B3E087B80D0678D  CN=Microsoft Windows Production PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US


PS C:\WINDOWS\system32> (Get-UEFISecureBootCerts DBdefault).signature

Thumbprint                                Subject
----------                                -------
CB0259714826C867D1422C310B88150160398F0B  CN=Lenovo UEFI CA 2014, O=Lenovo, S=North Carolina, C=US
D0B089CE2F5B4DFEFDA59940F7FD852B2CB2A6CB  CN=Trust - Lenovo Certificate
3FB39E2B8BD183BF9E4594E72183CA60AFCD4277  CN=Microsoft Option ROM UEFI CA 2023, O=Microsoft Corporation, C=US
B5EEB4A6706048073F0ED296E7F580A790B59EAA  CN=Microsoft UEFI CA 2023, O=Microsoft Corporation, C=US
45A0FA32604773C82433C3B7D59E7466B3AC0C67  CN=Windows UEFI CA 2023, O=Microsoft Corporation, C=US
46DEF63B5CE61CF8BA0DE2E6639C1019D0ED14F3  CN=Microsoft Corporation UEFI CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
580A6F4CC4E4B669B9EBDC1B2B3E087B80D0678D  CN=Microsoft Windows Production PCA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
```

How to verify digital signature of Boot Loader

First the EFI partition has to be mounted:



Elevated CMD:

```
diskpart
>list disk
>sel disk 0
>list part
>sel part 1
>assign letter=s:
>exit
```

Then digital signature check on the following files:

```
\EFI\Microsoft\Boot\bootmgfw.efi
\EFI\Boot\bootx64.efi
```

Elevated Powershell:

```
Get-PfxCertificate –FilePath "S:\EFI\Microsoft\Boot\bootmgfw.efi" | Select-Object Subject,
Issuer, Thumbprint, NotBefore, NotAfter

Get-PfxCertificate –FilePath "S:\EFI\Boot\bootx64.efi" | Select-Object Subject, Issuer,
Thumbprint, NotBefore, NotAfter
```

Monitoring the process through EventLogs and RegKeys

- The text value of the **UEFICA2023Status** registry key will indicate if your certificate deployment status is not started, in progress, or updated. The value will change progressively until all new certificates and the new boot manager have been deployed successfully.
- Audit the Windows System Event Log events for **Event ID 1808** (source: TPM-WMI)
    - This informational event indicates that the device has the required new Secure Boot certificates applied to the device's firmware.
- Check that the text value of the **UEFICA2023Status** registry key reads as "Updated."

Errors during deployment

- Audit the Windows System Event Log for **Event ID 1801** (source: TPM-WMI)
    - This error event indicates that the updated certificates have not been applied to the device.
- Audit the **UEFICA2023Error** registry key for issues.
    - This key should not exist unless an error is pending. The error itself won't appear in the Event Log.

Smarter technology for all

Lenovo

thanks.