Lenovo

Secure Boot CA 2023 Guide for Azure Local and Windows Server

Last update: **May 2026**

Version 1.0

Provides guidance for transitioning Lenovo Windows Server environments to Secure Boot CA 2023

Helps maintain system security and boot integrity through the certificate transition

Outlines required firmware and operating system updates across supported deployment scenarios

Documents recovery actions to address common transition-related failures

Andreína Vivas Thomas
Gary Cudak
Ron Arndt
Guiqing Li

LENOVO PRESS

Abstract

This document provides guidance for Lenovo customers to transition Windows Server and Azure Local environments from Microsoft Secure Boot Certificate Authority (CA) 2011 to CA 2023 to maintain system security and boot integrity as CA 2011 certificates approach expiration in June 2026.

Procedures are outlined for validating the presence and activation of CA 2023 certificates within system firmware and operating system components, including minimum Lenovo UEFI firmware levels and required servicing updates.

Deployment-specific guidance spans existing environments, new installations, and Azure Local solutions, with additional coverage of recovery procedures for common failure conditions such as Secure Boot violations, recovery media incompatibility, and loss of custom Secure Boot keys.

Contents

Introduction

A basic understanding of the Secure Boot trust chain is assumed in this document. The trust chain is explained in detail in the following Microsoft Support announcement: Windows Secure Boot certificate expiration and CA updates.

Instructions are provided in this document for Lenovo Windows Server and Azure Local customers so that environments may be kept secure with respect to the Secure Boot certificate transition. The CA (Certificate Authority) 2011 certificates will expire in June 2026* and, to accommodate this transition, Lenovo UEFI/BIOS firmware has been updated to include the new CA 2023 certificates (see the Minimum Lenovo UEFI builds that automatically include Microsoft Secure Boot CA 2023 certificates). However, every Lenovo customer is expected to verify that the environment has correctly ingested and applied all CA 2023 certificates.

***Reminder**: Customers have been given a grace period until October 2026 to transition from CA 2011 certificates to CA 2023 certificates, ensuring they can maintain their Secure Boot postures before CA 2011 certificates are officially revoked by Microsoft.

Check Which Certificates Are Installed

A group of keys is included in the Secure Boot trust chain. Those keys work in conjunction to establish the security baseline for a system at boot time. The Microsoft CA 2023 certificates and their respective purpose for guaranteeing the complete Secure Boot trust chain (now that CA 2011 is sunsetting) are shown in the following table:

Table 1: Microsoft CA 2023 certificate set

Full Certificate Name	Purpose
Microsoft Corporation KEK 2K CA 2023	Key Exchange Key (KEK) that authorizes changes to db (Signature Database or allow list) and dbx (Revoked Signature Database or deny list) with a 2048-bit (2K) RSA cryptographic key
Windows UEFI CA 2023	Certificate Authority (CA) that signs the Windows boot loader
Microsoft UEFI CA 2023	Certificate Authority (CA) that signs third-party boot loaders and EFI applications
Microsoft Option ROM UEFI CA 2023*	Certificate Authority (CA) that signs option ROMs (Read-Only Memory), which contains pre-boot firmware for hardware components

*All certificates except for Microsoft Option ROM UEFI CA 2023 have been incorporated into all Lenovo UEFI firmware for all platforms certified for Windows Server since 2025. Adoption of the Option ROM CA 2023 is delayed, and publication into Lenovo UEFI firmware will be completed by June 2026.

A server is considered properly secured by CA 2023 when the Microsoft Corporation KEK 2K CA 2023 has been added to KEK and both Windows UEFI CA 2023 and Microsoft UEFI CA 2023 are present in db.

Either of the following methods can be used to check which certificates are installed in each system.

Via PowerShell

If a Windows Server operating system has already been installed in the environment, the PowerShell module UEFIv2 can be used to check for installed Secure Boot certificates. The execution policy may need to be changed if the UEFIv2 PS module has not already been installed.

Figure 1: PowerShell script to check for installed Secure Boot certificates

```
Install-Module -Name UEFIv2 # download module bits onto the machine
$currentPolicy = Get-ExecutionPolicy # save execution policy to restore to later
if ($currentPolicy -ne 'RemoteSigned') {
    Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser -Force # `
    adjust execution policy if necessary to allow module to run in the next step
}
Import-Module -Name UEFIv2 # run module within this shell
(Get-UEFISecureBootCerts pk).signature # Platform Key, which controls KEKs
(Get-UEFISecureBootCerts kek).signature # Key Exchange Keys, which control db/dbx
(Get-UEFISecureBootCerts db).signature # active signature database, which is `
currently being enforced
(Get-UEFISecureBootCerts dbdefault).signature # back-up signature database to which `
db is restored when resetting to factory settings
if ((Get-ExecutionPolicy) -ne $currentPolicy) {
    Set-ExecutionPolicy -ExecutionPolicy $currentPolicy -Scope CurrentUser -Force # `
restore execution policy if it was changed
}
```

An environment is considered properly secured by CA 2023 when the Microsoft Corporation KEK 2K CA 2023 has been added to `KEK` and both Windows UEFI CA 2023 and Microsoft UEFI CA 2023 are present in `db`:

Figure 2: Example of environment with Microsoft Corporation KEK 2K CA 2023 in KEK via PowerShell

```
PS C:\> (Get-UEFISecureBootCerts kek). signature

Thumbprint                                Subject
----------                                -------
459AB6FB5E284D272D5E3E6ABC8ED663829D632B  CN=Microsoft Corporation KEK 2K CA 2023, O=Microsoft Corporation, C=US
6612399A4849CB38792EA443180C59ABB4DDC103  CN=Lenovo, OU=ISG, O=Lenovo, L=Morrisville, S=North Carolina, C=US
BCA4E38ED1842BC86FF76D4DA74951F1628859F8  E=build@suse.de, OU=Build Team, O=SUSE Linux Products GmbH, L=Nuremberg, C=DE, CN=SUSE Linux E
31590BFD89C9D74ED087DFAC66334B3931254B30  CN=Microsoft Corporation KEK CA 2011, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
```

Figure 3: Example of environment with Windows UEFI CA 2023 and Microsoft UEFI CA 2023 in db

```
PS C:\> (Get-UEFISecureBootCerts db). signature

Thumbprint                                Subject
----------                                -------
791977FE907722F50FEE8286C4E06B1EE16C2CFF  E=security@nutanix.com, CN=Nutanix Secure Boot Key, OU=Security, O=Nutanix, L=San Jose, S=CA, C=U
45A0FA32604773C82433C3B7D59E7466B3AC0C67  CN=Windows UEFI CA 2023, O=Microsoft Corporation, C=US
B5EEB4A6706048073F0ED296E7F580A790B59EAA  CN=Microsoft UEFI CA 2023, O=Microsoft Corporation, C=US
DBB85746CC4E7BDC283585D2407773A685C5C452  CN=Lenovo, OU=ISG, O=Lenovo, L=Morrisville, S=North Carolina, C=US
B08CBB1BC93C2CAE1BB63500EEDAB4472FEB2B79  C=US, S=CA, L=Santa Clara, OU=DEG, O=Intel Corporation, CN=Intel(R) Power Thermal Utility Option
738A962BD9C81B727717AF17EE093FE9B4BAEEC0  CN=VMware Secure Boot Signing, O="VMware, Inc.", L=Palo Alto, S=California, C=US
137E571F0B818A0F5C323DA27F4AECCF95980C96  O="VMware, Inc.", L=Palo Alto, S=California, C=US
02C2DB63ABEC31D1484C143172FC9268F864C7DD  E=build@suse.de, OU=Build Team, O=SUSE Linux Products GmbH, L=Nuremberg, C=DE, CN=SUSE Linux Ente
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
```

Via UEFI Settings

All Secure Boot settings can always be managed directly under the UEFI Security Settings.

1. Reboot the server to the F1 Setup menu to enter UEFI Settings
2. Navigate to System Settings > Security > Secure Boot Configuration

3. Use the View Secure Boot Keys menu option to display a complete table of keys including `PK` (Platform Key), `KEK` (Key Exchange Keys), `db` (Authorized Signature Database), and `dbx` (Forbidden Signature Database)

An environment is considered properly secured by CA 2023 when the Microsoft Corporation KEK 2K CA 2023 has been added to `KEK` and both Windows UEFI CA 2023 and Microsoft UEFI CA 2023 are present in `db`:

Figure 4: Example of environment with Microsoft Corporation KEK 2K CA 2023 in KEK via UEFI

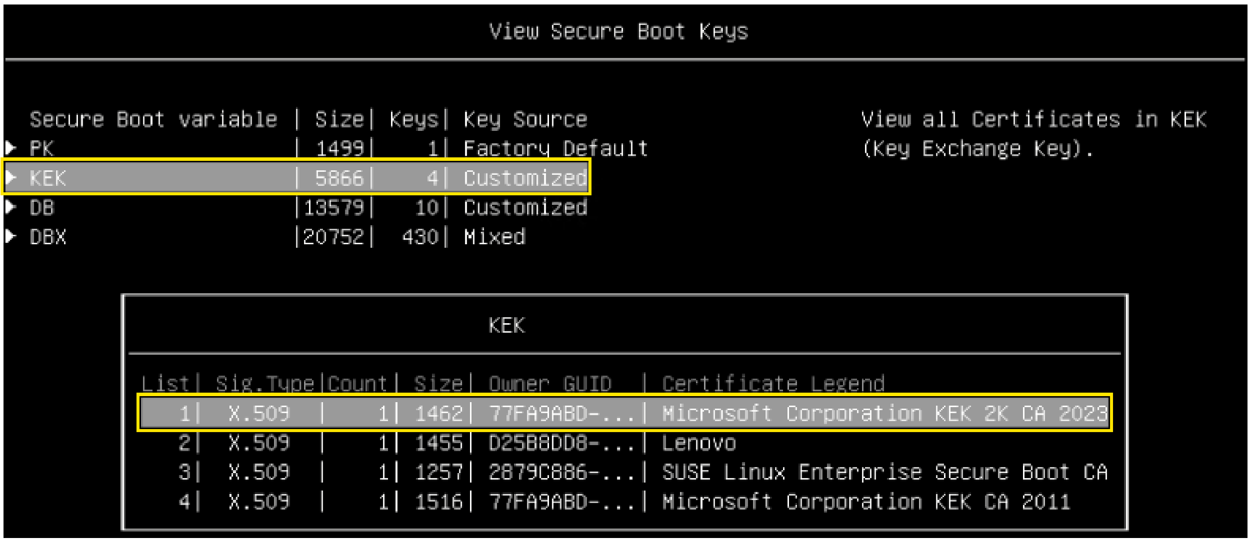
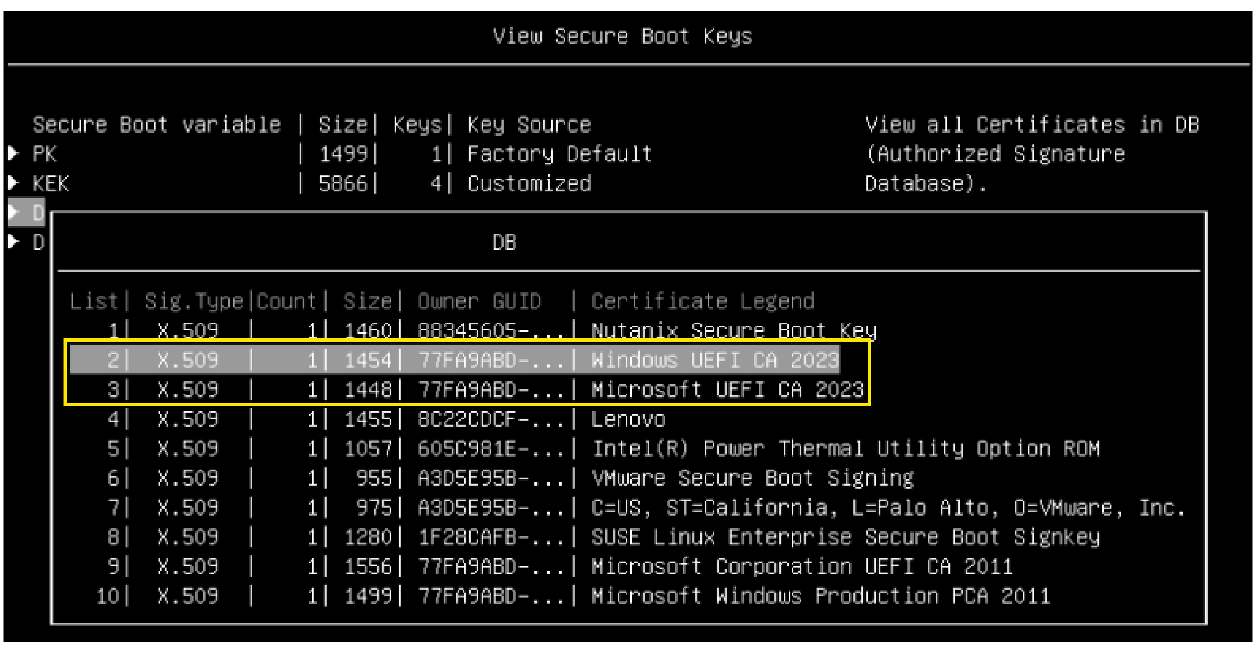


Figure 5: Example of environment with Windows UEFI CA 2023 and Microsoft UEFI CA 2023 in db in UEFI Settings



Certificate expiration vs revocation

Warning: Certificate expiration and revocation have different effects. An expired certificate may remain present in `db` (allow list) and can still permit boot in some scenarios. A revoked certificate is added to `dbx` (deny list)and is blocked by Secure Boot, preventing affected boot binaries (including boot loaders, boot managers, and recovery media components) from loading. After June 2026 (and beyond the October 2026 grace period), systems may continue to boot if CA 2011 certificates remain only in `db`. Customers should verify in `dbx` whether revocation has been applied, particularly before system reboots or when validating environment readiness for recovery or deployment operations, and continue doing so until Microsoft formally announces the CA 2011 certificates' revocation.

Update Windows Server to Secure Boot CA 2023

If any of the CA 2023 keys are missing from the environment, the following instructions should be followed so that the Secure Boot keys may be updated.

Before You Start

Secure Boot requirement

Secure Boot must be enabled in Windows Server environments before proceeding. Note that Secure Boot is enabled by default on all Azure Local solutions.

`Confirm-SecureBootUEFI` can be run via command prompt or PowerShell to check the environment's Secure Boot status.

If Secure Boot is not enabled, it can be enabled via UEFI Settings or via OneCLI.

BitLocker requirement

If BitLocker is already in use, it must be suspended before proceeding and resumed after the update is complete.

For Windows Server environments, BitLocker can be suspended via PowerShell.

For Azure Local instances, BitLocker can be suspended via PowerShell.

Minimum Lenovo UEFI builds that automatically include Microsoft Secure Boot CA 2023 certificates

The minimum Lenovo UEFI build that incorporates Microsoft Secure Boot CA 2023 certificates for each server is documented in the following table. After the respective firmware update has been applied, CA 2023 certificates are included in `dbDefault`, the UEFI Secure Boot variable that acts as a secure backup of `db` (Signature Database or allow list); however, the certificates may not automatically be present in the active Secure Boot key list, `db`. Enrollment into `db` occurs only after one of the following actions is performed:

1. Windows servicing updates the Secure Boot variables during normal OS operation, or
2. Secure Boot keys are reset to factory defaults via UEFI Settings, which propagates default keys into NVRAM (Non-Volatile Random Access Memory, which retains data even when power is turned off)

Reminder: Even if the environment is at the minimum Lenovo UEFI build that incorporates Microsoft Secure Boot CA 2023 certificates, the state of the certificates must be verified, and if not present, the keys must be reset to factory defaults and verified again.

Warning: Customer Secure Boot keys can be overwritten when the Secure Boot keys are restored to factory settings, and re-enrollment may be required.

Newer generation servers that are not listed are already pre-configured with CA 2023 certificates directly from manufacturing.

The following tables (divided by CPU family) should be reviewed to confirm the minimum UEFI build that includes CA 2023 certificates, and the instructions next to the table should be followed to if it is necessary to activate the CA 2023 certificates in the environment.

AMD CPU family

Table 2: AMD CPU family Minimum UEFI builds with Secure Boot CA 2023

CPU Family	Platform	UEFI Build
AMD Ryzen 7000 Series (Codename: AM5 Raphael)	ST45V3	QIE102W-1.10
AMD EPYC 8004 Series (Codename: Siena/Genoa)	SE455 V3	MBE116F-6.10
AMD EPYC 9004 Series (Codename: Genoa) / AMD EPYC 9005 Series (Codename: Turin)	SR635 V3	KAE128C-5.10
	SR645 V3	
	SR655 V3	
	SR665 V3	
	SR685a V3	R5E114J-3.10
	SD665 V3	QGE132T-6.10
	SD665-N V3	
	SR675 V3	
	SD535 V3	GPE110B-2.10
AMD EPYC 7002 Series (Codename: Rome) / AMD EPYC 7003 Series (Codename: Milan)	SR635	CFE146C-7.50
	SR655	
	SR645	D8E140B-3.50
	SR665	

Intel CPU family

Table 3: Intel CPU family Minimum UEFI builds with Secure Boot CA 2023

CPU Family	Platform	UEFI Build
Intel Xeon 6 Granite Rapids / Sierra Forest (Codename: Birch Stream)	SR850 V4	RVE1xxx
	SR860 V4	
	SR630 V4	IHE1xxx
	SR650 V4	
	SC750 V4	Q5E1xxx
	SD550 V4	
	SD520 V4	DBExxx

CPU Family	Platform	UEFI Build
Intel Xeon Scalable 4th/5th Gen Sapphire Rapids / Emerald Rapids (Codename: Eagle Stream)	SR860 V3	RSE118F-7.10
	SR850 V3	
	SR950 V3	EBE114G-6.10
	SD650 V3	USE134F-7.10
	SD650-I V3	
	SD650-N V3	
	ST650 V3	
	SR630 V3	ESE130E-3.40
	SR650 V3	
	SD530 V3	FNE120E-3.10
	SD550 V3	
	SR680a V3	R3E106G-2.10
	SR780a V3	
Intel Xeon Scalable 3rd Gen Ice Lake-SP (Codename: Whitley)	SE450	CME122E-3.20
	SR670 V2	U8E132E-3.20
	SN550 V2	
	ST650 V2	
	SD630 V2	
	SD650 V2	
	SD670 V2	
	SR630 V2	AFE134E-3.50
	SR650 V2	
Intel Xeon Scalable 2nd/3rd Gen Cooper Lake-SP (Codename: Cedar Island)	SR850 V2	M5E132E-3.20
	SR860 V2	
Intel Xeon E-2300 Rocket Lake-E (Codename: Tatlow)	SR250 V2	TQE120E-7.10
	ST250 V2	
	ST50 V2	TOE112C-4.10

CPU Family	Platform	UEFI Build
Intel Xeon Scalable 1st/2nd Gen Skylake-SP / Cascade Lake-SP (Codename: Purley)	SD650	OTE186H-4.21
	SN550	IVE186H-4.21
	SN850	
	SR630	
	SR650	
	SR650 - M1	IVE562A-4.10 / IVE566a-4.10
	SD530	TEE186H-4.21
	SR530	
	SR550	
	SR570	
	SR590	
	SR850	
	SR850P	
	SR860	
	SR670	G1E140F-4.20
	SR950	PSE154C-4.10
	SR950 - A2	PSE530E-7.12
	SR950 - G1	PSEJ56A-6.75
	SR950 - M1	PSE661A-4.10
	ST550	O0E186H-4.21
Intel Xeon E-2100 / E-2200 Series Coffee Lake (Codename: Mehlow)	SR150	ISE1xxx
	SR250	
	ST250	
	ST50	ITE1xxx
Intel Xeon E-2400 Raptor Lake (Codename: Catlow)	ST50 V3	CTE1xxx
	SR250 V3	
	ST250 V3	
Intel Xeon D-2700 / D-1700 Series (Codename: Icelake-D)	SE350 V2	IYE118E-6.20
	SE360 V2	
Intel Xeon D-2100 Series (Codename: Skylake-D)	SE350	HYE140C-3.30
Intel Xeon E5 v3 / v4 Haswell, Broadwell (Codename: Grantley)	x240 m5	C4E1xxx
	X3550 M5	TBE1xxx
	X3650 M5	TCE1xxx

Reminder: If Microsoft Corporation KEK 2K CA 2023 is already present in `KEK` and both Windows UEFI CA 2023 and Microsoft UEFI CA 2023 are present in `db` after applying the minimum UEFI build, no further action is required. If any of those certificates are missing, perform the Restore Factory Keys procedure.

Activate CA 2023 Keys via Restore Factory Keys

If the CA 2023 keys are not reflected in the `db` when the server is at least at the minimum Lenovo UEFI build that includes CA 2023 certificates, a final step may be required for the CA 2023 keys to be properly activated.

Warning: Restore Factory Keys will do the following:

- Wipe any custom `db`/`dbx`/`PK` entries
- Potentially break BitLocker re-seal flows even if only suspended temporarily

Via OneCLI (ideal for fleet management)

Lenovo's OneCLI tool is a standalone utility that can be used to configure server settings either in-band (from the host OS) or out-of-band (through the BMC). If OneCLI has not been used before, it must be installed on the system from which the command is run and confirm that the required access is available (local administrator on the host and/or valid BMC credentials with configuration privileges).

OneCLI can be downloaded at https://pubs.lenovo.com/lxce-onecli/.

Before proceeding, confirm connectivity to the target (BMC IP or host), and double-check the account and target selection in the command to avoid the Secure Boot key reset being applied to the wrong system.

```
OneCli.exe config set SecureBootConfiguration.SecureBootPolicy “Reset All Keys to Default” --bmc BMC_username:BMC_password@BMC_IP
```

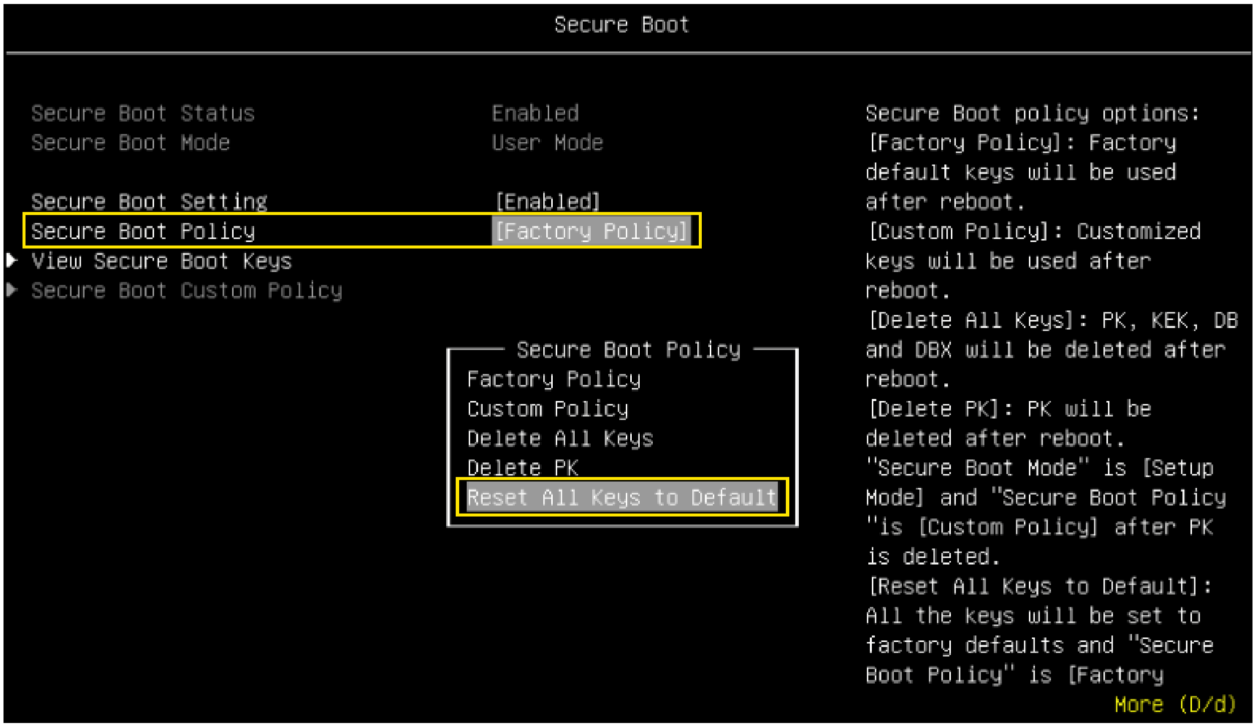
Warning: All custom keys will be erased when the keys are reset, and those keys will need to be added to the environment again.

Via UEFI Settings

As mentioned previously, all Secure Boot settings can always be managed directly under the UEFI Security Settings of a respective system.

1. Reboot the server to the F1 Setup menu to enter UEFI Settings
2. Navigate to System Settings > Security > Secure Boot Configuration
3. Open the Secure Boot Policy dropdown menu (currently showing “Factory Policy”) to view all policy options
4. Select “Reset All Keys to Default” to initialize the Secure Boot variables to load with CA 2023 keys as shown in Figure 5.

Figure 6: Reset All Keys to Default via UEFI Settings



Warning: Resetting the keys will erase all custom keys and those will need to be added to the environment again

Scenario: Windows Server environment is already deployed

Windows Server 2025

The CA 2023 boot certificate keys are automatically pushed and written into the UEFI `db` (allow list) in all Windows Server 2025 builds (since the July 2025 Full Media Refresh (FMR) release) during Windows installation and servicing. If an older WS2025 is already installed (deployed before July 2025 FMR), applying the latest KB to the server will update the boot manager.

However, the latest Lenovo UEFI firmware must be installed first, before any system reboots occur to guarantee that the Secure Boot posture is registered directly as the new factory default (`dbDefault`) and to ensure that no keys are accidentally replaced during a BIOS reset.

Refer to the Minimum UEFI builds with Secure Boot CA 2023 section to ensure the environment is at the minimum (ideally latest) firmware containing CA 2023 keys.

Windows Server 2022

Warning: Windows Server 2022 images **DO NOT** ship with CA 2023 keys pre-populated. To establish the Secure Boot CA 2023 trust chain on a WS2022 environment, two independent updates are required, and both must be completed before June 2026 to ensure continuous Secure Boot operation:

1. Firmware (Lenovo UEFI): Install the Minimum UEFI builds with Secure Boot CA 2023, so that the Microsoft Corporation KEK 2K CA 2023, Windows UEFI CA 2023, and Microsoft UEFI CA 2023 certificates are present in `KEK` and `dbDefault`, respectively, and are ready for activation if necessary.

2. Operating system (Microsoft cumulative updates): Follow the existing Lenovo documentation to [Update Windows Boot Manager with Windows UEFI CA 2023 Certificate](). A WS2022 installation that predates the CA 2023 servicing updates still has a Windows Boot Manager on disk that is signed only by the 2011 certificate chain — even after the firmware has been updated and the new CA 2023 keys are enrolled in `db`. Once the 2011 certificates expire (or are revoked via `dbx`), that older Boot Manager will no longer be trusted by Secure Boot and the system will fail to boot. Updating the firmware alone is not sufficient; the on-disk boot files must also be refreshed.

Warning: Windows Server 2022 reaches the end of mainstream support in October 2026. All environments should plan migration to Windows Server 2025 to maintain a supported configuration. Completing the CA 2023 transition on WS2022 in the interim is advised to keep existing workloads bootable and secure through the migration window.

Reminder: After completing the steps in this scenario, re-check the Secure Boot keys to confirm that Microsoft Corporation KEK 2K CA 2023 is present in `KEK` and that Windows UEFI CA 2023 and Microsoft UEFI CA 2023 are present in `db`. If the CA 2023 keys are not showing as active (i.e., they appear only in `dbDefault` and not in `db`), follow Activate CA 2023 Keys via Restore Factory Keys to enroll them.

Windows Server 2019 or older

Warning: Windows Server 2019 images **DO NOT** automatically include CA 2023 keys. However, more importantly, Windows Server 2019 has been out of mainstream support since January 9th, 2024. All Windows Server 2019 environments should be updated to Windows Server 2025 to return to a supported configuration.

WinPE recovery media

WinPE-based recovery media is subject to the same Secure Boot trust chain as a fully installed Windows Server environment. WinPE images built before the CA 2023 servicing updates contain a boot loader signed only by the Microsoft Windows Production PCA 2011 certificate chain and will fail to boot on any system where the 2011 certificates have expired (June 2026) or have been revoked via `dbx` — even when the underlying server is at the latest Lenovo UEFI build with the CA 2023 keys correctly enrolled in `db`. Two prerequisites must therefore be satisfied for recovery media to remain usable through and beyond the CA 2023 transition:

1. Firmware (Lenovo UEFI): Confirm the target server is at the Minimum UEFI builds with Secure Boot CA 2023 so that Windows UEFI CA 2023 is present in `db` and the WinPE boot loader signature can be validated at boot.
2. Recovery media (WinPE rebuild): Rebuild all WinPE-based recovery, deployment, and rescue media using a Windows ADK / WinPE add-on that includes the CA 2023-signed boot files. Follow the existing Lenovo documentation to Create WinPE Bootable Media with CA 2023. Pre-staged media that cannot be rebuilt (for example, read-only OEM USB keys or archived ISO images) must be re-issued or replaced before June 2026.

Warning: Recovery media is frequently the last artifact updated in an environment because it sits outside normal patch cycles. A working production server with CA 2023 fully enrolled can still become unrecoverable if its only recovery media is signed by the 2011 chain. Lenovo recommends validating recovery media boot on a representative system after the firmware has been updated and the CA 2023 keys are confirmed in db, so that media that would fail post-transition is identified while the 2011 chain is still trusted as a fallback.

Scenario: Windows Server environment is not yet deployed

The Microsoft Corporation KEK 2K CA 2023 has been incorporated by Microsoft into Windows Server 2025 images since January 21st, 2026, via the Full Media Refresh (FMR) release. However, even when a current Windows operating system (OS) image that integrates support for the CA 2023 boot certificates is being run, the UEFI must contain the correct Secure Boot keys to maintain the integrity of the Secure Boot trust chain during the CA 2023 transition.

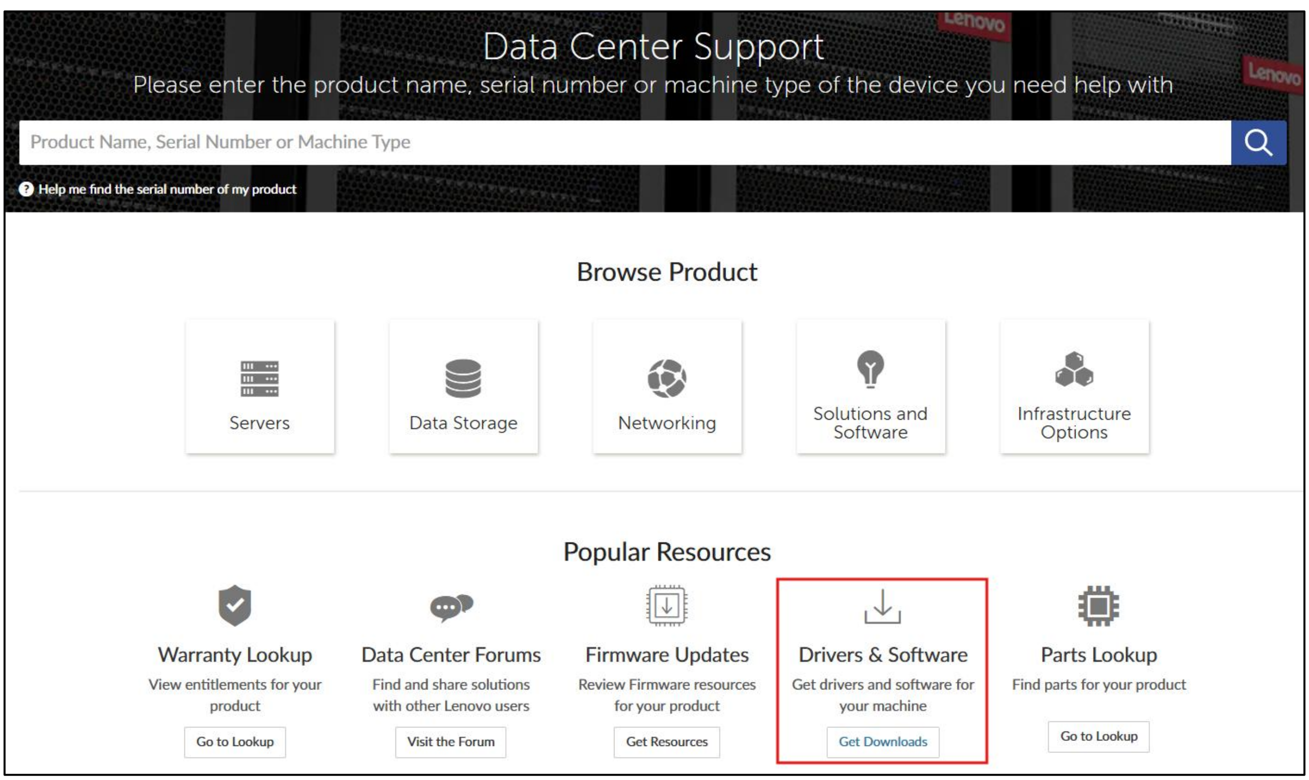
This is particularly imperative for servers that have not yet been deployed and on which no OS has been loaded so that Secure Boot certificate updates may be adopted via OS updates. In this pre-deployment scenario, reliance is placed solely on the correct UEFI firmware so that the integrity of Secure Boot may be maintained.

Deploying with Lenovo preload image

When deploying using a Lenovo preload image, verify that the selected media includes support for Secure Boot CA 2023 certificates.

- Lenovo OEM Windows Server installation ISOs may be downloaded from the server's Service and Support page under **Drivers & Software > Microsoft OEM Media** (availability varies by language) as shown next in the red box in Figure 6.

Figure 7: Lenovo Data Center Service and Support page to access Microsoft OEM Media via Drivers & Software section



- If the required installation media is not available for direct download, an electronic recovery media request can be submitted after logging in through Lenovo Data Center Support: [Request recovery media]

The following information is required when submitting a request:

- Server serial number
- Digital image of the Windows Server Certificate of Authenticity (COA) label
- Requestor name and email address

Including a Service contact name or case number in the submission notes is recommended.
For Japanese-language media, the requested language should be specified in the submission notes.

Deploying after re-installing a clean Windows Server image

It is advisable to deploy using a Lenovo preload image, so the environment is properly deployed with all the necessary and validated firmware and device drivers, which already inject the Secure Boot CA 2023 certificates.

Should there be a deployment with a clean Windows Server 2025 image, the latest Lenovo UEFI firmware should be installed prior to deployment to minimize any disruption with OS boot managers that are only signed with CA 2011 certificates.

Warning: Any new deployments with out-of-support images like Windows Server 2022, Windows Server 2019 or older, will trigger a Secure Boot violation once CA 2011 is revoked, which could render environments in an unbootable state. Windows Server 2022 reaches end of support in October 2026, and Windows Server 2019 has been out of support since January 2024.

Scenario: Azure Local solution running Azure Stack HCI

Starting with Azure Local 2603, Microsoft provides Secure Boot CA 2023 certificates via the built-in orchestration of platform updates. For more information on Microsoft's Azure Local Secure Boot announcements, please visit their [Manage Secure Boot updates] page.

New deployments

All new deployments after May 2026 use Lenovo ThinkAgile MX preload images that ship from manufacturing, with at least the Azure Local 2603 image, the latest ThinkAgile MX Best Recipe firmware and device drivers, and Secure Boot CA 2023 certificates.

Deployed clusters

Secure Boot CA 2023 certificates are delivered either through the OS servicing method (starting with Azure Local 2603 release) or through firmware update updates included in the latest ThinkAgile MX Best Recipes (including the MXBR2410 for MX3520 and SR650 certified nodes).

Reminder: After completing the steps in this scenario, [re-check the Secure Boot keys] to confirm that Microsoft Corporation KEK 2K CA 2023 is present in `KEK` and that Windows UEFI CA 2023 and Microsoft UEFI CA 2023 are present in `db`. If the CA 2023 keys are not showing as active (for example, they appear only in `dbDefault`), follow [Activate CA 2023 Keys via Restore Factory Keys] to enroll them.

Recovery Scenarios

If the environment was not updated with CA 2023 certificates before the CA 2011 certificates expired in June 2026*, or if a partial update left the firmware and operating system out of sync, one or more of the following symptoms may be observed.

Reminder: Capture a record of the current Secure Boot key state (using either the PowerShell or UEFI Settings methods described in Check Which Certificates Are Installed) and document any custom `KEK/db/dbx` entries enrolled in the environment. Several recovery procedures below require resetting Secure Boot keys to factory defaults, which will erase custom entries and require re-enrollment.

***Reminder**: Customers have been given a grace period until October 2026 to transition from CA 2011 certificates to CA 2023 certificates, ensuring they can maintain their Secure Boot postures before CA 2011 certificates are officially revoked by Microsoft.

Scenario: Firmware was updated but CA 2023 keys are not present in db

Table 4: Recover scenario where CA 2023 keys are not present in db after firmware update

Symptom	The Lenovo UEFI build is at or above the minimum listed in Table 2: Minimum UEFI builds with Secure Boot CA 2023, but the PowerShell or UEFI Settings check shows that one or more CA 2023 certificates are missing from `KEK` or `db`. The certificates may be present in `dbDefault`.
Root cause	The CA 2023 certificates are populated only into `dbDefault` by the firmware update and are not automatically activated in `db`. Activation requires a Restore Factory Keys operation.
Recovery	1. Perform the Restore Factory Keys procedure described in Activate CA 2023 Keys via Restore Factory Keys. After the operation, re-verify the key state and re-enroll any custom keys that were erased.

Scenario: System fails to boot after June 2026 with a Secure Boot violation

Table 5: Recovery scenario where system fails to boot with SB violation

Symptom	The system halts at POST with a Secure Boot violation message (for example, "Secure Boot

	Violation: Invalid signature detected. Check Secure Boot Policy in Setup."), or boots directly into the UEFI Setup menu instead of the OS.
Root cause	The Windows Boot Manager on disk is signed only by the Microsoft Windows Production PCA 2011 certificate, and that certificate is no longer trusted by the firmware (either through expiration or through a `dbx` revocation entry).
Recovery	1. Boot the system from CA 2023-signed WinPE recovery media (see Create WinPE Bootable Media with CA 2023). If no compliant media is available, temporarily disable Secure Boot via UEFI Settings (System Settings > Security > Secure Boot Configuration > Secure Boot Setting > Disabled) so that the existing OS can be booted long enough to apply the recovery procedure. **Warning**: Disabling Secure Boot removes boot-time integrity validation. This should be treated as a temporary measure, and Secure Boot should be re-enabled immediately after the recovery procedure is complete. 2. Apply the latest Microsoft cumulative update so that the on-disk Windows Boot Manager is refreshed with a Windows UEFI CA 2023-signed copy. Refer to Update Windows Boot Manager with Windows UEFI CA 2023 Certificate. 3. Re-enable Secure Boot in UEFI Settings if it was disabled in step 1. 4. Verify the trust chain is restored using the PowerShell or UEFI Settings methods in Check Which Certificates Are Installed.

Scenario: BitLocker recovery key prompt appears after Secure Boot key update

Table 6: Recover scenario with BitLocker recovery key prompt

Symptom	On the next reboot following a firmware update, a Restore Factory Keys operation, or a Microsoft cumulative update that modified the Secure Boot databases, the system prompts for the BitLocker recovery key.
Root cause	BitLocker measures the Secure Boot configuration into the TPM PCRs (most commonly PCR 7). When the Secure Boot keys change, the PCR values change, and the TPM-sealed BitLocker key can no longer be released automatically.
Recovery	1. Enter the BitLocker recovery key from the location where it was escrowed (Active Directory, Microsoft Entra ID, Azure Key Vault, or the customer's key management system) to allow the OS to boot. 2. Once the OS is running, suspend BitLocker for one reboot using **`Suspend-BitLocker -MountPoint "C:" -RebootCount 1`** so that the TPM re-seals against the new Secure Boot configuration on the next boot. 3. Reboot and confirm that subsequent boots no longer prompt for the recovery key. **Warning**: This scenario can be avoided entirely by suspending BitLocker before applying any firmware update or Restore Factory Keys procedure. See the [BitLocker requirement] section under Before You Start.

Scenario: Recovery or deployment media fails to boot

Table 7: Recover scenario where recovery media fails to boot

Symptom	WinPE-based recovery media, MDT/SCCM/WDS deployment media, or OEM service USB keys fail to boot with a Secure Boot violation, even though the production OS on the same server boots normally.
Root cause	The recovery media's boot loader is signed only by the 2011 certificate chain. The production OS boot manager has been refreshed to CA 2023, but pre-staged media has not.
Recovery	1. Rebuild the affected media using the procedure in Create WinPE Bootable Media with CA 2023. For media that cannot be rebuilt in time (for example, archived ISO images required for an immediate recovery), Secure Boot may be temporarily disabled in UEFI Settings to complete the recovery operation and re-enabled afterward.

Scenario: Custom Secure Boot keys lost after Restore Factory Keys

Table 8: Recover scenario where custom Secure Boot keys are lost after factory reset

Symptom	After a Restore Factory Keys operation was used to activate the CA 2023 certificates in `db`, customer-enrolled custom `KEK`, `db`, or `dbx` entries are no longer present, and applications, third-party boot loaders, or option ROMs that depended on those custom keys fail to load.
Root cause	The Restore Factory Keys operation replaces all Secure Boot variables (`PK`, `KEK`, `db`, `dbx`) with the contents of `dbDefault`, erasing any custom entries that were not part of the factory key set.
Recovery	1. Re-enroll the custom keys using the same procedure originally used to add them

	(typically OneCLI, UEFI Settings, or the customer's key management tooling). 2. If the original key material is no longer available, re-issue the keys from the customer's certificate authority and re-sign or re-enroll the dependent components. **Reminder**: Always export and archive custom Secure Boot keys before performing a Restore Factory Keys operation. OneCLI can be used to capture the current Secure Boot variable contents prior to reset.

Scenario: Azure Local cluster node fails to rejoin cluster after CA 2023 update

Table 9: Recover scenario where Azure Local node fails to rejoin cluster

Symptom	Following a per-node CA 2023 transition on an Azure Local (Azure Stack HCI) cluster, the updated node fails to rejoin the cluster, or the cluster reports the node as unhealthy.
Root cause	The most common cause is that BitLocker was not properly suspended and re-sealed before the node was returned to the cluster, leaving the node in a state where storage volumes cannot be unlocked. Less commonly, the node's Secure Boot posture no longer matches the cluster's attestation policy.
Recovery	1. Confirm BitLocker status on the node using **`Get-BitLockerVolume`**. If any volume is in a Locked or Suspended state unexpectedly, resume protection with **`Resume-BitLocker -MountPoint "<drive>:"`** or supply the recovery key as required. 2. Verify that all CA 2023 certificates are present in db on the node and that they match the configuration of the other cluster nodes.

	3. Resume the cluster node and validate cluster health before proceeding to the next node. **Reminder**: Always perform Azure Local CA 2023 transitions one node at a time, with BitLocker suspended for the duration of the firmware update and Restore Factory Keys operation and validate full node health before moving to the next node.

If recovery is not possible using any of the procedures above — for example, the system is fully unbootable, no compliant recovery media is available, and Secure Boot cannot be temporarily disabled due to policy — please contact Lenovo Support with the platform model, current UEFI build, and the output of the Secure Boot key checks captured before the failure occurred.

References

For more information, the following resources can be referenced:

- Lenovo Press, “Updating Windows Boot Manager and WinPE with the Windows UEFI CA 2023 Certificate,” https://lenovopress.lenovo.com/lp2353-updating-windows-boot-manager-and-winpe-windows-uefi-ca-2023-certificate
- Lenovo Support, “2011 Microsoft Secure Boot Certificate Expiration – Lenovo Commercial PCs,” https://support.lenovo.com/us/en/solutions/HT518129
- Microsoft Support, “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
- Microsoft, “Manage Secure Boot updates for Azure Local 2603,” https://learn.microsoft.com/en-us/azure/azure-local/manage/manage-secure-boot-updates?view=azloc-2603
- UEFI, “Secure Boot and Driver Signing,” https://uefi.org/specs/UEFI/2.10/32_Secure_Boot_and_Driver_Signing.html

Document history

Version 1.0	May 2026	First release of the Windows Server Secure Boot CA 2023 Transition Guide document including transition requirements, firmware guidance, update scenarios and recovery procedures.

Authors

This paper was produced by the following specialists:

- **Andreína Vivas Thomas** is an Advisory Software Engineer working at the Lenovo Center for Microsoft Technologies in Bellevue, Washington. She has worked at Lenovo for over 8 years, specializing in Microsoft on-premises, cloud solutions, developing automation update tools for Azure Stack Hub and Azure Local as well as managing Windows Server enablement and certification as Project Manager.
- **Gary Cudak** is an OS Architect and Master Inventor for Software & Solutions Development with Lenovo. His current focus is on solution architectures and platform development in the areas of Hyperconvergence, Cloud, IoT and Innovation. In his more than 15 years with Lenovo and IBM before that, Gary has led diverse projects ranging from hardware and solution product development and large software projects. Additionally, Gary has more than 200 granted U.S patents and is part of the invention review board leadership at Lenovo.
- **Ron Arndt** is an Advisory Software Engineer at the Lenovo Center for Microsoft Technologies in Bellevue, Washington. He has worked for over 13 years at Lenovo and prior IBM as the global Windows Level 3 Lead and Customer Support Escalation Support Engineer for all issues related to Microsoft Windows platform products, working directly with Microsoft Escalation Engineers, Development Teams and PMs.
- **Guiqing Li** is an Advisory Software Engineer working in the Lenovo Infrastructure Solutions Group based in Beijing, China. She has more than ten years of experience with driver development, and eight years of experience with Windows debugging.

A special thank you to the following Lenovo colleagues for their contributions to this project:

- David Feisthammel, Senior Solutions Architect – Microsoft Technology and Enablement
- Wewe Chang, Staff OS Engineer – OS & Preload Development
- Hussein Jammal, Principal Technical Consultant – Partner Infrastructure Solutions Development
- Shawn Sremaniak, Preload Architect & TPM – ISG ThinkAgile Development

Trademarks and special notices

This document was created or updated on May 21, 2026.

Send us your comments via the **Rate & Provide Feedback** form found at http://lenovopress.com/lp2441