Kyowa Electronic Instruments Co., Ltd.
Product Development Department,
Instrument Engineering Group
June 26,2026

Interim Workaround for USB Device Driver Signature Errors in Our Products

1. Introduction

Recently, we have received reports regarding some of our products that are controlled by a PC via a USB interface suddenly becoming unavailable.
Upon conducting an investigation after confirming a similar issue within our own PC environments, we found it highly likely that the USB device driver's digital signature is being judged as invalid due to enhanced security features in the OS (Windows 11), thereby restricting its operation.

2. Affected Products

The following four product series are expected to be affected by this issue:

- EDX-100A Series（including MCA-200A）
- EDX-200A Series（including MCA-300A）
- EDX-10 Series
- PCD-400 Series

Note: This issue does not occur on the following products:

- CTRS-100A
- UCAM-80A
- NTB-100/200/500 Series

3. Cause of the Issue

Due to recent security updates in Windows 11, monitoring of "kernel-mode device drivers" that operate as part of the OS has been tightened. As a result, the specifications have changed to prevent drivers that do not meet Microsoft's latest standards from starting.
The device drivers used in the affected products were created before these standards were revised. Although they previously continued to function under an exemption, it is believed that recent updates have sequentially phased out this exemption, leading to the current issue.
This security enhancement applies to **Windows 11 (Version 24H2) and later**. Therefore, these products are expected to remain fully operational without issues on earlier versions of Windows 11, as well as on Windows 10 (which has already reached end-of-support).

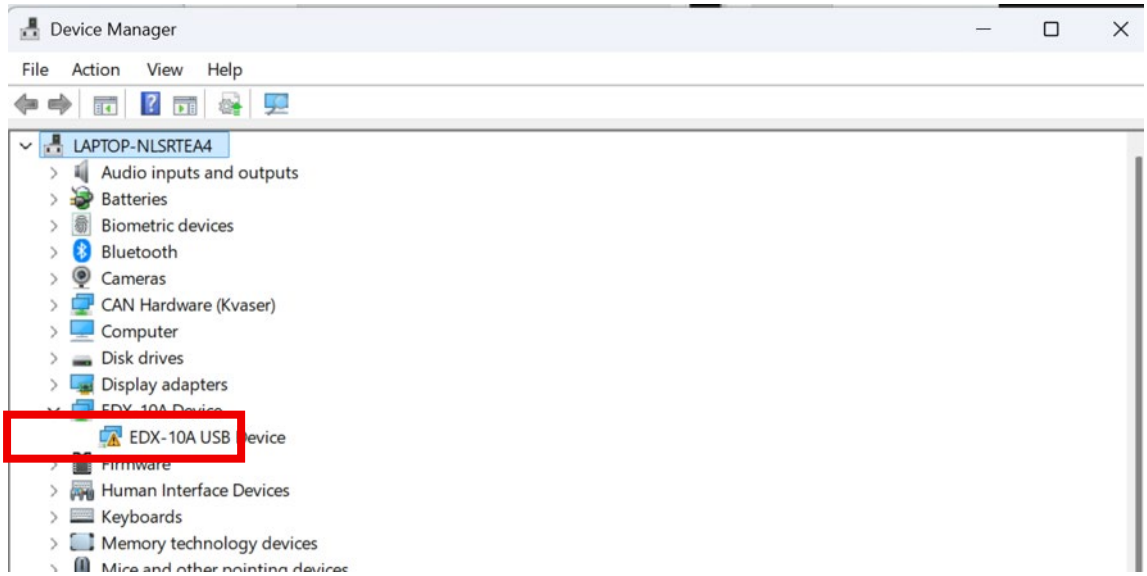
4. Verifying the Issue

If you were previously able to control the measuring instrument via the USB interface without any issues, but later begin experiencing communication errors on the control software, you may be affected by this issue.

Please follow the steps below to check whether this specific issue is occurring on your system:

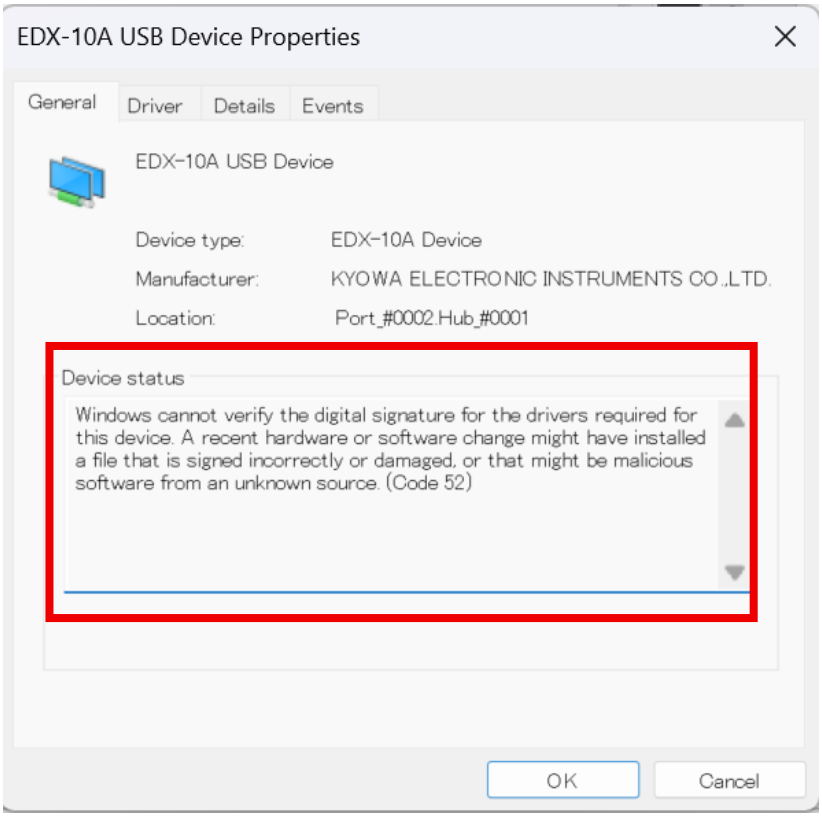
(1) Connect the PC and the measuring instrument using a USB cable, and turn on the power to the measuring instrument (ensuring it is in the state where the communication error occurs).
Note: For the EDX-10 series, this can be verified even if the LED on the main unit is not lit.

(2) Right-click the Windows 11 **Start** button, and select **Device Manager** from the displayed menu.
Note: The following steps are explained using screenshots from the "EDX-10 series" measuring instrument as an example.



(3) Check whether a warning icon (such as a yellow "!" exclamation mark) is displayed on the "EDX-10A USB Device" icon listed under "EDX-10A Device" (indicated by the red box in the image above).

(4) Double-click "EDX-10A USB Device" or right-click it and select "Properties" to display the following "EDX-10A USB Device Properties" window.



(5) If the following message is displayed in the **"Device status"** field under the **"General"** tab (indicated by the red box), it confirms that this issue is occurring:

”Windows cannot verify the digital signature for the drivers required for this device. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source (Code52)

5. Interim Workarounds

We are currently working on a permanent solution. In the meantime, we kindly ask that you consider the following interim workarounds:

① Use a different PC that is not affected by this issue.

② Use a communication interface other than USB, such as a LAN connection (Available only for the EDX-100A and EDX-200A series).

Note: If your PC does not have a built-in LAN port, a commercially available USB-to-LAN adapter can be used.

From the perspective of security and operational stability, **we highly recommend using method ① or ② whenever possible.** Only if neither of these options is feasible, please consider method ③ below as an alternative. Detailed steps for implementing method ③ are provided in the next section.

③ Boot the PC while bypassing the device driver signature check.

Note: For the EDX-10 and PCD-400 series, method ③ is the recommended workaround if method ① is not possible.

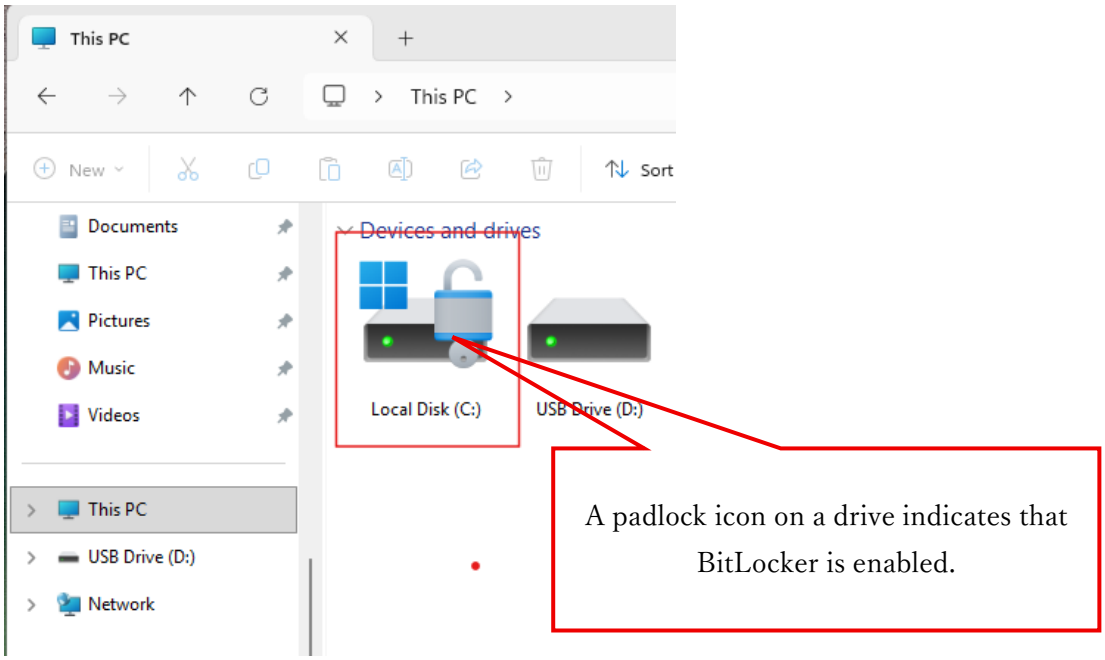
6. Setup Procedure for Interim Workaround ③

6.1 Preparation and Preliminary Check

Please check in advance whether the BitLocker feature is enabled or disabled on your PC (the subsequent steps will vary depending on this setting).

Open **"File Explorer"** and navigate to **"This PC"**. If a **"lock icon"** is displayed on the drive icon as shown in the figure below, the BitLocker feature is enabled.

Note: If the icon is difficult to see, please switch the View menu to "Large icons" to check.



⚠ **Important Caution if BitLocker is "Enabled" If the procedure is not completed successfully, you may be prompted to enter a "Recovery Key (a 48-digit number)" when booting your PC. If you cannot provide this key, the PC will become unbootable. Therefore, please ensure you complete the following preparations in advance:**

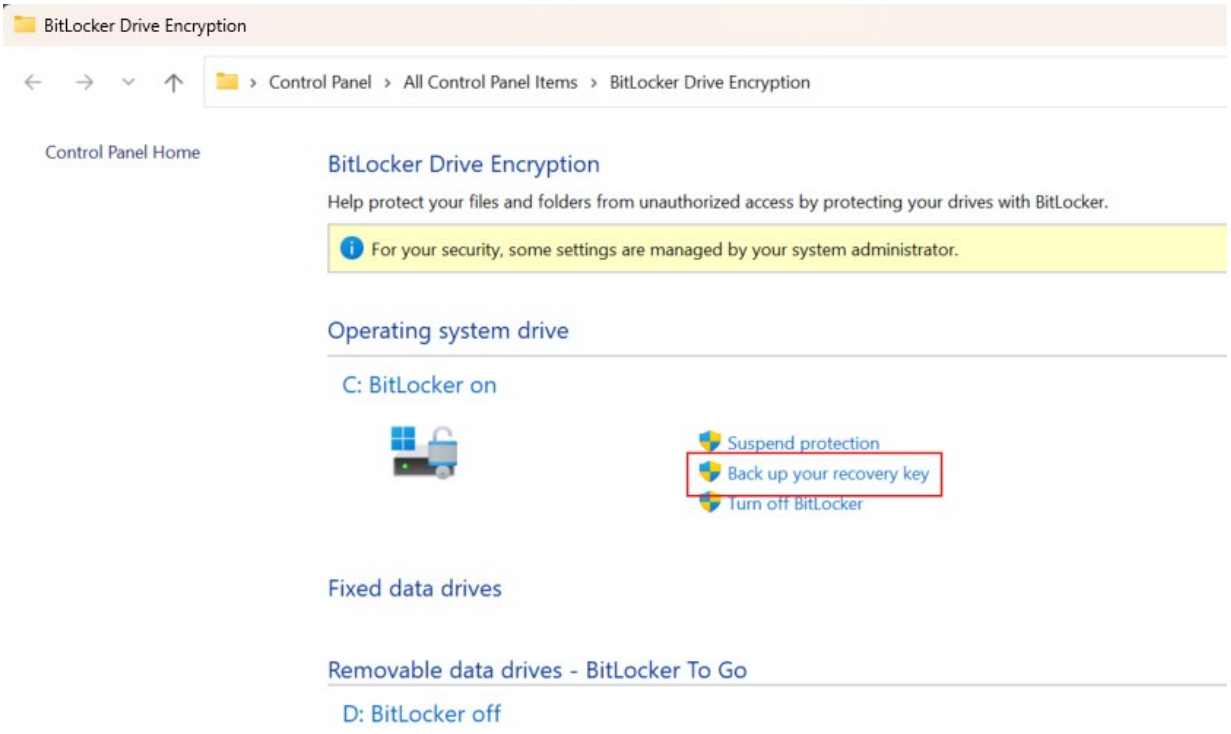
① **Prepare your Recovery Key: Print the key out on paper or ensure it can be accessed from another device before proceeding.**

② **Consult your IT/Management Department: If you do not know your recovery key, please verify it with your IT support department before starting this work (typically, it is stored outside the PC during initial setup).**

The procedure for saving or printing the recovery key from your current PC is as follows:

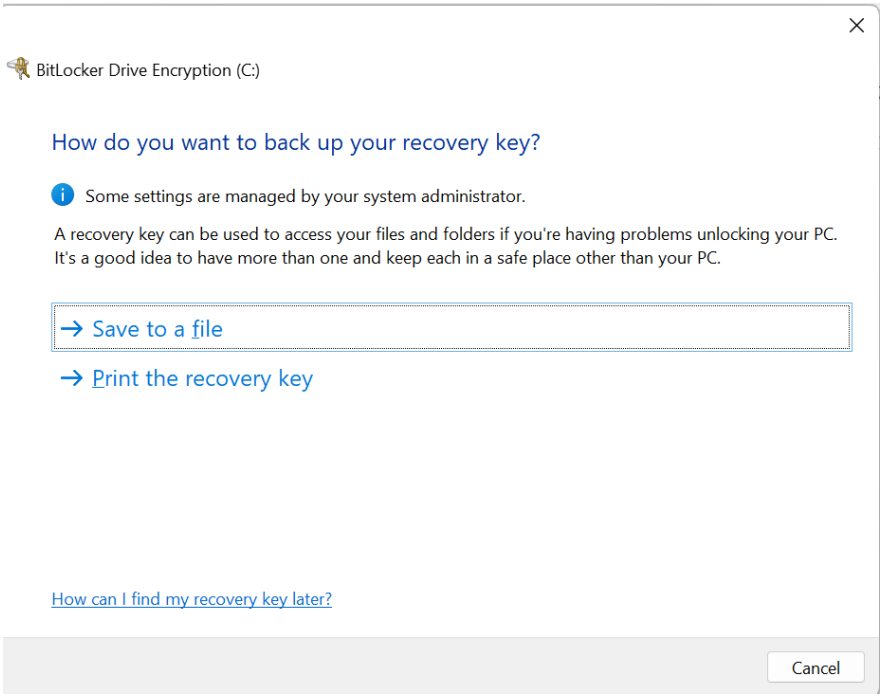
(1) In File Explorer, right-click the drive icon where BitLocker is enabled, and select **"Manage BitLocker"** from the displayed menu.

(2) The **"BitLocker Drive Encryption"** window will appear. Click **"Back up your recovery key"** (indicated by the red box) to the right of the drive icon.



(3) The **"How do you want to back up your recovery key?"** window will appear. Choose whether to save it to a file or print it.

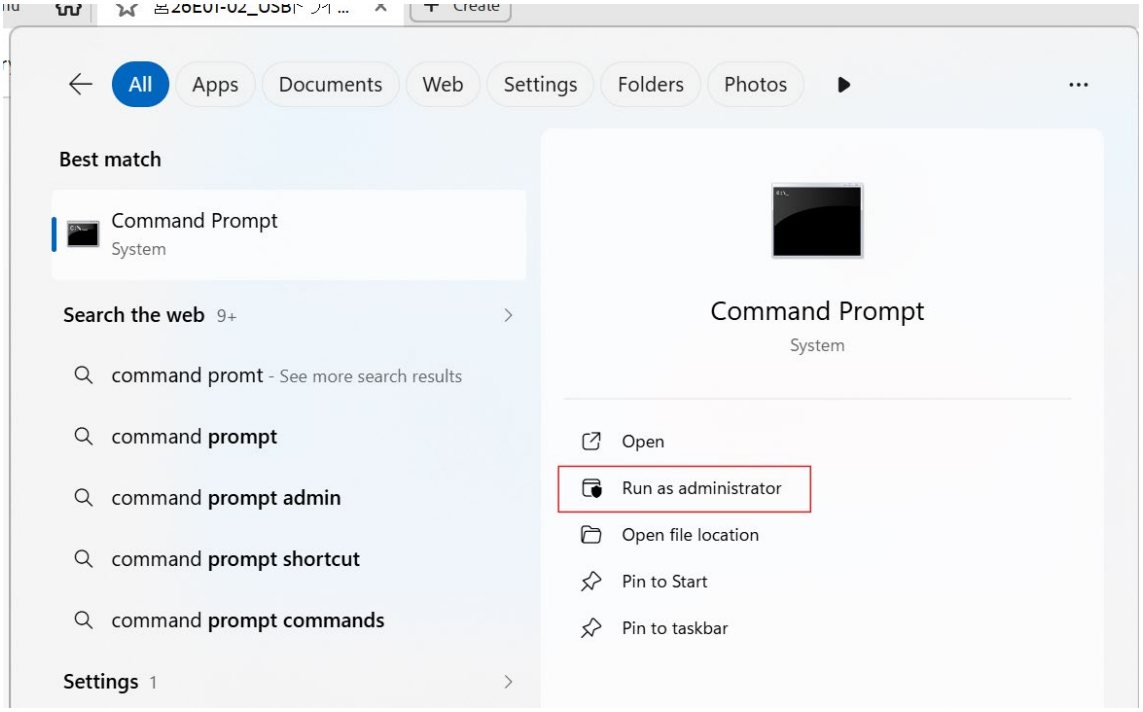
Note: If you select **"Save to a file"**, you must choose a destination drive that is not encrypted by BitLocker. Please save it to a USB flash drive or other external storage.



6.2. Setup Procedure if BitLocker is "Disabled"

Note: If the BitLocker feature is "Enabled," please refer to Section 6.3.

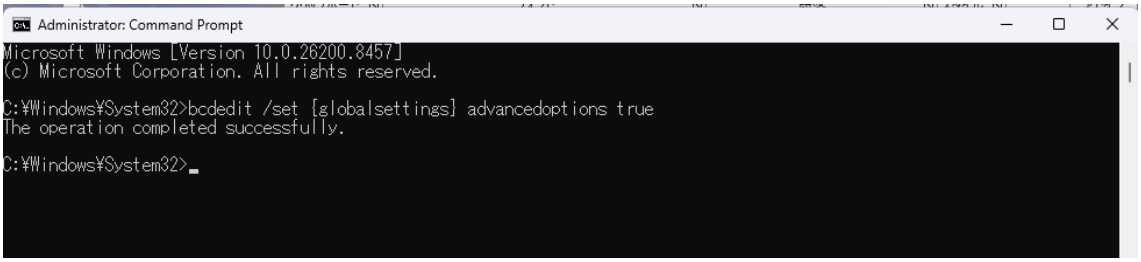
(1) After booting the PC, launch the Command Prompt with **Administrator privileges**. Left-click the **Start** button, type **"Command Prompt"** into the search box at the top of the Start menu, and then select **"Run as administrator"** from the options displayed on the right.



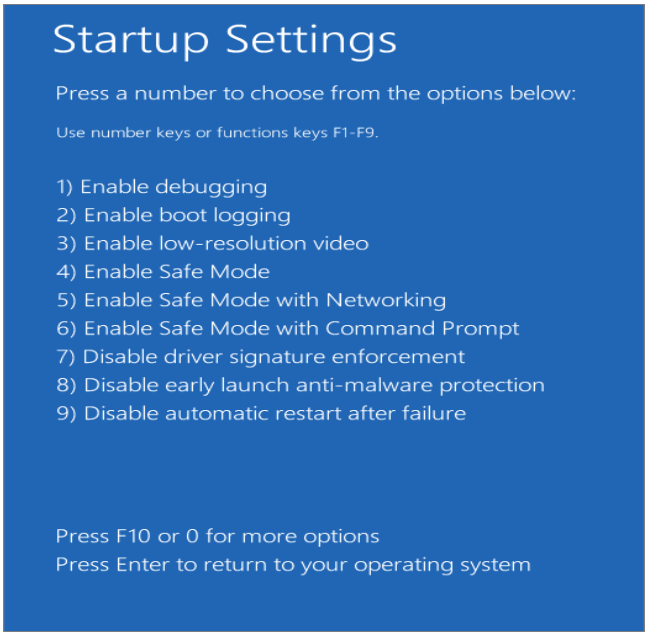
(2) Type the following command and press the **[ENTER]** key.

bcdedit /set {globalsettings} advancedoptions true

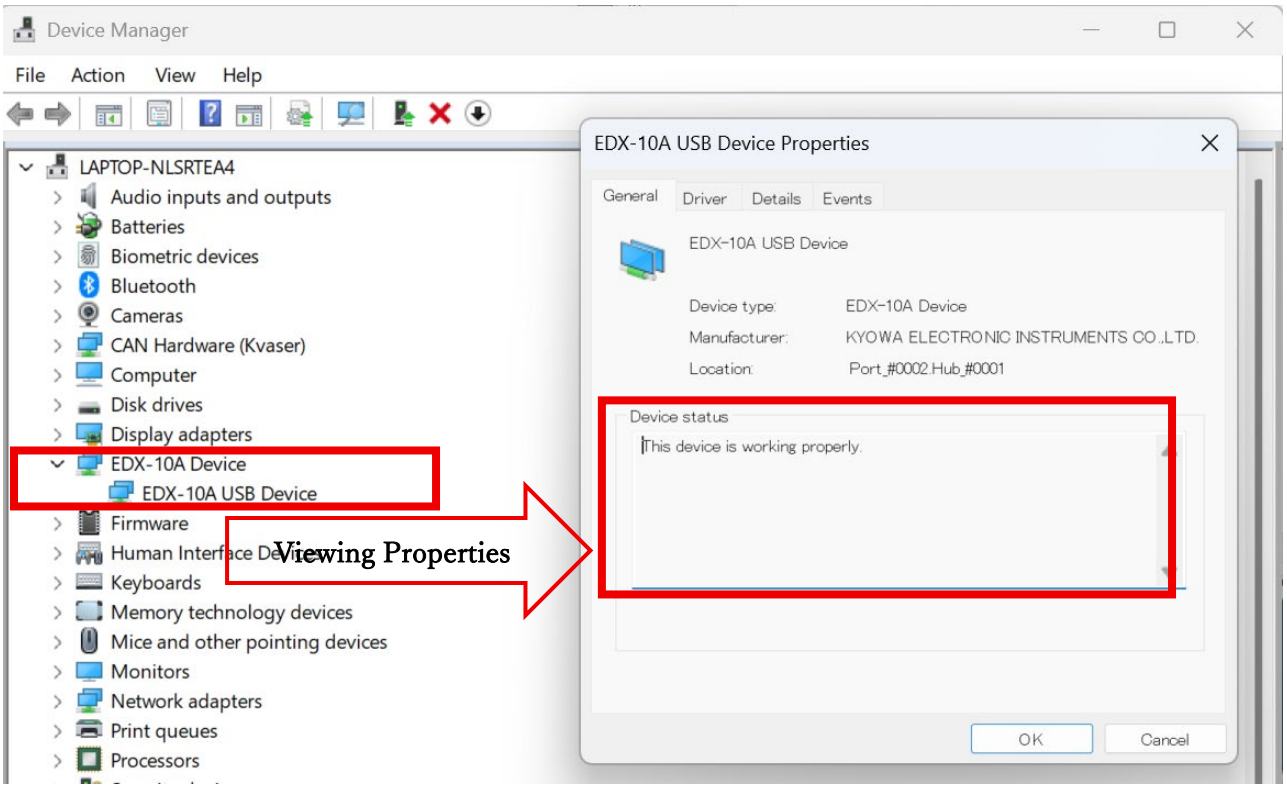
(3) Verify that the message **"The operation completed successfully"** is displayed, and then close the Command Prompt window. Restart your PC to apply the changes.



(4) When the PC restarts, the **"Startup Settings"** screen shown below will be displayed every time. Select **"7) Disable driver signature enforcement"** (or press the **[7]** or **[F7]** key).



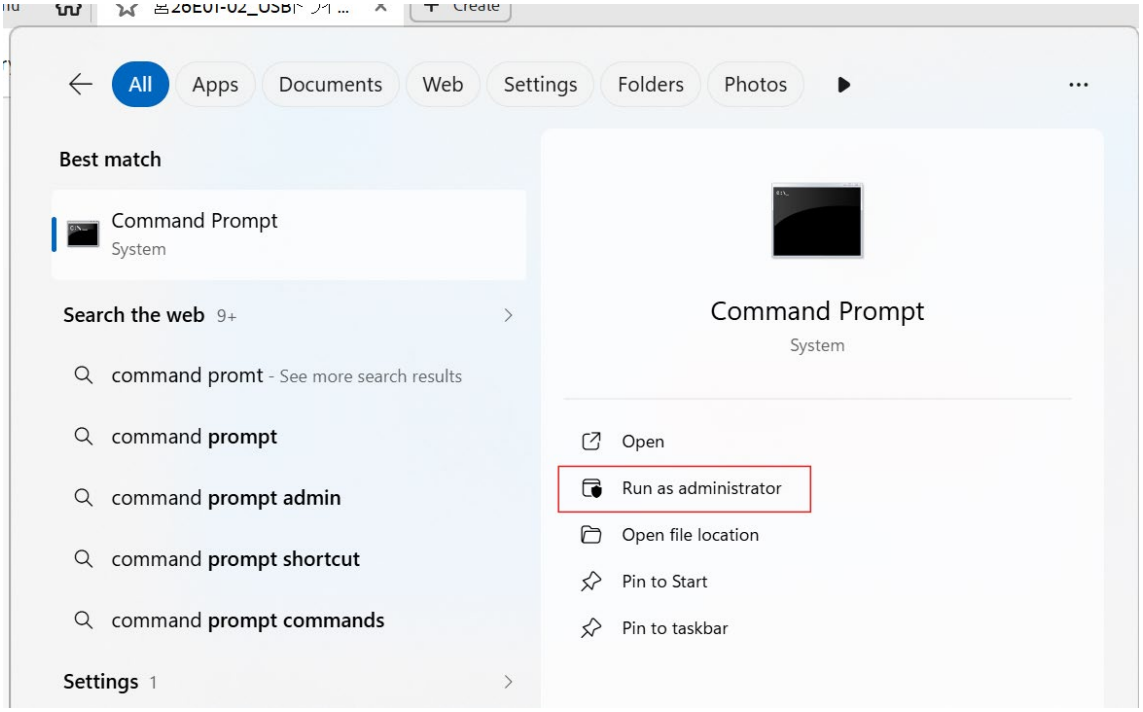
(5) After Windows 11 boots up, the restrictions on the affected device driver will be lifted, making it available for use. If you check Device Manager, you can confirm that the warning icon has been removed from the target measuring instrument's device driver and that it is ready for use (the image below shows the EDX-10 series as an example). *(Please refer to **Section 4** for details on how to access Device Manager and view Device Properties.)*



6.3. Setup Procedure if BitLocker is "Enabled"

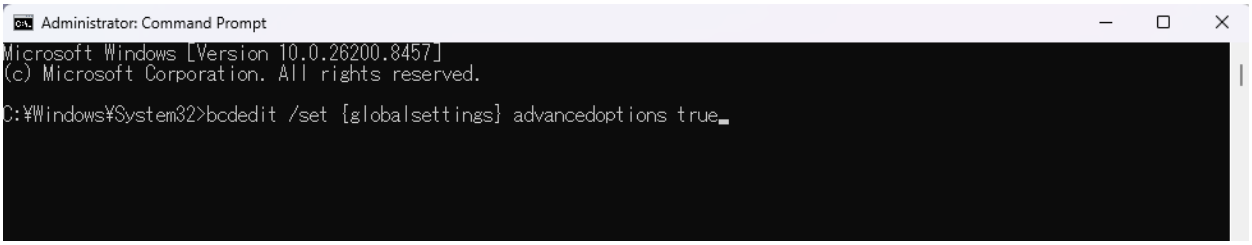
Note: If the BitLocker feature is "Disabled," please refer to Section 6.2.

(1) After booting the PC, launch the Command Prompt with **Administrator privileges**. Left-click the **Start** button, type **"Command Prompt"** into the search box at the top of the Start menu, and then select **"Run as administrator"** from the options displayed on the right.

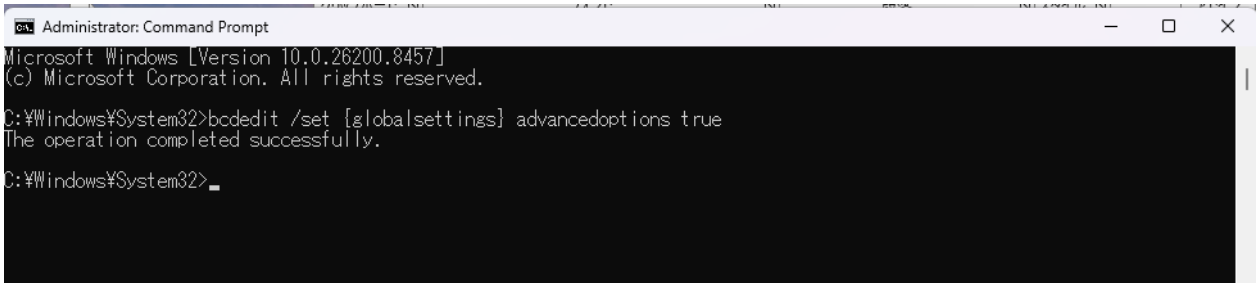


(2) Type the following command and press the **[ENTER]** key.

bcdedit /set {globalsettings} advancedoptions true



(3) Verify that the message **"The operation completed successfully"** is displayed, and then close the Command Prompt window.



(4) Open a text editor such as Notepad and create a text file containing the following text (ensure all characters are half-width).

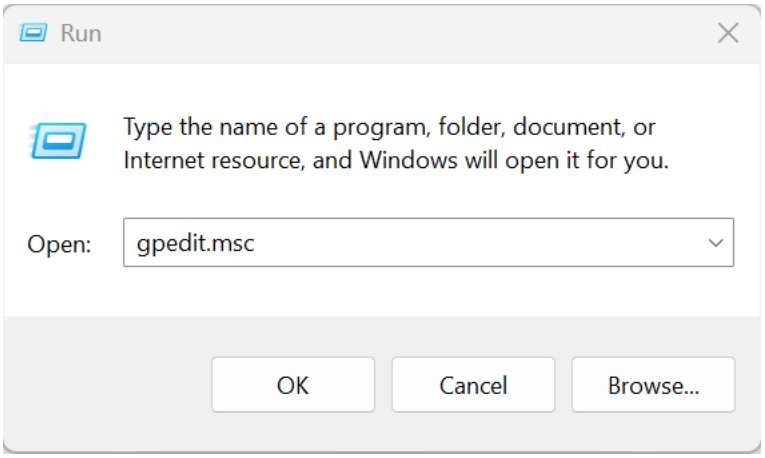
@echo off

manage-bde -protectors -disable C:

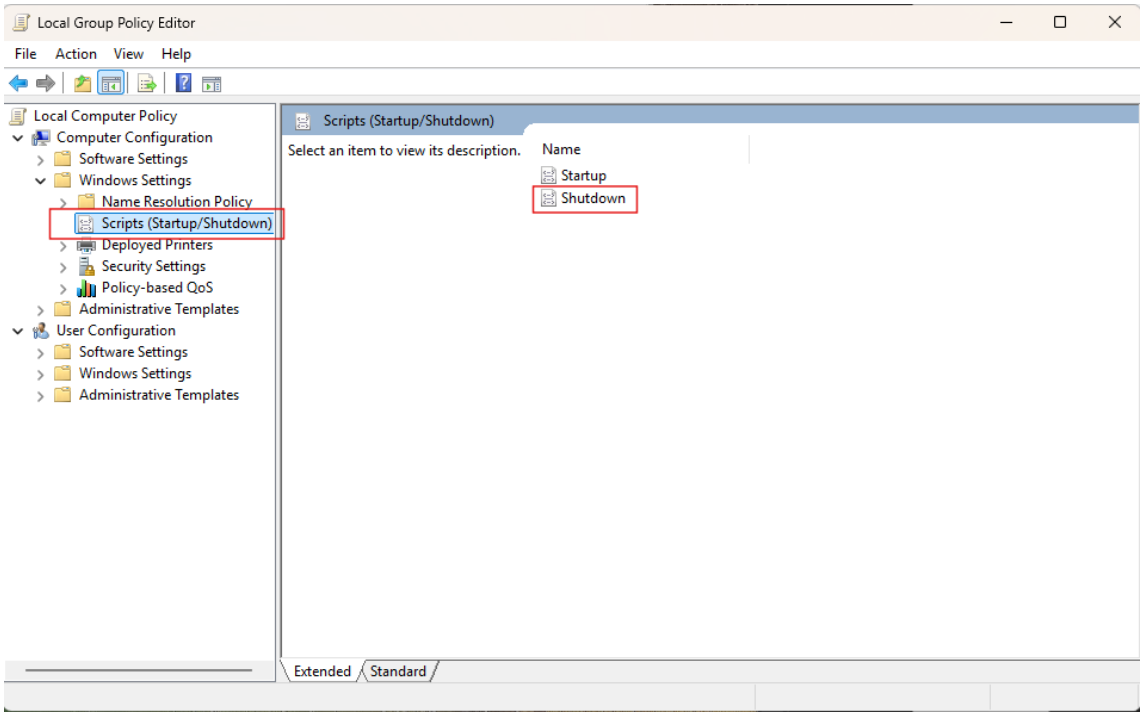
(5) After saving the text file, rename it to **shutdown_tasks.bat**.

Note: Please configure File Explorer to show file extensions.

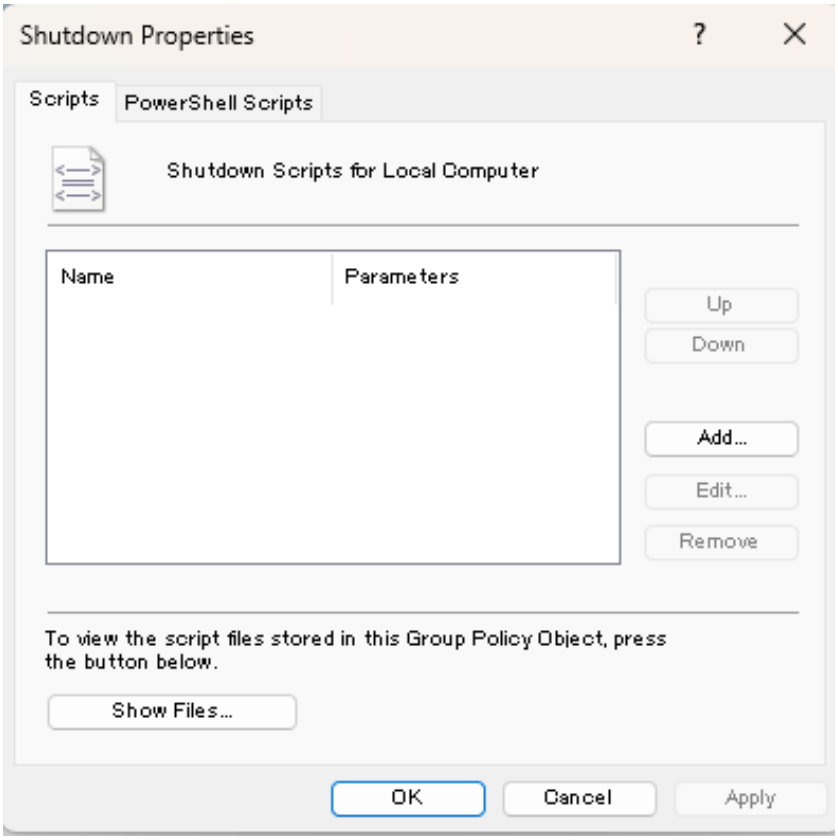
(6) Right-click the **Start** menu and select **"Run"** from the displayed menu. Type **gpedit.msc** into the text box and click the **OK** button to open the **Local Group Policy Editor** window.



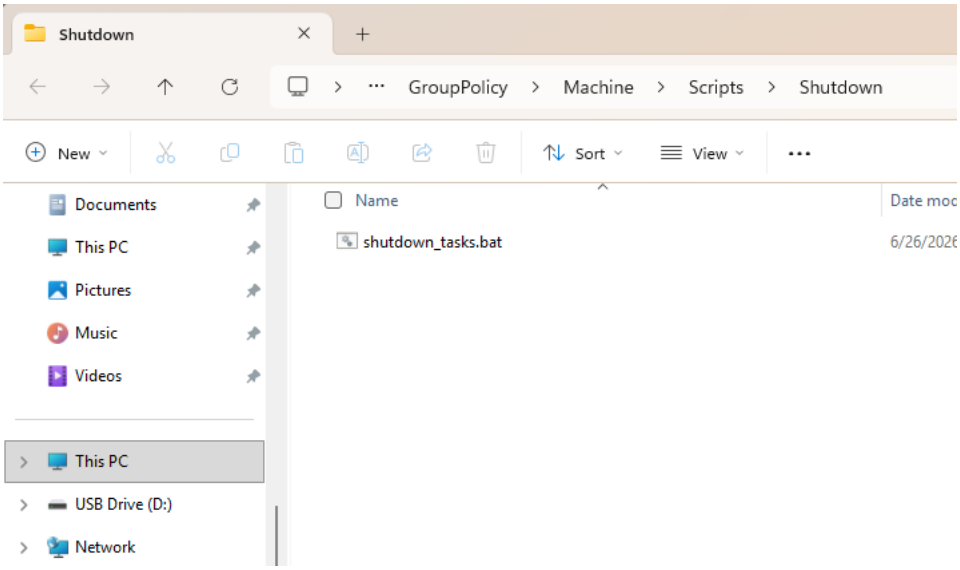
(7) In the left pane of the Local Group Policy Editor window, navigate to **Computer Configuration** > **Windows Settings** > **Scripts (Startup/Shutdown)**. This will display the "Startup" and "Shutdown" items in the right pane. Double-click **Shutdown**.



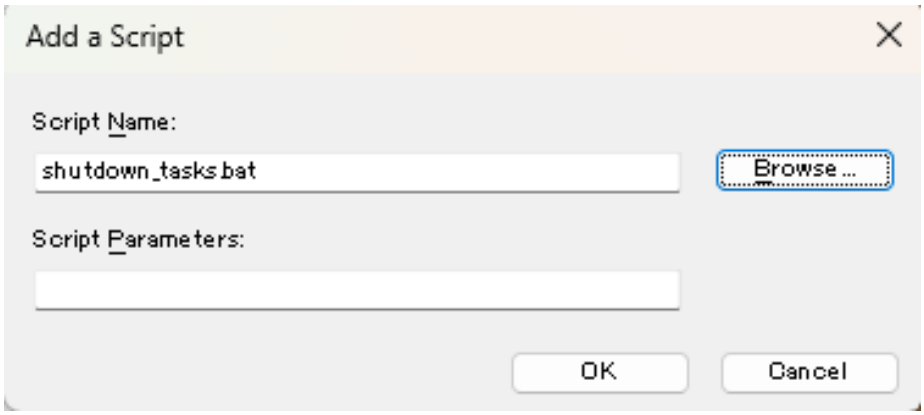
(8) The **"Shutdown Properties"** window will appear.



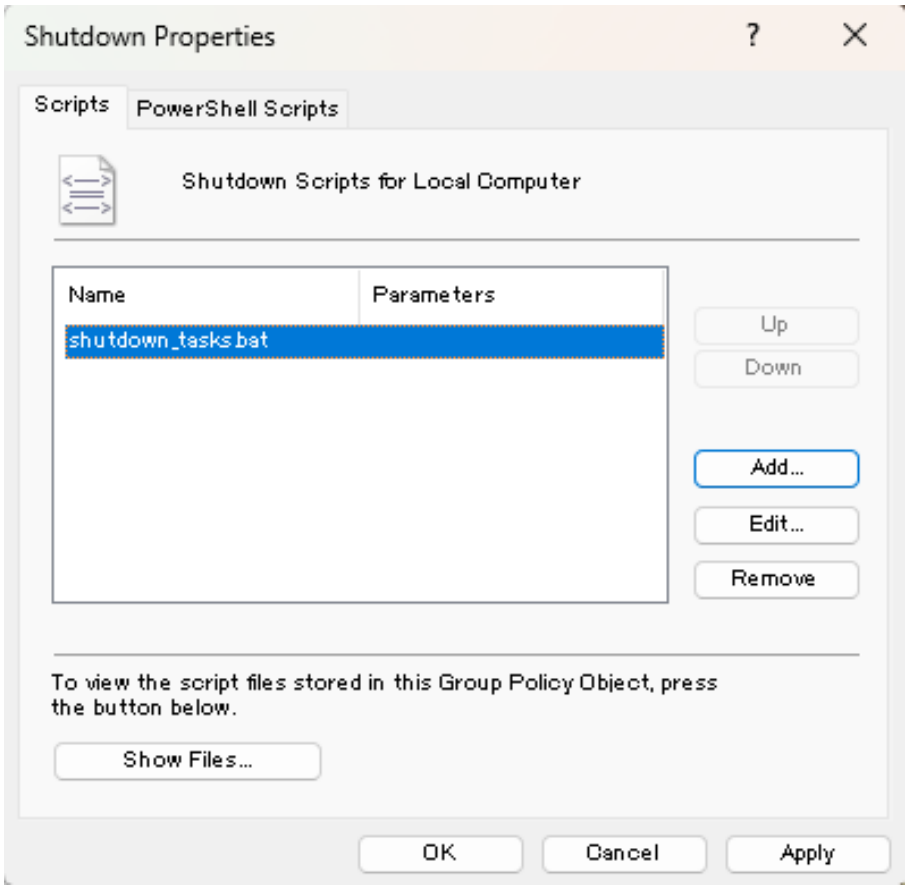
(9) Click the **"Show Files..."** button to open the folder shown below, and copy the **shutdown_tasks.bat** file saved in step (5) into this folder. If a message such as *"You will need to provide administrator permission..."* appears during the copy process, click **"Continue"**. Once the file has been copied, close this folder.



(10) Click the **"Add..."** button in the Shutdown Properties window to open the **"Add a Script"** window. Click the **"Browse..."** button, which will open the folder from step (9). Select **shutdown_tasks.bat** from that folder and click the **"OK"** button.

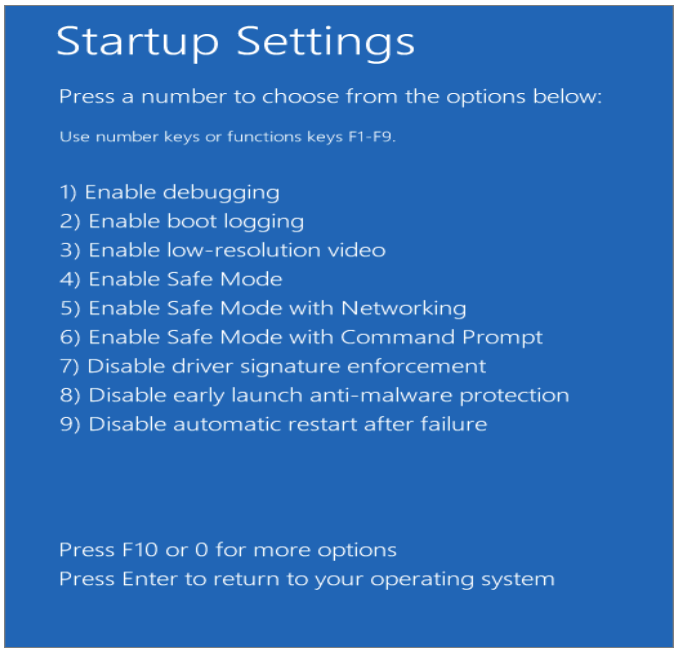


(11) Once you have confirmed that **shutdown_tasks.bat** is registered in the list box of the Shutdown Properties window, click the **"Apply"** button and then the **"OK"** button to close the properties window.

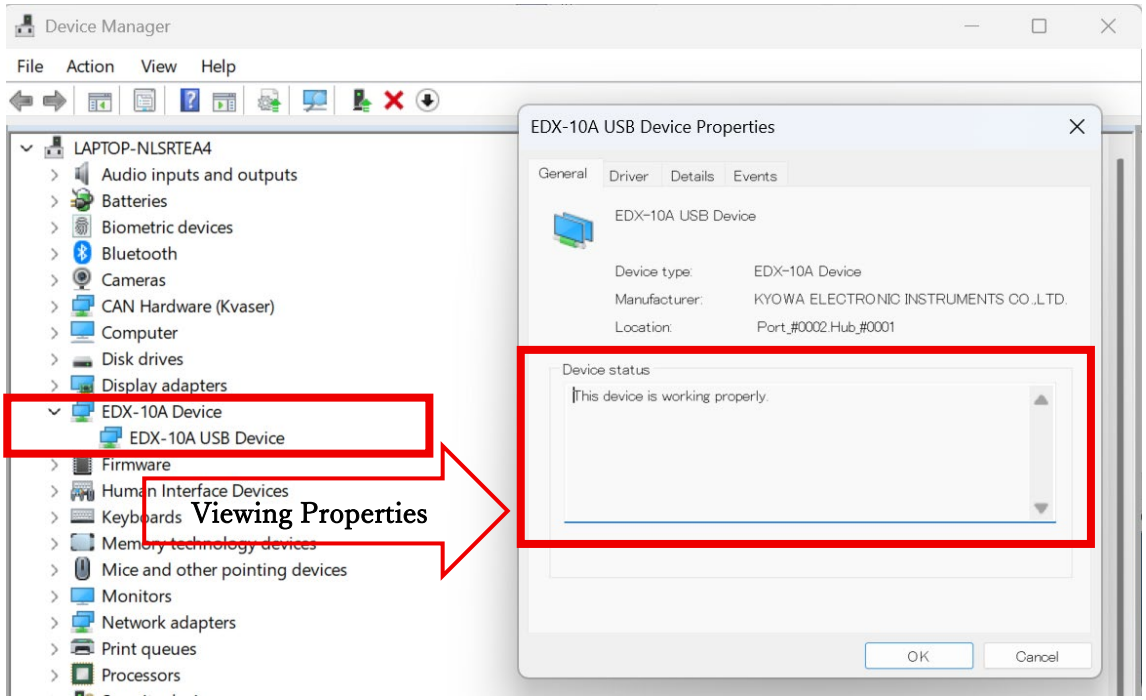


(12) Close the Local Group Policy Editor window. Restart your PC to apply the changes.

(13) When the PC restarts, the **"Startup Settings"** screen shown below will be displayed every time. Select **"7) Disable driver signature enforcement"** (or press the **[7]** or **[F7]** key).



(14) After Windows 11 boots up, the restrictions on the affected device driver will be lifted, making it available for use. If you check Device Manager, you can confirm that the warning icon has been removed from the target measuring instrument's device driver and that it is ready for use (the image below shows the EDX-10 series as an example). *(Please refer to* ***Section 4*** *for details on how to access Device Manager and view Device Properties.)*



7. Procedure for Reverting Interim Workaround ③

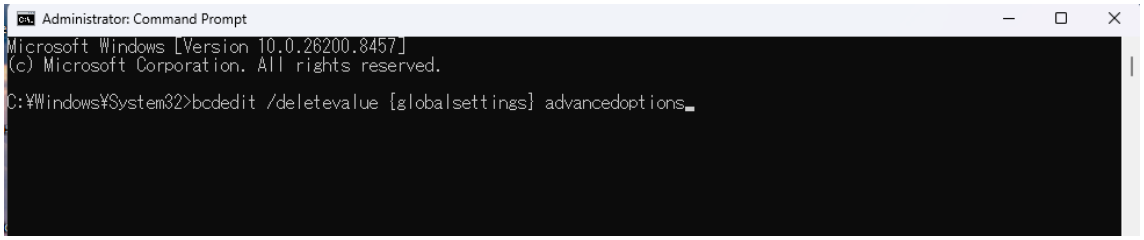
The following steps outline how to revert the settings applied for Interim Workaround ③ in Section 6. If Interim Workaround ③ is no longer required, please follow this procedure to restore your original settings.

7.1. Reverting Settings if BitLocker is "Disabled"

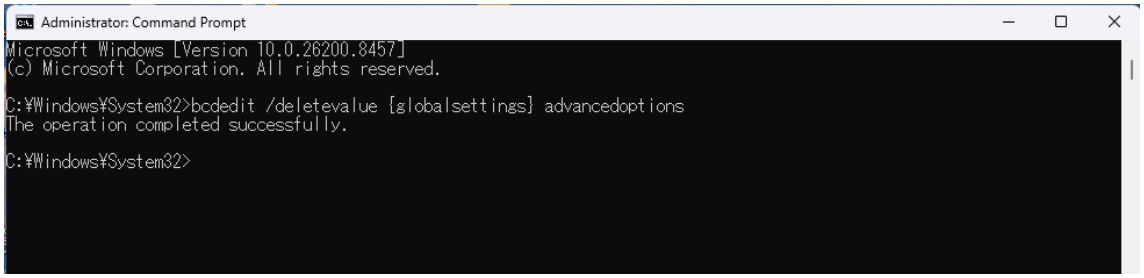
Note: If the BitLocker feature is "Enabled," please refer to Section 7.2.

(1) After booting the PC, launch the Command Prompt with **Administrator privileges**.
Left-click the **Start** button, type **"Command Prompt"** into the search box at the top of the Start menu, and select **"Run as administrator"** from the options displayed.

(2) Type the following command and press the **[ENTER]** key.
bcdedit /deletevalue {globalsettings} advancedoptions



(3) Verify that the message **"The operation completed successfully"** is displayed, and then shut down or restart your PC.



(4) If the "Startup Settings" screen no longer appears when restarting, the settings have been successfully reverted.

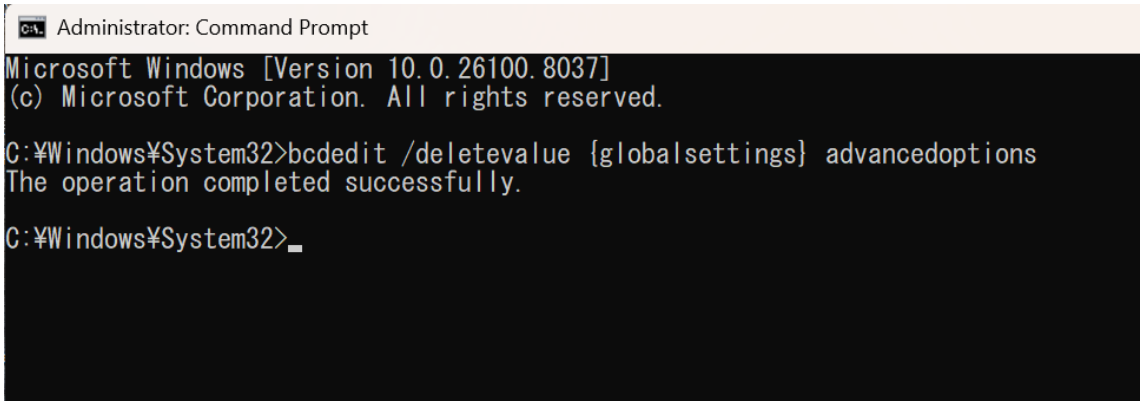
7.2. Reverting Settings if BitLocker is "Enabled"

Note: If the BitLocker feature is "Disabled," please refer to Section 7.1.

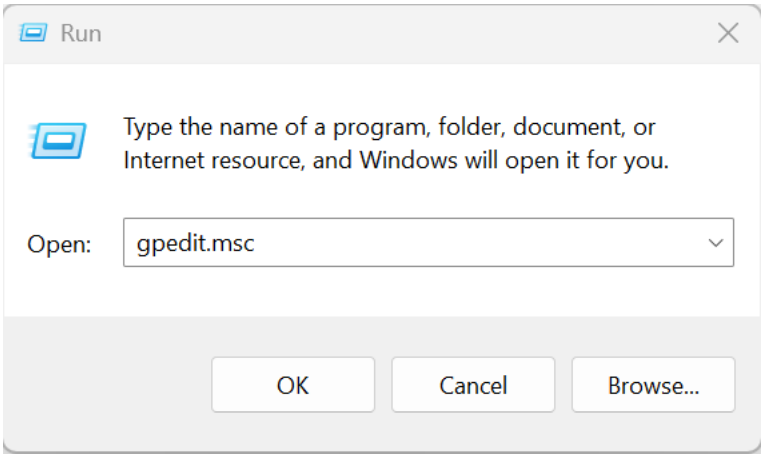
(1) After booting the PC, launch the Command Prompt with **Administrator privileges**.
Left-click the **Start** button, type **"Command Prompt"** into the search box at the top of the Start menu, and select **"Run as administrator"** from the options displayed.

(2) Type the following command and press the **[ENTER]** key.
bcdedit /deletevalue {globalsettings} advancedoptions

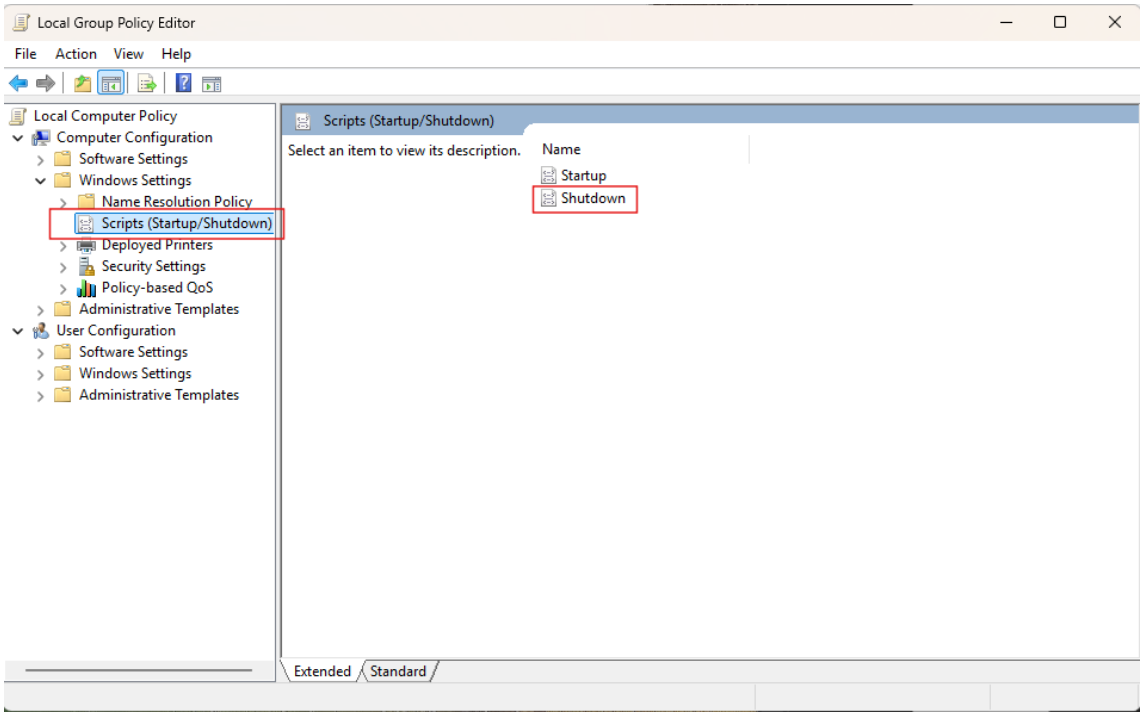
(3) Verify that the message **"The operation completed successfully"** is displayed, and then close the Command Prompt window.



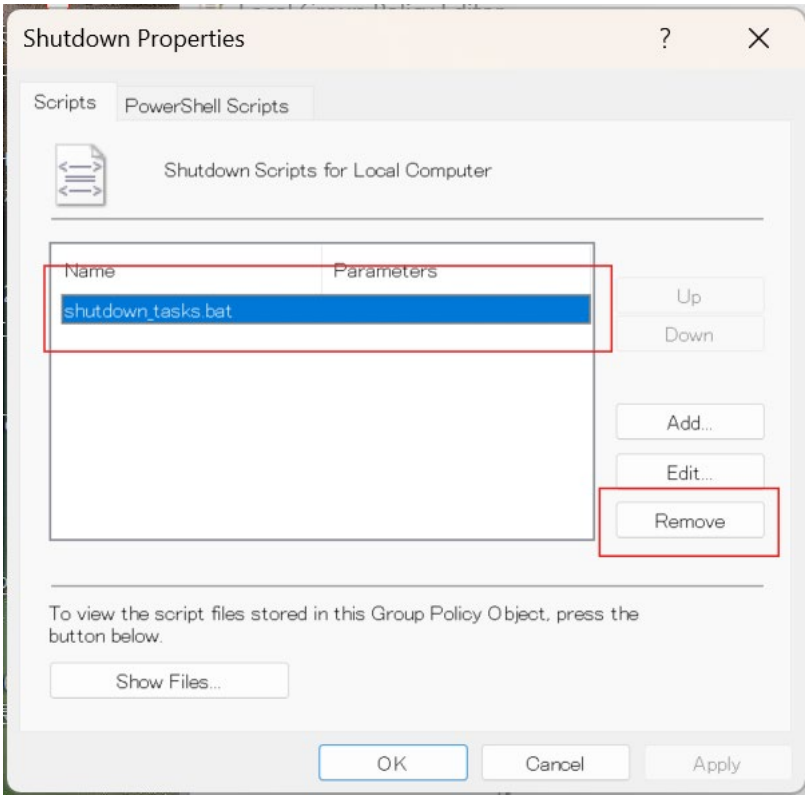
(4) Right-click the **Start** menu and select **"Run"** from the displayed menu. Type **gpedit.msc** into the text box and click the **OK** button to open the **Local Group Policy Editor** window.



(5) In the left pane of the Local Group Policy Editor window, navigate to **Computer Configuration** > **Windows Settings** > **Scripts (Startup/Shutdown)**. This will display the "Startup" and "Shutdown" items in the right pane. Double-click **Shutdown**.



(6) The **"Shutdown Properties"** window will appear. Select **shutdown_tasks.bat** in the list box, and then click the **"Remove"** button.



(7) Confirm that **shutdown_tasks.bat** has been removed from the list box.

(8) Click the **"Show Files..."** button, delete **shutdown_tasks.bat** from the folder that opens, and then close the folder.

(9) Click the **"OK"** button to close the Shutdown Properties window. Then, close the Local Group Policy Editor window as well.

(10) Restart or shut down your PC.

(11) If the "Startup Settings" screen no longer appears when restarting, the settings have been successfully reverted.

8. Important Notes & Precautions

⚠ Important Security Risk Warning > Booting Windows 11 by selecting "7) Disable driver signature enforcement" from the Startup Settings screen (as required by Interim Workaround ③) places the operating system in a vulnerable and less secure state. If you must operate under these settings, please implement the following precautions and limit this mode of operation to the absolute minimum necessary.

- **Disconnect the PC from the network (LAN/Wi-Fi) while using this mode.**
- **Avoid connecting external storage devices (such as USB flash drives) that have not been verified as safe.**

< Returning to Normal Boot Mode >
If you do not select "7)" on the Startup Settings screen and simply press the [ENTER] key, the PC will perform a "Normal" boot. Whenever you are not using the measuring instrument, always ensure you use the PC in this "Normal" boot mode.