Manage DFCI on Surface devices

Article • 01/03/2023 • 11 minutes to read • Applies to: Windows 10, Windows 11

Introduction

With Device Firmware Configuration Interface (DFCI) profiles built into Microsoft Intune, Surface UEFI management extends the modern management stack down to the Unified Extensible Firmware Interface (UEFI) hardware level. DFCI supports zero-touch provisioning, eliminates BIOS passwords, provides control of security settings, including boot options and built-in peripherals, and lays the groundwork for advanced security scenarios in the future. This page lists all DFCI policy settings on eligible Autopilot-deployed Surface devices.

Designed to be used with software-level mobile device management (MDM), DFCI enables IT admins to remotely disable specific hardware components and prevent end users from accessing them. For example, if you need to protect sensitive information in highly secure areas, you can disable the camera, and if you don't want users booting from USB drives, you can disable that also.

> **Tip**
>
> Support for some DFCI policy settings varies by device. Review the **DFCI policy settings reference** on this page and follow **Intune instructions** to configure and deploy settings to your devices.

Prerequisites

- Windows 11 or Windows 10 version 1809 (released November 2018)
- Devices must be registered with Windows Autopilot via one of the following methods:
  - Microsoft Cloud Solution Provider (CSP) partner
  - Directly from Surface

> **Note**

Devices manually or self-registered for Autopilot, such as imported from a CSV file, aren't allowed to use DFCI. By design, DFCI management requires external attestation of the device's commercial acquisition via a Microsoft CSP partner or Surface registration.

DFCI policy settings reference for Surface devices

Eligible devices

- Surface Pro 9 (commercial SKUs only)
- Surface Pro 9 with 5G (commercial SKUs only)
- Surface Pro 8 (commercial SKUs only)
- Surface Pro 7+ (commercial SKUs only)
- Surface Pro 7 (all SKUs)
- Surface Pro X (all SKUs)
- Surface Laptop Studio (commercial SKUs only)
- Surface Laptop 5 (commercial SKUs only)
- Surface Laptop 4 (commercial SKUs only)
- Surface Laptop 3 (Intel processors only)
- Surface Laptop Go
- Surface Laptop Go 2
- Surface Laptop SE
- Surface Book 3
- Surface Go 3 (commercial SKUs only)
- Surface Studio 2+

Note

Surface Pro X doesn't support DFCI settings management for built-in camera, audio, and Wi-Fi/Bluetooth. Some newer settings are only supported on the latest devices.

Table 1. DFCI policy settings reference: Autopilot-deployed Surface devices

DFCI setting	Description	Supported on
UEFI access		
Allow local user to change UEFI (BIOS) settings	This setting lets you manage whether end users can modify UEFI settings on eligible devices. - If you select **Only not configured settings,** local users (also known as end users) may change any UEFI setting *except* any settings that you've explicitly enabled or disabled via Intune. - If you select **None**, local users may not change UEFI settings, including settings not shown in the DFCI profile.	All eligible devices
Security settings		
Simultaneous multithreading	This setting lets you manage whether simultaneous multithreading (SMT) support is enabled on eligible devices. SMT supports Intel hyperthreading technology, which provides two logical processors for each physical core. - If you enable this setting, SMT is turned on in the UEFI layer. - If you disable this setting, SMT is turned off in the UEFI layer. - If you don't configure this setting, SMT is enabled.	All eligible devices
Cameras		
Cameras	This setting lets you manage whether the built-in camera can function on eligible devices. - If you enable this setting, all built-in cameras are allowed. Peripherals, like USB cameras, aren't affected. - If you disable this setting, all built-in cameras are disabled. Peripherals, like USB cameras, aren't affected. - If you don't configure this setting, all built-in cameras are enabled.	- Not supported on Surface Pro X. - Supported on Surface Pro 9 with 5G and all other eligible devices.
Front Camera	This setting lets you manage whether the Front camera can function on eligible devices. - If you enable this setting, the Front camera is allowed. Peripherals, like USB cameras, aren't affected. - If you disable this setting, the Front camera is	- Not supported on Surface Pro X. - Supported on Surface Pro 9 with 5G and all other eligible devices.

DFCI setting	Description	Supported on
	disabled. Peripherals, like USB cameras, aren't affected. - If you don't configure this setting, the Front camera is enabled.	
Rear Camera	This setting lets you manage whether the Rear camera can function on eligible devices. - If you enable this setting, the Rear camera is allowed. Peripherals, like USB cameras, aren't affected. - If you disable this setting, the Rear camera is disabled. Peripherals, like USB cameras, aren't affected. - If you don't configure this setting, the Rear camera is allowed.	- Not supported on Surface Pro X. - Supported on Surface Pro 9 with 5G and all other eligible devices.
Infrared (IR) Camera	This setting lets you manage whether the Infrared camera can function on eligible devices. - If you enable this setting, the Infrared camera is allowed. Peripherals, like USB cameras, aren't affected. - If you disable this setting, the Infrared camera is disabled. Peripherals, like USB cameras, aren't affected. - If you don't configure this setting, the Infrared camera is allowed.	- Not supported on Surface Pro X. - Supported on Surface Pro 9 with 5G and all other eligible devices.
Microphones and speakers		
Microphones and speakers	This setting lets you manage whether on-board audio can function on eligible devices. - If you enable this setting, all built-in microphones and speakers are allowed. Peripherals, like USB devices, aren't affected. - If you disable this setting, all built-in microphones and speakers are disabled. Peripherals, like USB devices, aren't affected. - If you don't configure this setting, microphones and speakers are enabled.	- Not supported on Surface Pro X. - Supported on Surface Pro 9 with 5G and all other eligible devices.
Microphones	This setting lets you manage whether the built-in microphone can function on eligible devices. - If you enable this setting, all built-in microphones are enabled. Peripherals, like USB devices, aren't affected. - If you disable this setting, all built-in microphones are disabled. Peripherals, like USB devices, aren't	- Not supported on Surface Pro X. - Supported on Surface Pro 9 with 5G and all other eligible devices.

DFCI setting	Description	Supported on
	affected. - If you don't configure this setting, microphones are enabled.	
Radios		
Radios (Bluetooth, Wi-Fi, NFC, etc.)	This setting lets you manage whether built-in Bluetooth, Wi-Fi, or 5G wireless can function on eligible devices. - If you enable this setting, all built-in radios are allowed. Peripherals, like USB devices, aren't affected. - If you disable this setting, all built-in radios are disabled. Peripherals, like USB devices, aren't affected. - If you don't configure this setting, all built-in radios are enabled. **TIP:** Configure the category setting **Radios (Bluetooth, Wi-Fi, NFC, etc.)** or the granular settings **Bluetooth, Wi-Fi**. If you configure all the settings, these settings can cause a conflict. For more information, go to DFCI profile overview: Conflicts. **CAUTION:** The **Disable** setting should only be used on devices with a wired Ethernet connection.	- Not supported on Surface Pro X. - Supported on all other eligible devices.
Bluetooth	This setting lets you manage whether built-in Bluetooth can function on eligible devices. - If you enable this setting, Bluetooth is enabled. - If you disable this setting, Bluetooth is disabled. - If you don't configure this setting, Bluetooth is enabled.	- Not supported on Surface Pro X. - Supported on Surface Pro 9 with 5G and all other eligible devices.
WWAN	This setting lets you manage whether built-in WWAN (5G wireless) can function on eligible devices - If you enable this setting, WWAN is enabled. - If you disable this setting, WWAN is disabled. - If you don't configure this setting, WWAN is enabled.	- Not supported on Surface Pro X. - Supported on Surface Pro 9 with 5G and all other eligible devices.
Wi-Fi	This setting lets you manage whether built-in Wi-Fi can function on eligible devices - If you enable this setting, Wi-Fi is enabled.	- Not supported on Surface Pro X. - Supported on Surface Pro 9 with 5G

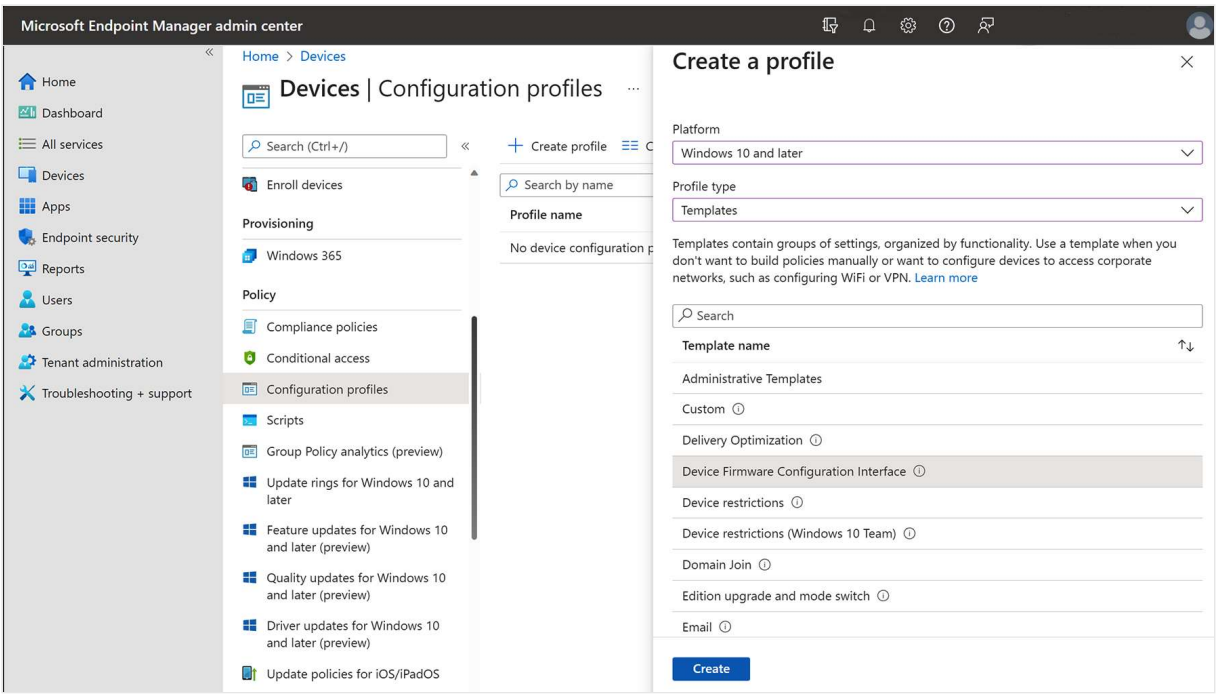
DFCI setting	Description	Supported on
	- If you disable this setting, Wi-Fi is disabled. - If you don't configure this setting, Wi-Fi is enabled.	and all other eligible devices.
Boot options		
Boot from external media (USB, SD)	This setting lets you manage whether eligible devices can be booted from external media. - If you enable this setting, end users can boot the device from USB flash drives or other non-hard drive storage technologies. - If you disable this setting, end users can't boot the device from USB flash drives or other non-hard drive storage technologies. - If you don't configure this setting, end users can boot the device from USB flash drives or other non-hard drive storage technologies.	All eligible devices
Ports		
USB type A	This setting lets you manage how devices can utilize USB-A connections. - If you enable this setting, USB-A data connections can function on eligible devices. - If you disable this setting, USB-A data connections can't function on eligible devices. - If you don't configure this setting, USB-A data connections can function on all devices. **CAUTION:** If you disable both **Boot from external media** and **USB type A**—and the device becomes unbootable for any reason—you won't be able to recover the device without replacing the SSD. You'll be unable to boot from external media and perform a PXE boot or DFCI refresh from the network.	Supported only on Surface Laptop Go 2 and later (devices released after 1 June, 2022).
Wake settings		
Wake on LAN	This setting lets you manage whether eligible devices can be remotely started from Modern Standby or Hibernate. - If you enable this setting, eligible devices can be	Supported only on Surface Laptop Go 2 and later (devices released after 1 June, 2022).

DFCI setting	Description	Supported on
	configured to remotely Wake on LAN. - If you disable this setting, eligible devices can't be configured to remotely wake on LAN. - If you don't configure this setting, eligible devices can be configured to remotely wake on LAN.	
Wake on power	This setting lets you manage whether eligible devices can be automatically started from hibernation or powered-off states when connected to power. - If you enable this setting, eligible Surface devices can be configured to automatically start when connected to power - If you disable this setting, eligible Surface devices can't be configured to automatically start when connected to power. - If you don't configure this setting, eligible Surface devices can't be configured to automatically start when reconnected to power.	Supported only on Surface Laptop Go 2 and later (devices released after 1 June, 2022).

> **Note**
>
> DFCI in Intune includes settings that don't currently apply to Surface devices: CPU and IO virtualization, Disable Boot from network adapters, Windows Platform Binary Table (WPBT), NFC, and SD card.

Get started

1. Sign in to your tenant at endpoint.microsoft.com.
2. In the Microsoft Endpoint Manager Admin Center, select **Devices** > **Configuration profiles** > **Create profile**.
3. Under Platform, select **Windows 10 and later**.
4. Under Profile type, select **Templates** > **Device Firmware Configuration Interface** and then select **Create.**

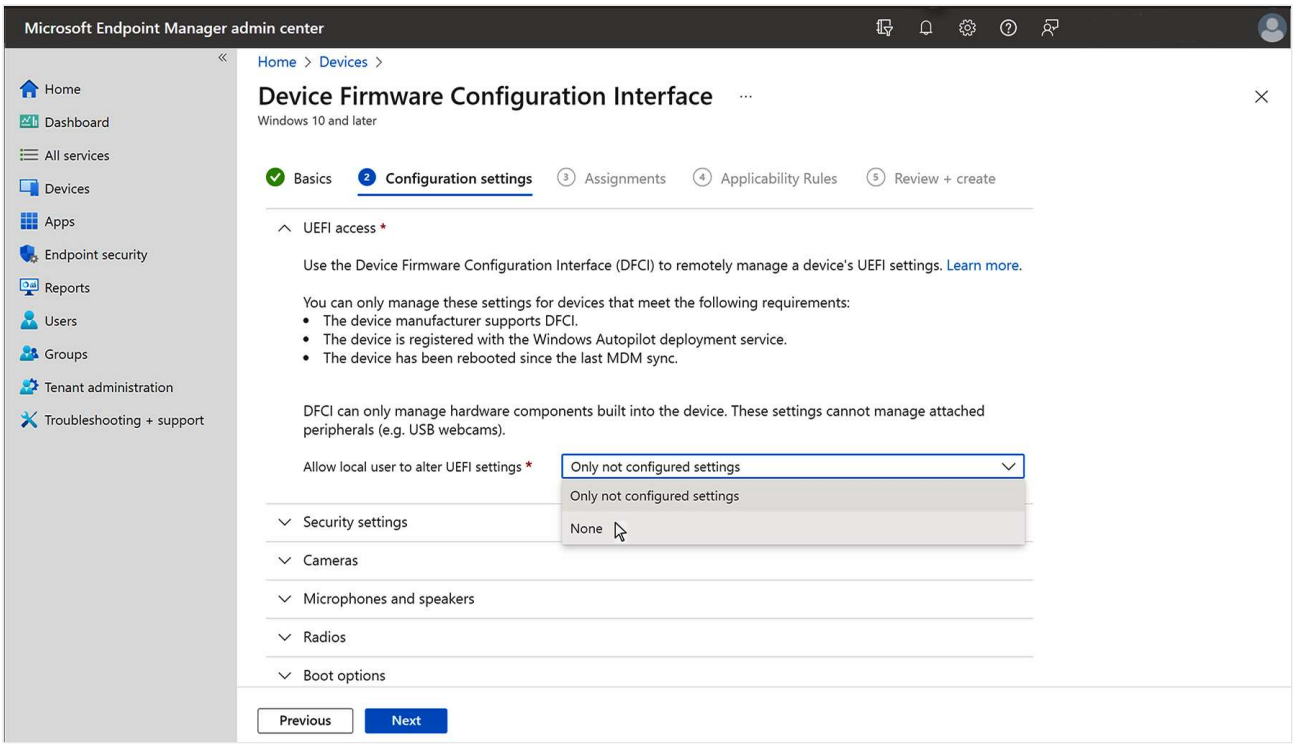


5. See Use DFCI profiles on Windows devices in Microsoft Intune for complete instructions, including:

    - Create your Azure AD security groups
    - Create the profiles
    - Assign the profiles and reboot
    - Update existing DFCI settings
    - Reuse, retire, or recover the device

Prevent users from changing UEFI settings

For many customers, the ability to block users from changing UEFI settings is critically important and a primary reason to use DFCI. As listed above in Table 1, this functionality is managed via the setting **Allow local user to change UEFI settings**. If you don't edit or configure this setting, the local user can change any UEFI setting not managed by Intune. Therefore, it's highly recommended to set **Allow local user to change UEFI settings** to **None.**



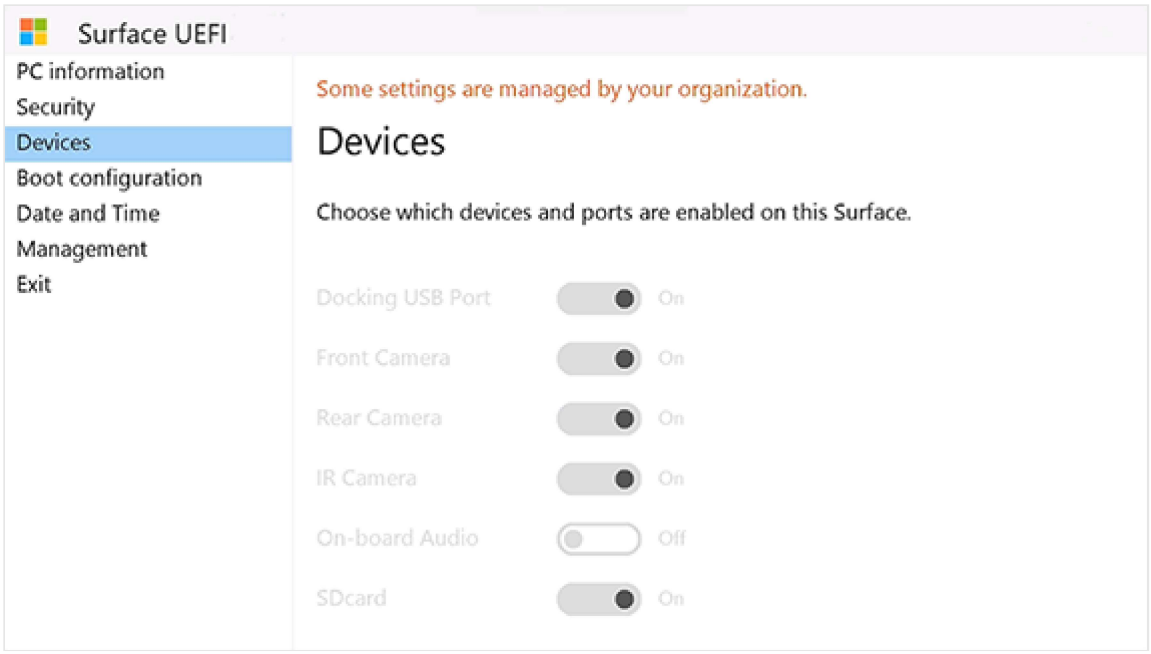
Verify UEFI settings on DFCI-managed devices

In a test environment, you can verify settings in the Surface UEFI interface.

1. Open Surface UEFI:

    - Press and hold the **volume-up button** on your Surface and, at the same time, press and release the **power** button.
    - When you see the Surface logo, release the volume-up button. The UEFI menu will display within a few seconds.

2. Select **Devices**. The UEFI menu will reflect configured settings, as shown in the following figure.



Note:

- The settings are grayed out (inactive) because **Allow local user to change UEFI setting** is set to **None**.
- On-board Audio is set to off because the **Microphones and speakers** policy is set to **Disabled**.

Remove DFCI policy settings

When you create a DFCI profile, all configured settings will remain in effect across all devices within the profile's scope of management. You can only remove DFCI policy settings by editing the DFCI profile directly. If the original DFCI profile has been deleted, create a new profile and edit the appropriate settings.

Removing DFCI management

To remove DFCI management and return device to factory new state:

1. Retire the device from Intune:
   a. In Endpoint Manager at endpoint.microsoft.com, choose **Devices** > **All Devices**.
   b. Select the device you want to retire, then choose **Retire/Wipe.** To learn more, see Remove devices by using wipe, retire, or manually unenrolling the device.
2. Delete the Autopilot registration from Intune:
   a. Choose **Device enrollment** > **Windows enrollment** > **Devices**.

b. Under Windows Autopilot devices, choose the devices you want to delete, then choose **Delete**.

3. Connect the device to wired internet with a Surface-branded ethernet adapter. Restart the device and open the UEFI menu (press and hold the volume-up button while also pressing and releasing the power button).
4. Select **Management** > **Configure** > **Refresh from Network**, and then choose **Opt-out.**

To manage the device with Intune but without DFCI management, self-register it to Autopilot and enroll it in Intune. DFCI won't be applied to self-registered devices.

Learn more

- DFCI Management | Microsoft Docs
- Use DFCI profiles on Windows devices in Microsoft Intune
- DFCI settings for Windows 10/11 in Microsoft Intune
- Windows Autopilot
- Windows Autopilot and Surface devices
- Ignite 2019: Announcing remote management of Surface UEFI settings from Intune