ASUS DFCI Support

Transforming device management landscape for IT admins

ASUS Device Firmware Configuration Interface (DFCI) simplifies deployments, enhances security effortlessly and ensures consistency. Seamlessly configure BIOS settings prior to shipment and gain complete control over device status through Microsoft MDM and Intune dashboard.

Key Values of DFCI

Zero-touch deployment

DFCI is a cutting-edge zero-touch deployment tool for UEFI BIOS settings within the Microsoft Endpoint Manager service.

Robust Security

Ensures impenetrable fortresses, safeguarding data and blocking unauthorized access in a zero-touch remote environment by Windows Autopilot.

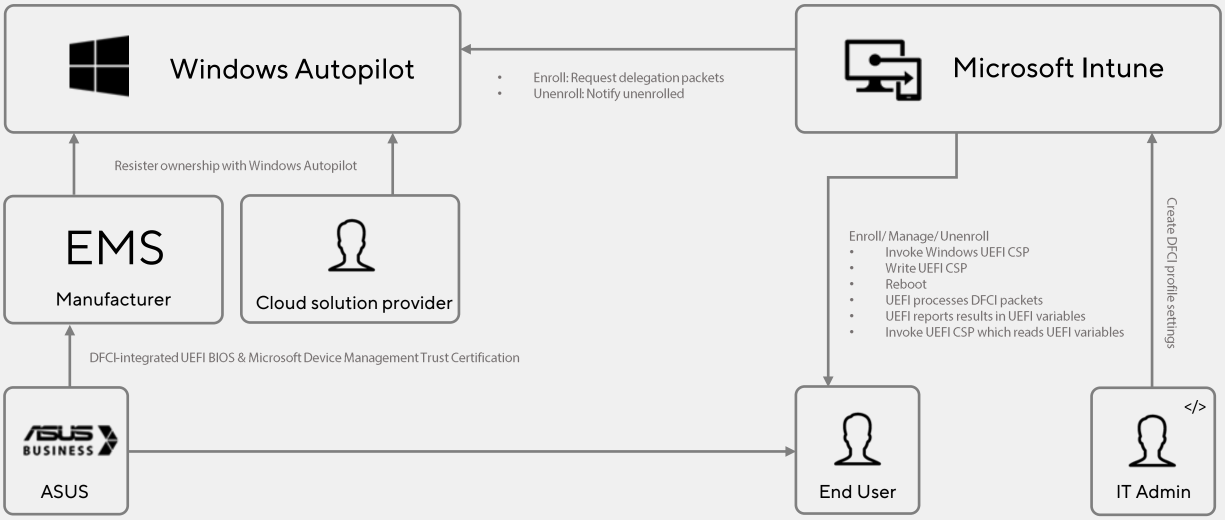
Center of Control

Remotely configure firmware settings across all devices. Ensure consistency, enforce compliance, and streamline device management.

Rapid Efficiency

Accelerates workflows with Autopilot and Microsoft MDM/ Intune, enabling swift configurations. Preload custom images, fine-tune BIOS settings pre-shipment.

How it’s work



Windows Autopilot

- Enroll: Request delegation packets
- Unenroll: Notify unenrolled

Microsoft Intune

Resister ownership with Windows Autopilot

EMS

Manufacturer

Cloud solution provider

Enroll/ Manage/ Unenroll

- Invoke Windows UEFI CSP
- Write UEFI CSP
- Reboot
- UEFI processes DFCI packets
- UEFI reports results in UEFI variables
- Invoke UEFI CSP which reads UEFI variables

Create DFCI profile settings

DFCI-integrated UEFI BIOS & Microsoft Device Management Trust Certification

ASUS

End User

</>

IT Admin

Features & Benefits

Key feature

- Easy settings applicable to all platforms
- Prevent end users control BIOS
- Resilient to malicious attacks
- Limited use the hardware components
- Keep high security even reinstall OS

Benefit for device management

- Maximize BIOS security
- Easy control and configure firmware settings of devices
- Reduce time - consuming process
- Maximize asset utilization
- Comply with specific compliance standards, reduce security vulnerability

Applicable for high-intensity industries

- High-turnover industries
- Data-sensitive sectors
- Asset leasing sectors

Why it’s better

Public key cryptography

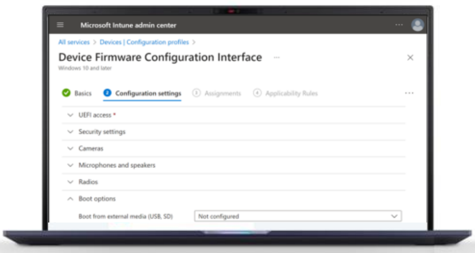
In the trust chain between Microsoft Intune and UEFI firmware ensures secure communication, preventing unauthorized access or manipulation of management commands

User accountability

Reduces the likelihood of user manipulation of UEFI settings, ensuring adherence to organizational security policies and maintaining accountability

Tailored security policies

Offers administrators the flexibility to implement policies aligning with specific organizational security and configuration needs, ensuring adaptability to diverse requirements.



Microsoft Intune admin center

All services > Devices | Configuration profiles >

Device Firmware Configuration Interface

Windows 10 and later

Basics · Configuration settings · Assignments · Applicability Rules

- UEFI access *
- Security settings
- Cameras
- Microphones and speakers
- Radios
- Boot options

Boot from external media (USB, SD): Not configured

Requirements

- Devices must include the DFCI feature in their UEFI
- Devices must be registered to the Windows Autopilot service by an OEM or Microsoft Cloud Solution Provider
- Devices must be managed with Microsoft Intune v2306
- Windows devices with Win10 OS or later