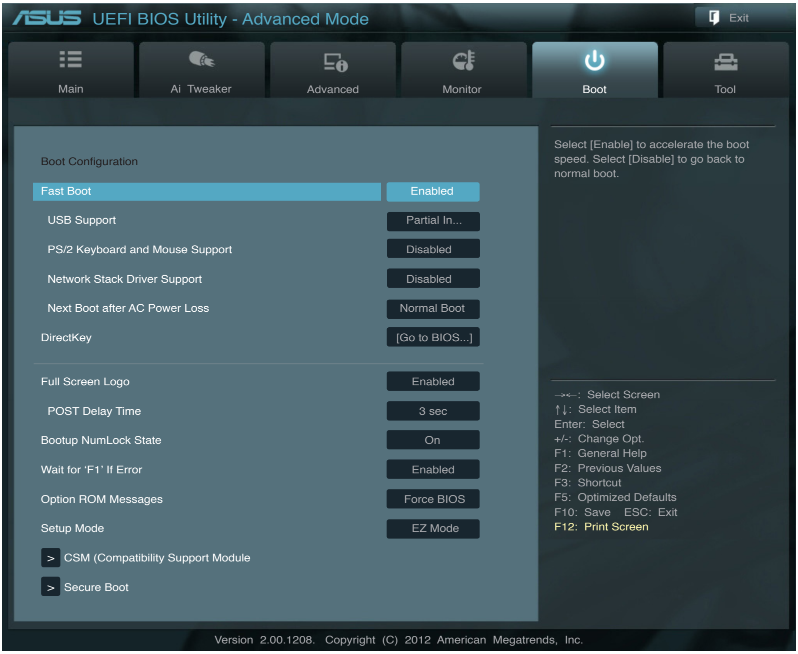
Windows® 8 BIOS Boot settings

The Windows 8® BIOS boot settings allow you to configure the new items of boot options for systems running in Windows® 8 operating system.



Boot Configuration

Fast Boot	Enabled
USB Support	Partial In...
PS/2 Keyboard and Mouse Support	Disabled
Network Stack Driver Support	Disabled
Next Boot after AC Power Loss	Normal Boot
DirectKey	[Go to BIOS...]
Full Screen Logo	Enabled
POST Delay Time	3 sec
Bootup NumLock State	On
Wait for 'F1' If Error	Enabled
Option ROM Messages	Force BIOS
Setup Mode	EZ Mode

> CSM (Compatibility Support Module

> Secure Boot

Select [Enable] to accelerate the boot speed. Select [Disable] to go back to normal boot.

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Shortcut
F5: Optimized Defaults
F10: Save ESC: Exit
F12: Print Screen

Version 2.00.1208. Copyright (C) 2012 American Megatrends, Inc.

Fast Boot [Enabled]

[Enabled]	Select to accelerate the boot speed.
[Disabled]	Select to go back to normal boot.

The following four items appear when you set Fast Boot to [Enabled].

USB Support [Partial Initialization]

[Disabled]	All USB devices will not be available until OS boot up for a fastest POST time.
[Full Initialization]	All USB devices will be available during POST. This process will extend the POST time.
[Partial Initialization]	For a faster POST time, only the USB ports with keyboard and mouse connections will be detected.

PS/2 Keyboard and Mouse Support [Auto]

Select any of these settings when PS/2 keyboard and mouse are installed. These settings only apply when Fast Boot is enabled.

[Auto] For a faster POST time, PS/2 devices will only be available when the system boots up or rebooted when the PS/2 devices have not been reconnected or changed. If you disconnect or change PS/2 devices before restarting the system, PS/2 devices will not be available and BIOS setup program will not be accessible via PS/2 devices.

[Full Initialization] For full system control, PS/2 devices will be available during POST at any circumstances. This process will extend POST time.

[Disabled] For the fastest POST time, all PS/2 devices will not be available until your computer enters the operating system.

Network Stack Driver Support [Disabled]

[Disabled] Select to skip the network stack driver from loading during POST.

[Enabled] Select to load the network stack driver during POST.

Next Boot after AC Power Loss [Normal Boot]

[Normal Boot] Returns to normal boot on the next boot after AC power loss.

[Fast Boot] Accelerates the boot speed on the next boot after AC power loss.

DirectKey [Go to BIOS...]

[Disabled] Disables the DirectKey function. The system will only power on or off when you press the DirectKey button.

[Go to BIOS Setup] Allows the system to power on and go to BIOS Setup directly when you press the DirectKey button.

Full Screen Logo [Enabled]

[Enabled] Enables the full screen logo display feature.

[Disabled] Disables the full screen logo display feature.

Set this item to [Enabled] to use ASUS MyLogo 2™ feature.

POST Delay Time [3 sec]

This item appears only when you set Full Screen Lgo to [Enabled]. This item allows you to select the desired additional POST waiting time to easily enter the BIOS setup. You can only execute the POST delay time during Normal Boot. The values range from 1 to 10 seconds.

This feature will only work under normal boot.

Post Report [5 sec]

This item appears only when you set Full Screen Logo to [Disabled]. This item allows you to select a desired post report waiting time. The values range from 1 to 10 seconds.

CSM (Compatibility Support Module)

Allows you to configure the CSM (Compatibility Support Module) items to fully support the various VGA, bootable devices and add-on devices for better compatibility.

Launch CSM [Auto]

[Auto] The system automatically detects the bootable devices and the add-on devices.

[Enabled] For better compatibility, enable the CSM to fully support the non-UEFI driver add-on devices or the Windows® UEFI mode.

[Disabled] Disable the CSM to fully support the Windows® Security Update and Security Boot.

The following four items appear when you set Launch CSM to [Enabled].

Boot Devices Control [UEFI and Legacy OpROM]

Allows you to select the type of devices that you want to boot up.

Configuration options: [UEFI and Legacy OpROM] [Legacy OpROM only] [UEFI only

Boot from Network Devices [Legacy OpROM first]

Allows you to select the type of network devices that you want to launch.

Configuration options: [Legacy OpROM first] [UEFI driver first] [Ignore]

Boot from Storage Devices [Legacy OpROM first]

Allows you to select the type of storage devices that you want to launch.

Configuration options: [Both, Legacy OpROM first] [Both, UEFI first] [Legacy OpROM first] [UEFI driver first] [Ignore]

Boot from PCIe/PCI Expansion Devices [Legacy OpROM first]

Allows you to select the type of PCIe/PCI expansion devices that you want to launch.

Configuration options: [Legacy OpROM first] [UEFI driver first]

Secure Boot

Allows you to configure the Windows® Secure Boot settings and manage its keys to protect the system from unauthorized access and malwares during POST.

OS Type [Windows UEFI mode]

Allows you to select your installed operating system.

[Windows UEFI mode] Executes the Microsoft® Secure Boot check. Only select this option when booting on Windows® UEFI mode or other Microsoft® Secure Boot compliant OS.

[Other OS] Get the optimized function when booting on Windows® non-UEFI mode, Windows® Vista/XP, or other Microsoft® Secure Boot non-compliant OS. Microsoft® Secure Boot only supports Windows® UEFI mode.

Secure Boot Mode [Standard]

Allows you to select how the Secure Boot prevents unauthorized firmware, operating systems, or UEFI drivers from running during boot time.

[Standard] Allows the system to automatically load the Secure Boot keys from the BIOS database.

[Custom] Allows you to customize the Secure Boot settings and manually load its keys from the BIOS database.

•

This item only appears when you set OS Type item to [Windows UEFI mode]

Key Management

This item appears only when you set Secure Boot Mode to [Custom]. It allows you to manage the Secure Boot keys.

Manage the Secure Boot Keys (PK, KEK, db, dbx)

Install Default Secure Boot keys

Allows you to immediately load the default Security Boot keys, Platform key (PK), Key-exchange Key (KEK), Signature database (db), and Revoked Signatures (dbx). The Platform Key (PK) state will change from Unloaded mode to Loaded mode. The settings are applied after reboot or at the next reboot.

Key-exchange Key (KEK) refers to Microsoft® Secure Boot Key database (KEK).

Clear Secure Boot keys

This item appears only when you load the default Secure Boot keys. This item allows you to clear all default Secure Boot keys.

PK Management

The Platform Key (PK) locks and secures the firmware from any permissible changes. The system verifies the PK before your system enters the OS.

Load PK from File
Allows you to load the downloaded PK from a USB storage device.

Copy PK to File
Allows you to store the PK to a USB storage device.

Delete PK
Allows you to delete the PK from your system. Once the PK is deleted, all the system's Secure Boot keys will not be active.

Configuration options: [Yes] [No]

The PK file must be formatted as a UEFI variable structure with time-based authenticated variable.

KEK Management

The KEK (Key-exchange Key or Key Enrollment Key) manages the Signature database (db) and Revoked Signature database (dbx).

Key-exchange Key (KEK) refers to Microsoft® Secure Boot Key-Enrollment Key (KEK).

Load KEK from File
Allows you to load the downloaded KEK from a USB storage device.

Copy KEK to File
Allows you to store the KEK to a USB storage device.

Append KEK from file
Allows you to load the additional KEK from a storage device for an additional db and dbx loaded management.

Delete the KEK
Allows you to delete the KEK from your system.

Configuration options: [Yes] [No]

The KEK file must be formatted as a UEFI variable structure with time-based authenticated variable.

db Management

The db (Authorized Signature database) lists the signers or images of UEFI applications, operating system loaders, and UEFI drivers that you can load on the single computer.

Load db from File
Allows you to load the downloaded db from a USB storage device.

Copy db from file
Allows you to store the db to a USB storage device.

Append db from file

Allows you to load the additional db from a storage device so that more images can be loaded securely.

Delete the db

Allows you to delete the db file from your system.

Configuration options: [Yes] [No]

The db file must be formatted as a UEFI variable structure with time-based authenticated variable.

dbx Management

The dbx (Revoked Signature database) lists the forbidden images of db items that are no longer trusted and cannot be loaded.

Load dbx from File

Allows you to load the downloaded dbx from a USB storage device.

Copy dbx from file

Allows you to store the dbx to a USB storage device.

Append dbx from file

Allows you to load the additional dbx from a storage device so that more db's images cannot be loaded.

Delete the dbx

Allows you to delete the dbx file from your system.

Configuration options: [Yes] [No]

The dbx file must be formatted as a UEFI variable structure with time-based authenticated variable.