ASUSTeK Computer Inc.

ASUS Configuration Tool

General Frequently Asked Questions

CCBU | Software Team

Document Revision History

Version	Date	Description
01	2023/07/10	First release
02	2023/08/01	2 Modify description 3 Add read DMI settings function 8 Update Appendix C 11 Add Appendix F- table of DMI settings
03	2023/12/22	3.2 Add Boot Logo resolution suggestion 3.4 Add Others - Load BIOS to factory default or custom default 6 Update Appendix A – Scope of Setting 10 Remove Appendix E – TPM Device Selection
04	2024/01/25	6 Update Appendix A – Remove Security Device Support 9 Update Appendix D – Supported Model List
05	2024/04/12	2.4.1. Add password complexity skip command 6 Appendix update for both Intel and AMD
06	2024/09/27	Implement interface 4.0 for BIOS enrollment. 1.1, 1.2 Functions and Environment Update 2.2 ACT 1.4.0.0 Different Situation 2.3 Add migration situation 2.6 Add BIOS Enrollment 3 Add and Update Command Line Usage 3.4 Others – Add asset tag command 6 Update interface 4.0 of Appendix 6 7 Update Appendix B – List of Arguments 9 Update Appendix D – Supported Model List

Table of Contents

1 Introduction

IT administrators are looking for a more efficient way of managing client computers. ASUS Configuration Tool (ACT) combines software and firmware features that provides BIOS configuration capability for ASUS client systems. IT administrators can use this tool to configure BIOS settings, import or export settings, customize boot logo with Command Line and PowerShell.

1.1 Functions

- Read and write available BIOS settings and their values, or restore default settings
- Set or reset BIOS administrator password
- Import and export setup configurations
- Change BIOS boot logo
- Set and clear certificate with BIOS administrator password (Y2024 new function)
- Able to connect with "ASUS Trusted App" for management control (e.g. ASUS Control Center, Ciro)

Note: All functions above require rebooting the device to be activated.

1.2 Supported Environment

- **Supported Operating Systems**

  Windows 10/11
  Windows Preinstallation Environment (Windows PE)

- **Supported Model**

  Commercial Notebooks, Desktops, All-in-One from 2022 or newer that support WMI BIOS. (Intel 12th gen CPU or later.)

- **Prerequisite installations**

  - For ASUS Configuration tool version before 1.0.6.0:
    Please install ASUS Business Utility v3.5.15.0 ~ v3.0.18.0
    Please install ASUS Business Manager v3.0.24.0 ~v3.0.28.0
  - For ASUS Configuration tool v1.0.6.0~v1.3.2.0:
    Please install ASUS Business Utility v3.5.19.0 or later
    Please install ASUS Business Manager v3.0.29.0 or later
  - For ASUS Configuration tool v1.4.0.0 or later:
    Please install ASUS Business System Control Interface (BSCI) v0.4.3.0 or later
    Please install ASUS Business Manager v3.0.32.0 or later

1.3 Scope of Settings

The scope of configurable settings in the BIOS is listed in Appendix A. Please notice that the configurable settings in BIOS may be different in each model.

2 Security and Password

2.1 Different Groups in BIOS Setup Menu

ACT divides BIOS setup menu items into 3 groups:

- General Group: This group consists of the general settings in the BIOS menu that are not security-related.
- Security Group: This group consists of security-related items that would require BIOS administrator password to be able write. The items in this group are listed below:
  - Secure Boot
  - I/O Interface Security
- Password Group:
  - Administrator Password

2.2 Different Situation of a Device under ACT

ACT v1.3.2.0 and before

- Device without BIOS password: This is the default mode upon shipment, where the device has no BIOS password. In this mode, setting the BIOS administrator password is prohibited with the exception of *Trusted Apps*. See Chapter 4 for more information.
  - Able to read all BIOS settings
  - Only able to write settings in General Group
- BIOS password is set **from the BIOS setup menu**: In this situation, user must provide the password to write any settings.
  - Able to read all BIOS settings
  - Able to write settings in General Group and Security Group with password
- BIOS password is set with Trusted App: In this situation, all subsequent operations are protected by Trusted App.
  - Able to read all BIOS settings remotely
  - Able to write settings in General Group and Security Group without password remotely

**The password cannot be read in neither situations above.*

ACT v1.4.0.0 and later

- Default Mode: The device has no BIOS password. Most settings and functions are accessible for reading and writing. However, **we recommend that IT managers secure their devices with a BIOS administrator password after configuring the customized settings.**
- Protected Mode: In this mode, the BIOS admin password is set, offering basic protection. While all users can read the settings, only those with the BIOS administrator password can modify or update BIOS settings and perform enrollment.
- Enrolled Mode: In this mode, the BIOS admin password is set and BIOS provisioning is enrolled. All subsequent operations are protected by a digital signature, ensuring secure modifications.

2.3 Migrate to the Latest ACT/BIOS Interface.

ACT will detect ACT/BIOS interface revision and prompt user if the interface is outdated and need to be migrated to the latest implementation.

Please be noted that the migration is **irreversible** and will be effective after **rebooting**.

- **To migrate to the latest implementation**

```
act.exe --makemigration
```

If ACT detects the migration is required and it could be done automatically in silent mode.

On devices that are password locked, ACT might prompt a message to ask password if the password **could not** be resolved before the migration. ACT will wait for user to input password within 30 seconds. If the password is not given, the migration will not be started.

- **To disable the automatic migration**

  If ACT prompts a message to ask user to confirm the migration, and user wants to disable the migration.

```
act.exe --no_migration [other rest of the options]
```

2.4 Password Management

ACT can create an encrypted password file that saves the BIOS administrator password which can be used as a more secure method than plaintext passwords, though both plaintext and password file are applicable. The BIOS administrator password needs to be a set of strong password, see chapter 2.5 for detailed requirements. If the BIOS is reset, e.g. Factory reset, the created password file becomes invalid, but the BIOS is still protected by the same set of password. To counter an invalid password file, the user can create an entirely new password file.

To create, renew, or clear the password file, use the commands as follows:

2.4.1 Create a Password File

Arguments:

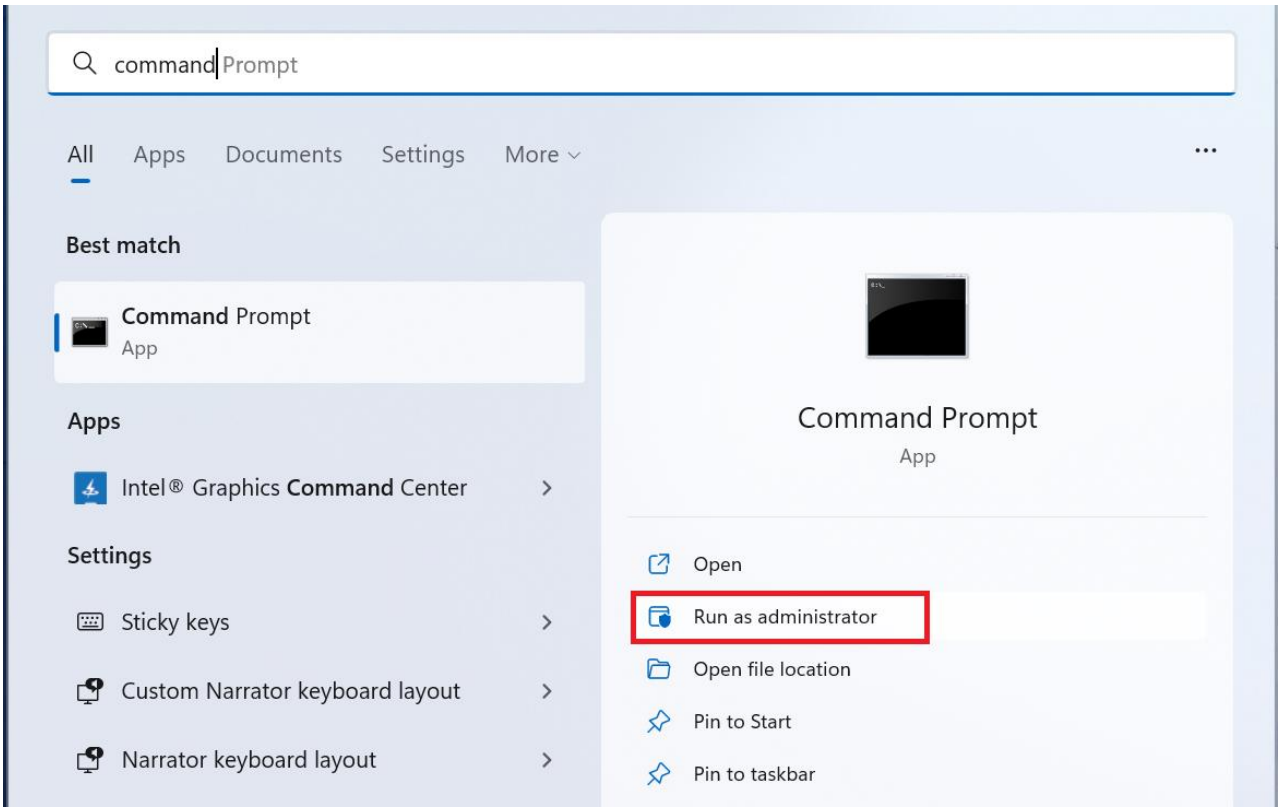
```
--newpwd <A strong password>
--output, -o <path to password file that will be created>
```

Command:

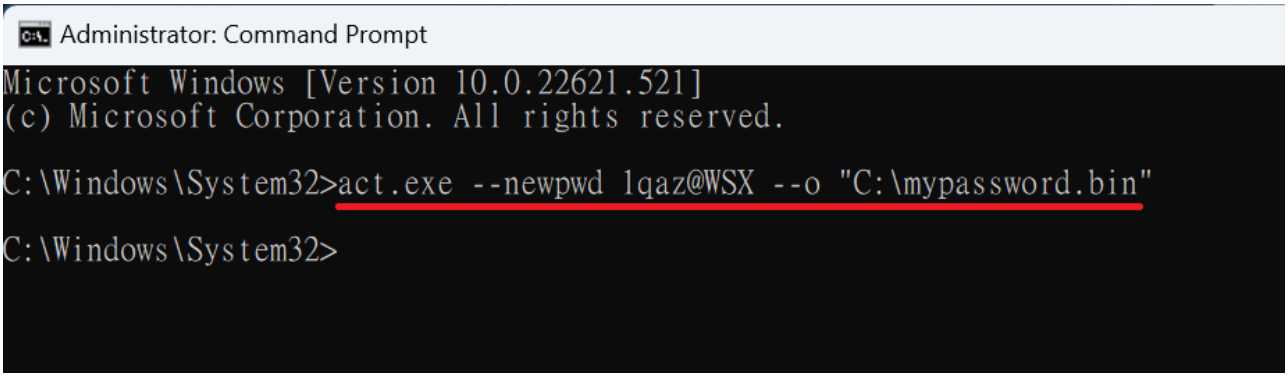
```
act.exe --newpwd <$YOUR_PASSWORD> --o "<$PATH_TO_PASSWORD_FILE>\mypassword.bin"
```

Example:

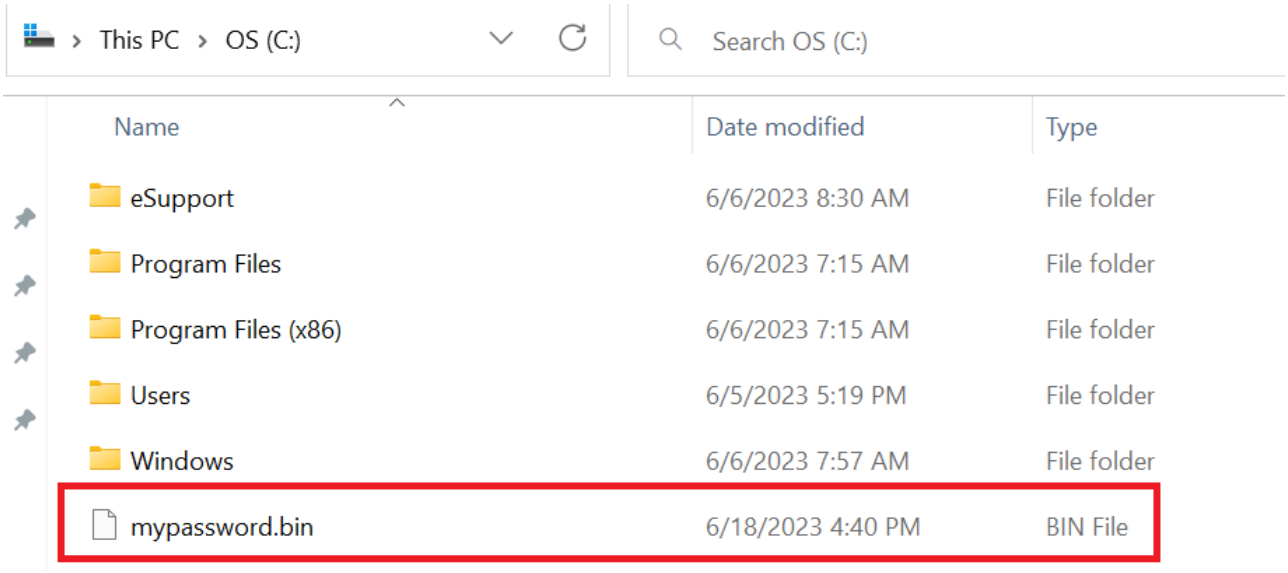
***Please remember to run the Command Prompt with administrator privileges.**



Create an encrypted password file, named `mypassword.bin`, to protect the password `"1qaz@WSX"`.



The “mypassword.bin” file will be automatically built in the specified path.



2.4.2 Renew Password File

Arguments:

`--renewpwd <A strong password>`

`--pwd, -p <path to an existing password file>`

`--signingkey <path to signing key file which is the RSA private key>`

`--signature <signature encoded in base64 for enrolled device>`

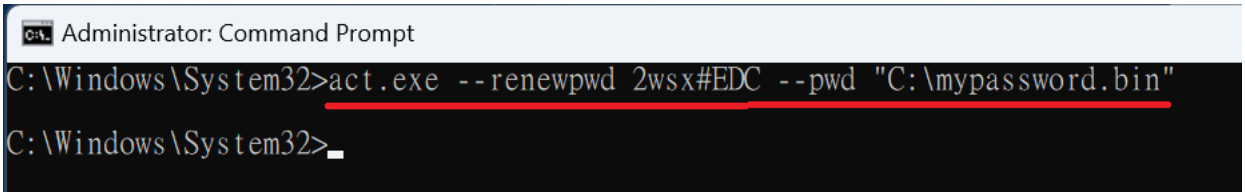
Command:

```
act.exe --renewpwd <$YOUR_NEW_PASSWORD> --pwd mypassword.bin
```

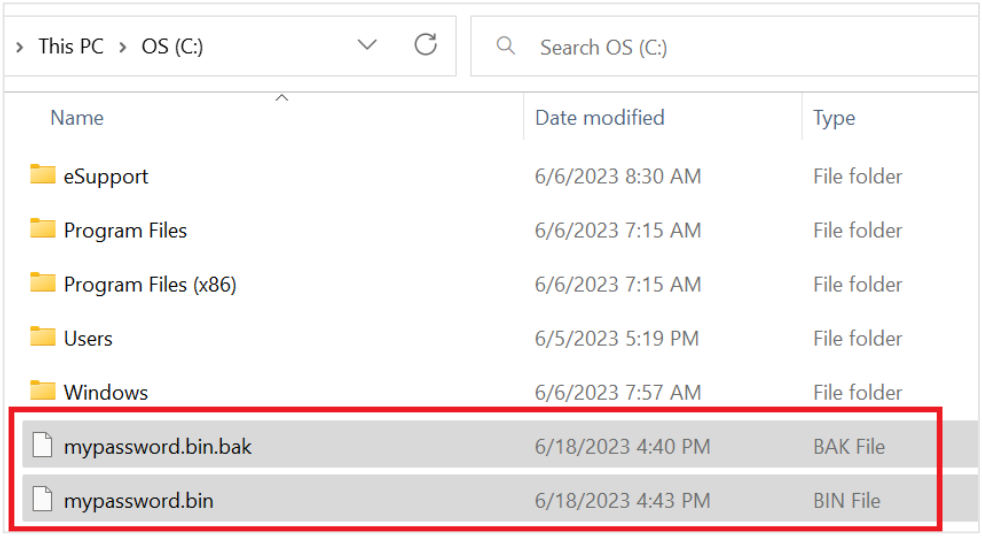
Example:

`mypassword.bin` is an encrypted password file created by command `--newpwd`.

Use the following example to renew it with a fresh password `"2wsx#EDC"`.



When a password file is renewed, ACT will automatically create a backup password file of the old password. E.g., “mypassword.bin.bak”.



Command:

When the device is enrolled. Renew password to `hmIC$4g691$T` with current password `eg5*7jV3N274`. Signature is calculated real-time based on the given private key `private.2048.pem`:

```
act.exe --renewpwd hmIC$4g691$T --pwd eg5*7jV3N274 --signingkey prive.2048.pem
```

For signature is pre-calculated and encoded in base64 string, `P4hFwQAELjI…r0vY1xLg==`:

```
act.exe --renewpwd hmIC$4g691$T --pwd eg5*7jV3N274 --signature P4hFwQ…1xLg==
```

2.4.3 Clear Password File

Arguments:

`--clrpwd`

`--pwd, -p <password in plaintext, or a file path to an existing password file>`

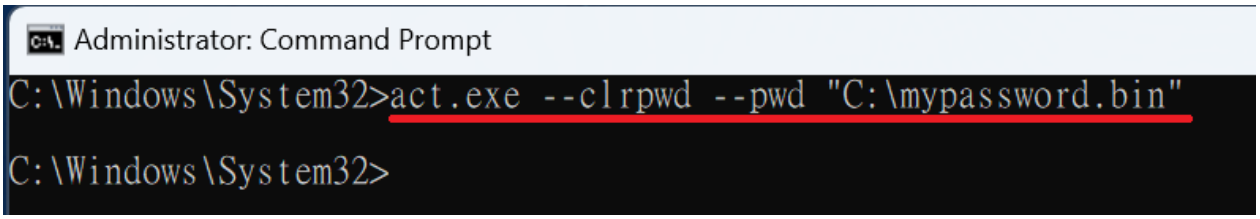
Command:

```
act.exe --clrpwd --pwd mypassword.bin
```

Example:

`mypassword.bin` is an encrypted password file created by command `--newpwd`.

The function bellow will clear the bios administrator password, and will also delete the password bin file.



2.5 Strong Password Requirements

The requirements for the BIOS administrator password are as follows:

- Password Length: 8~20 characters
- At least one lower case character: [a-z]
- At least one upper case character: [A-Z]
- At least one digit character: [0-9]
- At least one special character: [?=.*[!\"#$%&'()*+\\\\,-.\\/:;<=>?@\\[\\]^_`{|}~]

2.5.1 Password Complexity Check

Since 2024H2, ASUS BIOS starts to support whether to activate the password complexity check. ACT hence is allowed to set simple password if there is the requirement and its BIOS setting has been modified.

Arguments:

`--skip_password_complexity_check <To deactivate password complexity>`

```
act.exe --newpwd <$YOUR_SIMPLE_PASSWORD> --skip_password_complexity_check
```

Example:

Create a simple password `1234` to deactivate the password complexity that aligned with BIOS setting.

```
act.exe --newpwd 1234 --skip_password_complexity_check
```

Renew the simple password `1234` with another simple password `5678`.

```
act.exe --renewpwd 5678 --pwd 1234 --skip_password_complexity_check
```

2.6 BIOS Enrollment

From ACT v1.4.0.0 and later, ACT implements certificate to ensure secure communication and data encryption. User can enroll key pair to BIOS to authenticate devices, ensuring that only authorized hardware can interact with the BIOS.

Step1. Prepare Key Pair (If no existing key pair is available)

The key pair needs to be a **RSA** key pair with **2048-bit** length created by **OpenSSL** utility.

User is responsible to manage the key pair and keep the private key protected.

Example:

To create a 2048-bit RSA key pair by OpenSSL.

First, creating a private key using passphrase `private.2048.pem` to protect the private key.

```
.\openssl.exe genrsa -des3 -out private.2048.pem 2048
```

Second, extracting the public key `public.2048.pem` from the private key.

```
.\openssl.exe rsa -in private.2048.pem -outform PEM -pubout -out public.2048.pem
```

Now you have a key pair: private.2048.pem(private key) and public.2048.pem(public key).

Step2. Enroll Public Key

Before enrolling a public key, user needs to ensure **BIOS administrator password is installed** in the device. This step can also be used to **update** the public key if it is already enrolled.

Arguments:

```
--enroll <path to public key>
--pwd <BIOS admin password in plaintext or a path to password file>
```

```
act.exe --enroll <$PATH_TO_PUBLIC_KEY_FILE > --pwd <$YOUR_PASSWORD>
```

Example:

Enroll `public.2048.pem`. Password is `eg5*7jV3N274`.

```
act.exe --enroll public.2048.pem --pwd eg5*7jV3N274
```

Step3. Revoke Public Key

This step is used to revoke public key. User needs the admin password to revoke public key.

To renew public key, user needs to revoke it then enroll again.

Arguments:

```
--revoke
--pwd <BIOS admin password in plaintext or a path to password file>
```

```
act.exe --revoke --pwd <$YOUR_PASSWORD>
```

Example:

Revoke the enrollment. Password is `eg5*7jV3N274`.

```
act.exe --revoke --pwd eg5*7jV3N274
```

3 Command Line Interface Usage

This chapter provides a general overview of the usage of ACT with Command Line Interface.

3.1 Read and Write Settings

3.1.1 Read BIOS/DMI Settings

To read BIOS/DMI settings, use the "`--get`" or "`-r`" command and the current settings will show in the console; or it can also be saved into a JSON file for later configuration with "`--output`" or "`-o`" command; To search items that are in a particular page or search with certain keywords, use the "`--filter`" command. See Appendix F for all displayable DMI settings.

Arguments:

```
--get, -r
[--output, -o <file path to BIOS configuration file that will be created>]
[--filter <Item Filter>]
[--pwd, -p <password in plaintext, or a file path to an existing password file>]
```

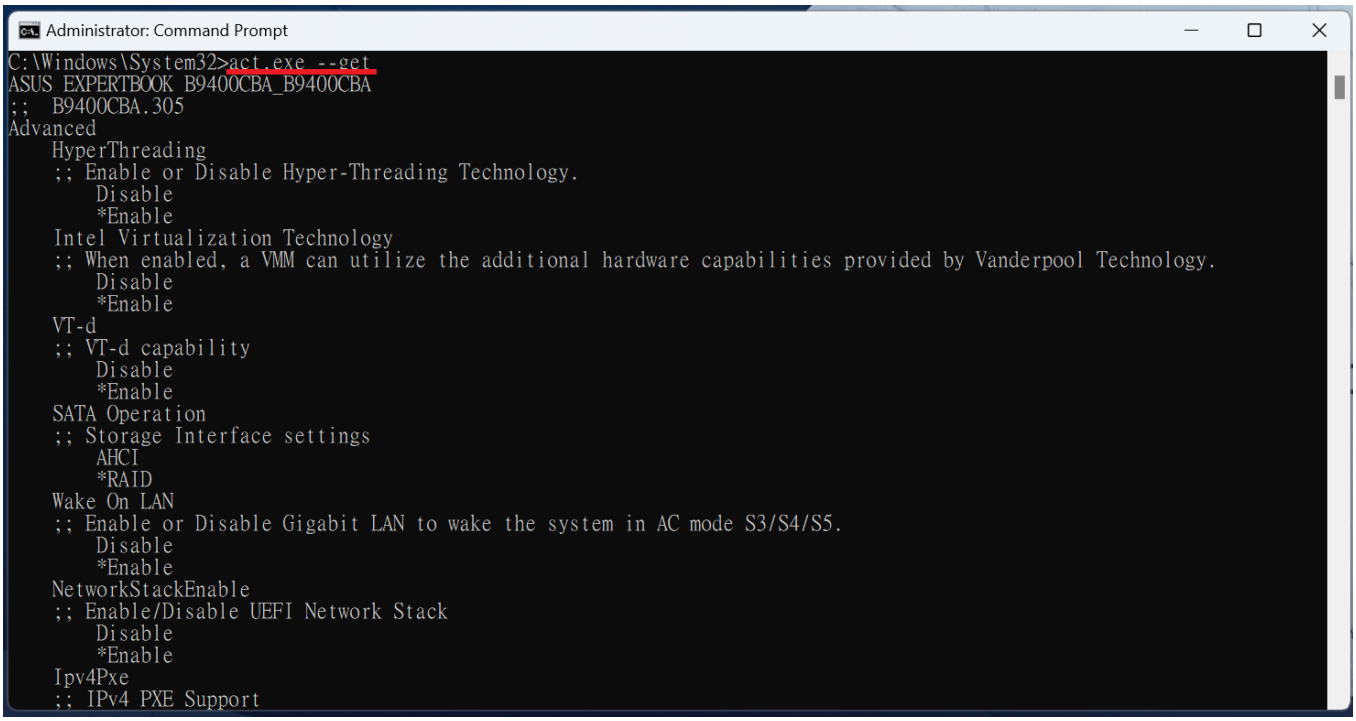
- **Read entire BIOS/DMI settings**

Command:

```
act.exe --get
```

Example:

The displayed information is as follows:

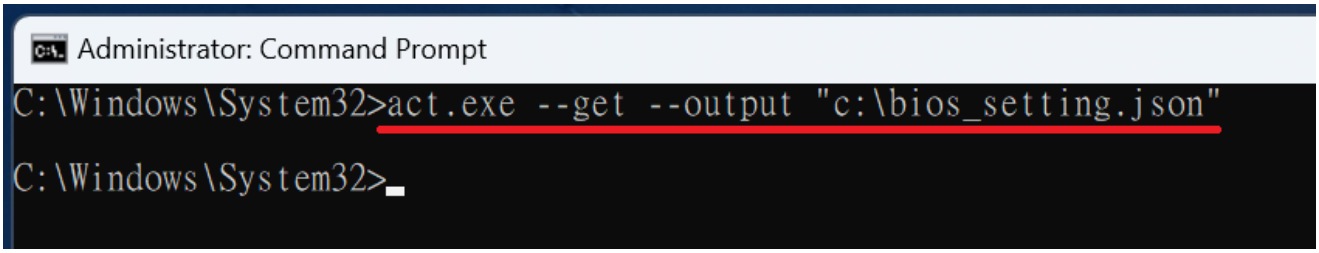


- **Read entire BIOS/DMI settings and save as a JSON file format**

Command:

```
act.exe --get --output "<$PATH_TO_JSON_FILE>\bios_setting.json"
```

Example:



3.1.2 Read BIOS Settings with Filter

This chapter explains the usage of the "`--filter`" argument and its' expressions.

Filter BIOS settings

Arguments:

`[--filter <Item Filter>]`

`<Item Filter>` expression contains: /Page Name/ + Item Name

Use slashes "/" to define BIOS settings pages, and use stars "*" to fuzzy search.

The name of the BIOS setup items are case-sensitive.

Command:

- **Show items only on the "Boot" page and filter other pages**

```
act.exe --get --filter "/Boot/*"
```

- **Show BIOS item "FastBoot" on the "Boot" page**

```
act.exe --get --filter "/Boot/FastBoot"
```

- **Show BIOS item name preceding with "Fast" on the page name preceding with "Boo"**

```
act.exe --get --filter "/Boo*/Fast*"
```

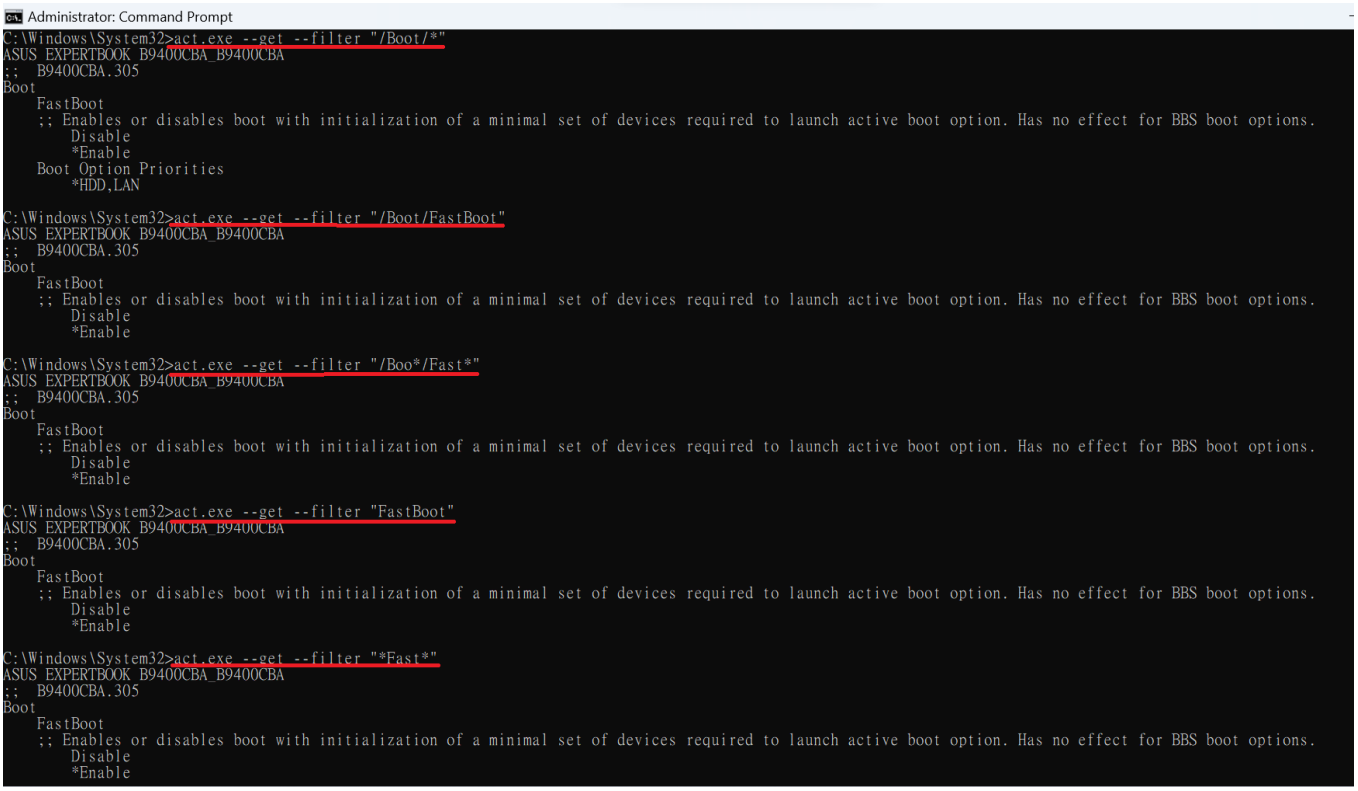
- **Show BIOS item name "FastBoot", disregarding which page it belongs to**

```
act.exe --get --filter "FastBoot"
```

- **Show BIOS item name that contains the text "Fast"**

```
act.exe --get --filter "*Fast*"
```

Example:



Filter DMI settings

Arguments:

`[--filter <Item Filter>]`

`<Item Filter>` expression contains: Item Name

Use stars “*” to fuzzy search.

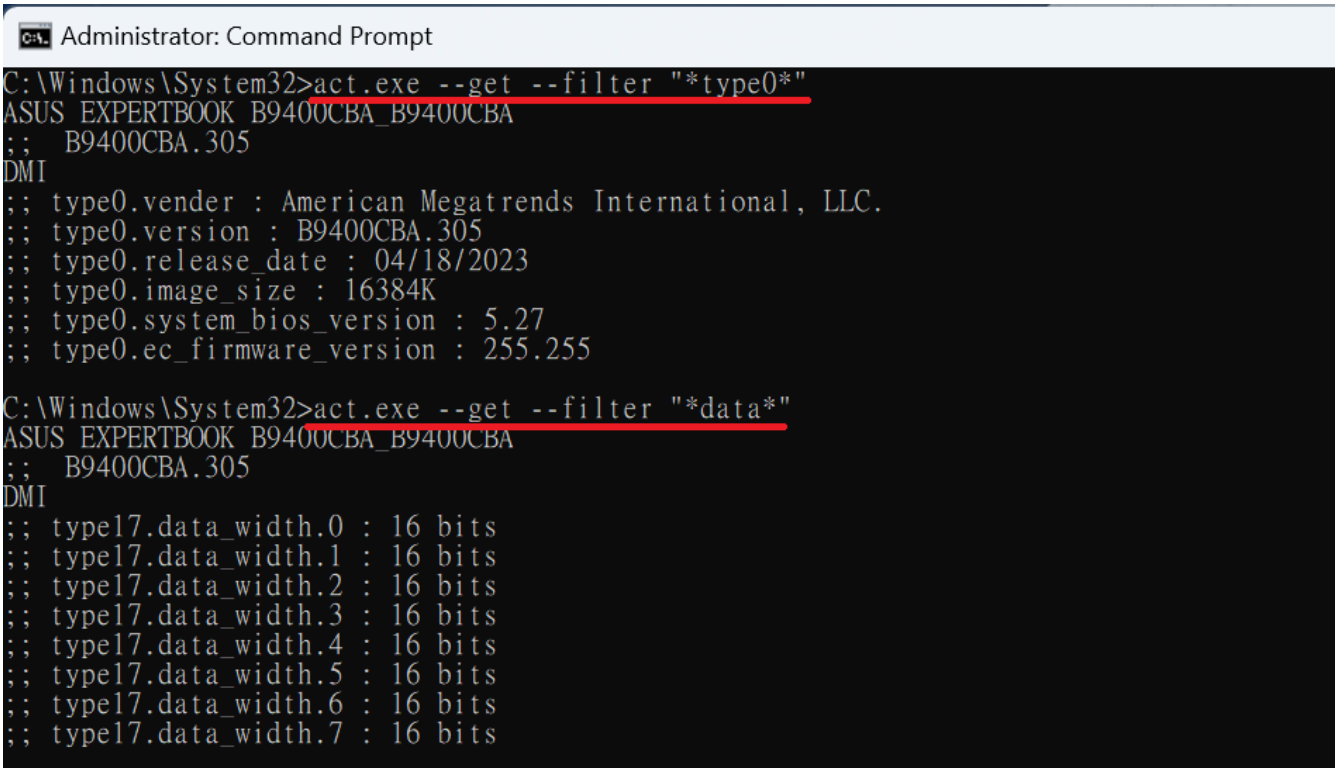
Example:

- **Show DMI items belonging to "type0"**

```
act.exe --get --filter “*type0*”
```

- **Show DMI items name that contains the text “data”**

```
act.exe --get --filter “*data*”
```



3.1.3 Write BIOS Settings

Use the "`--set`" command to apply a BIOS configuration file, which is a JSON file that is collected beforehand with the command "`--get --output bios_setting.json`". The JSON file can be edited to the users' preference, then apply it to ACT with the "`--set`" command.

If the BIOS administrator password is set, it is mandatory to provide the password or password file.

DMI information can only be read, and cannot be written through the .json file.

Arguments:

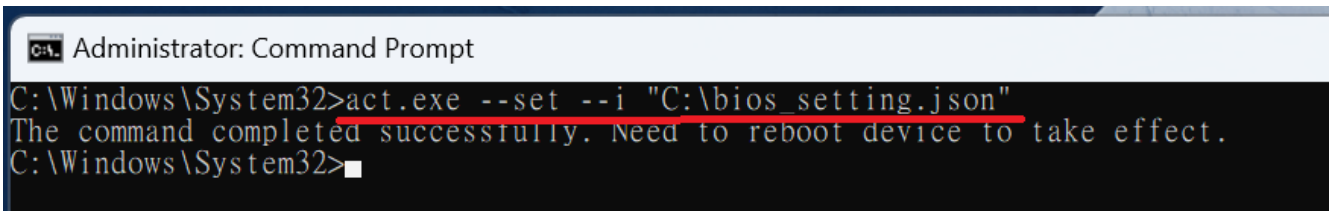
```
--set, -w
[--input, -i <path to BIOS configuration file>]
[--pwd, -p <password in plaintext, or a file path to an existing password file>]
[--signingkey <path to signing key file which is the RSA private key>]
```

- **Apply entire BIOS settings in the configuration file**

Command:

```
act.exe --set --input "<$PATH_TO_JSON_FILE>\bios_setting.json"
```

Example:



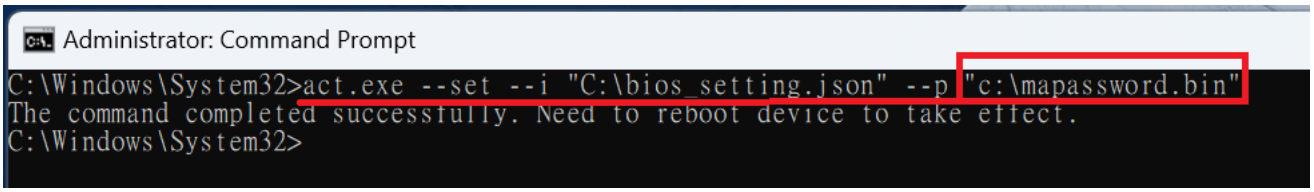
- **Apply entire BIOS settings in the configuration file when BIOS administrator password is set**

Command:

Apply with password file.

```
act.exe --set --i "<$PATH_TO_JSON_FILE>\bios_setting.json" --p mypassword.bin
```

Example:

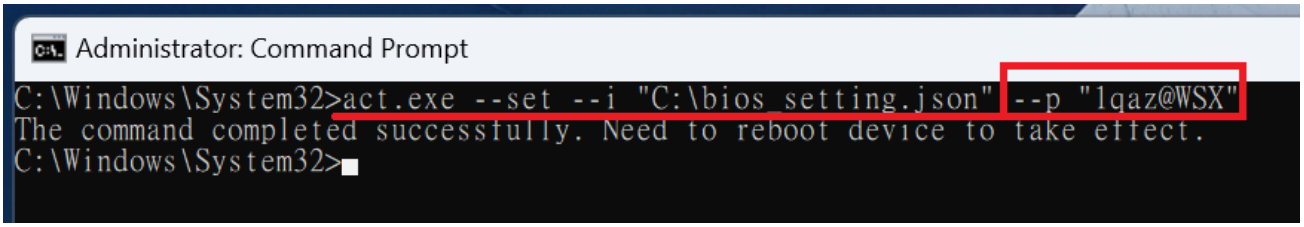


Command:

Apply with plaintext password.

```
act.exe --set --i "<$PATH_TO_JSON_FILE>\bios_setting.json" --p $YOUR_PASSWORD
```

Example:



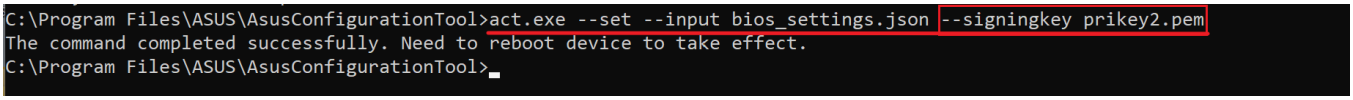
- **Apply entire BIOS settings in the configuration file when BIOS is enrolled.**

Command:

Apply with signing key `private.2048.pem`.

```
act.exe --set --input bios_setting.json --signingkey private.2048.pem
```

Example:

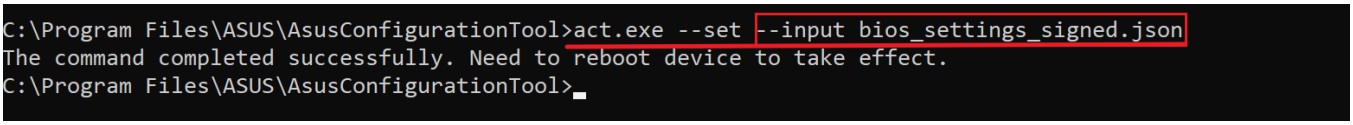


Command:

Apply all settings and all settings specified in configuration file are **signed** properly.

```
act.exe --set --input bios_setting_signed.json
```

Example:

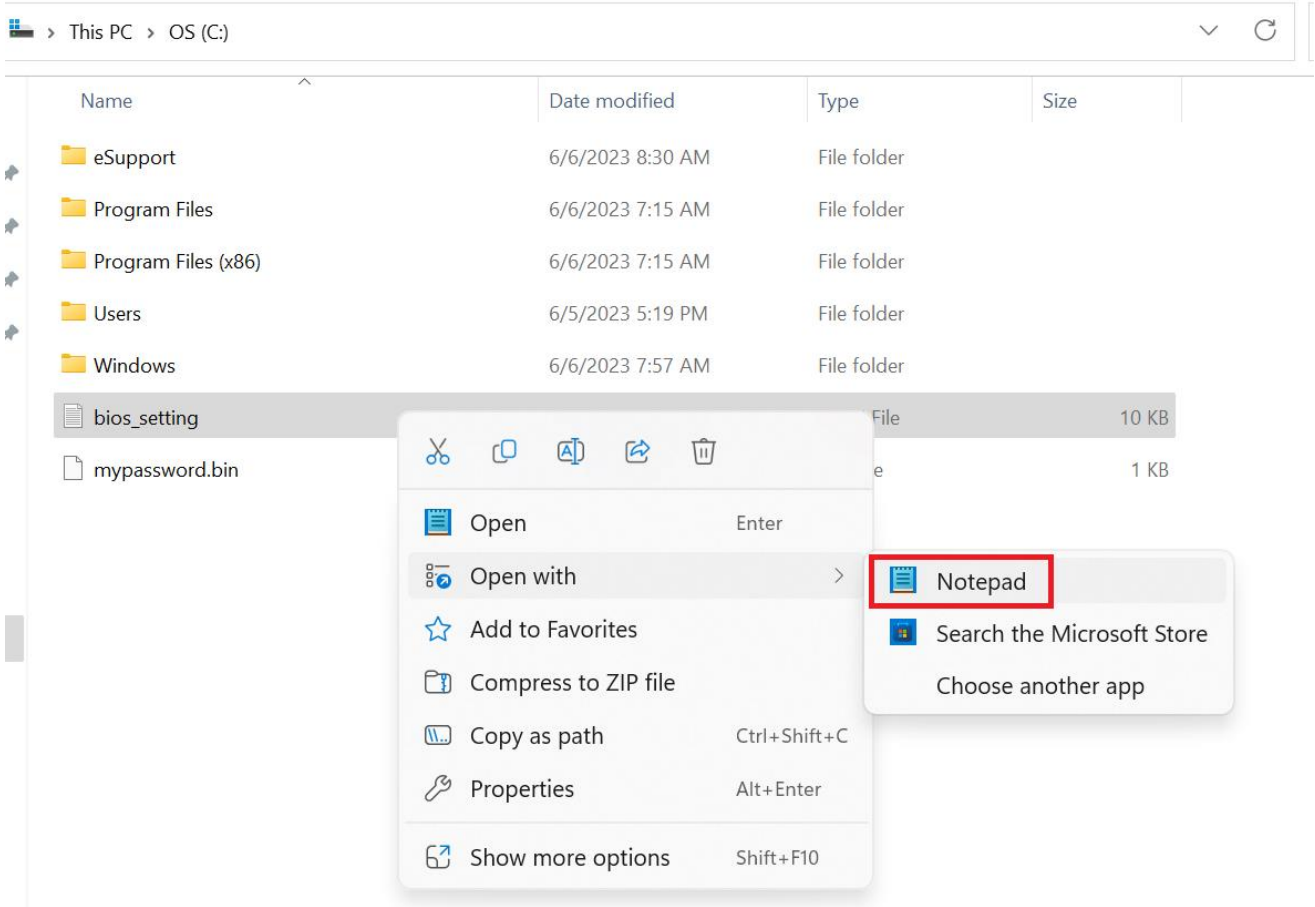


3.1.4 Edit JSON configuration file

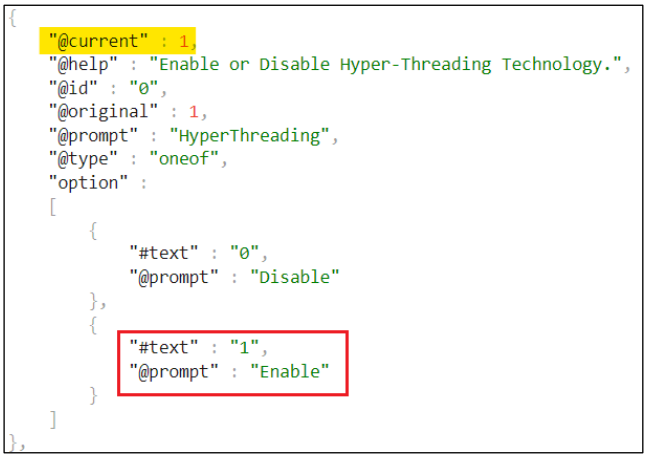
To edit the JSON file, open the JSON file with “NotePad” or JSON editor, find “@current” to set the variable to the desired setting. For the definition of the variable, see “option” for reference.

Example:

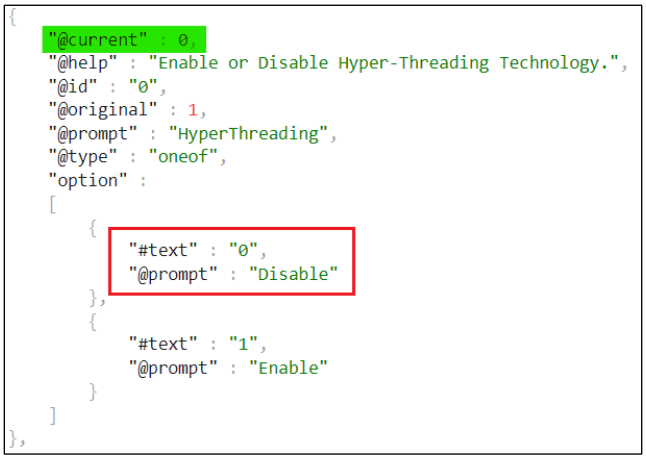
Open JSON file with “NotePad”.



Change “Hyper Threading” from enable to disable by editing “@current” from 1 to 0.



```
{
    "@current" : 1,
    "@help" : "Enable or Disable Hyper-Threading Technology.",
    "@id" : "0",
    "@original" : 1,
    "@prompt" : "HyperThreading",
    "@type" : "oneof",
    "option" :
    [
        {
            "#text" : "0",
            "@prompt" : "Disable"
        },
        {
            "#text" : "1",
            "@prompt" : "Enable"
        }
    ]
},
```



```
{
    "@current" : 0,
    "@help" : "Enable or Disable Hyper-Threading Technology.",
    "@id" : "0",
    "@original" : 1,
    "@prompt" : "HyperThreading",
    "@type" : "oneof",
    "option" :
    [
        {
            "#text" : "0",
            "@prompt" : "Disable"
        },
        {
            "#text" : "1",
            "@prompt" : "Enable"
        }
    ]
},
```

For BIOS Boot Order (Boot Option Priorities), edit the sequence in “@current”.

Example:

Change “Boot Option Priorities” from “HDD,LAN” to “LAN,HDD” by editing the sequence of the strings.

```
{
    "@id" : "0",
    "@pageModifyCount" : "0",
    "@prompt" : "Boot",
    "question" :
    [
        {
            "@current" : "HDD,LAN",
            "@modify" : "false",
            "@original" : "HDD,LAN",
            "@prompt" : "Boot Option Priorities",
            "@type" : "string_vector"
        }
    ]
},
```

```
{
    "@id" : "0",
    "@pageModifyCount" : "0",
    "@prompt" : "Boot",
    "question" :
    [
        {
            "@current" : "LAN,HDD",
            "@modify" : "false",
            "@original" : "HDD,LAN",
            "@prompt" : "Boot Option Priorities",
            "@type" : "string_vector"
        }
    ]
},
```

After editing the JSON file, use the command in Chapter 3.2.1 to write the configuration into the devices’ BIOS settings. The settings will apply after the device is rebooted.

3.1.5 Sign JSON configuration file

To sign a configuration (JSON) file.

This signed file can be used to apply settings to a device that is enrolled with the paired public key.

Arguments:

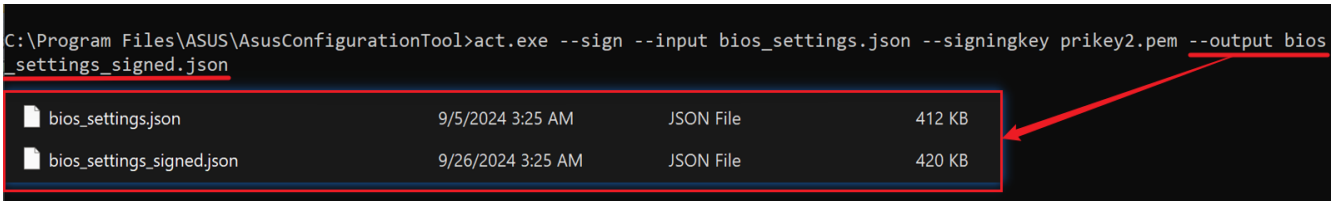
```
--sign

--input, -i <path to BIOS configuration file>

--signingkey <path to signing key file>

--output,-o <path to signed configuration file.
          If none, the input file will be edited in place.>
```

```
act.exe --sign --input <$PATH_TO_BIOS_SETTING_FILE> --signingkey
 <$PATH_TO_SIGNING_KEY_FILE> --output <$PATH_TO_SIGNED_FILE>
```

Example:

Sign bios_setting.json with private.2048.pem. The signed file is bios_setting_signed.json.

```
act.exe --sign --input bios_setting.json --signingkey  private2048.pem --output
bios_setting_signed.json
```



2.1 Boot Logo

This function allows the user to customize the boot logo. The logo requires:

- 24 bit BMP file
- File size cannot exceed 640 x 480
- Logo resolution suggestion versus monitor resolution suggestion

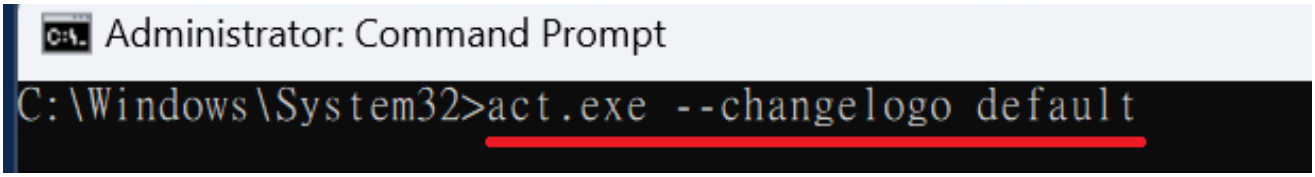
Monitor Resolution	Suggested Logo Image Resolution
1366 x 768	322 x 103
1024 x 768	250 x 104
1280 x 1024	293 x 135
1920 x 1080	448 x 142
1920 x 1200	448 x 142
1960 x 1080	448 x 142
2560 x 1600	580 x 180
2560 x 1440	580 x 180
2880 x 1620	580 x 180
2880 x 1800	654 x 203
3200 x 2000	726 x 226
3840 x 2160	820 x 270
3840 x 2400	820 x 270

- **Set Default Boot Logo**

Command:

```
act.exe --changelogo default
```

Example:



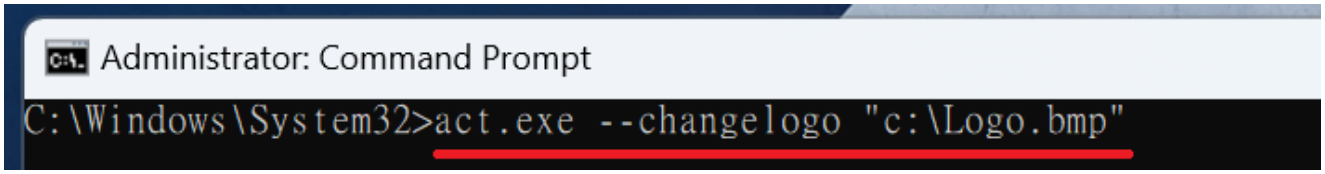
- **Set Custom Boot Logo**

Command:

```
act.exe --changelogo "d:\ASUSTekLogo.bmp"
```

Example:

Upload the logo file to be replaced to (C:) and enter the following command. Boot Logo will be changed after reboot.



- **Set Custom Boot Logo and the device is password protected.**

The password is exported to `mypassword.bin`.

```
act.exe --changelogo "d:\ASUSTekLogo.bmp" --pwd mypassword.bin
```

- **Set Custom Boot Logo and the device is enrolled.**

The Logo file should be signed by the private key first and get the signature encoded in base64, `VjbA…vYiw=`

```
act.exe --changelogo "d:\ASUSTekLogo.bmp" --signature VjbAKR…JDQbvYiw=
```

3.1 USB/DVD Storage Lock

This function requires ASUS Business Utility (ABU) v3.5.19.0 or later installed in the device.
Note: ASUS Business Manager (App) will not be able to control USB/DVD Lock when ACT is installed, the control rights will be given to ACT.
For ACT 1.4.0.0 or later
This function requires ASUS Business System Control Interface (BSCI) v0.4.3.0 or later installed in the device.
Under Enrolled Mode, USB Lock and DVD Lock functions are following the authority of JSON file settings.

3.1.1 USB Lock

Command:

- **Set USB Enable Storage**

```
act.exe --usblock 0 --pwd mypassword.bin
```

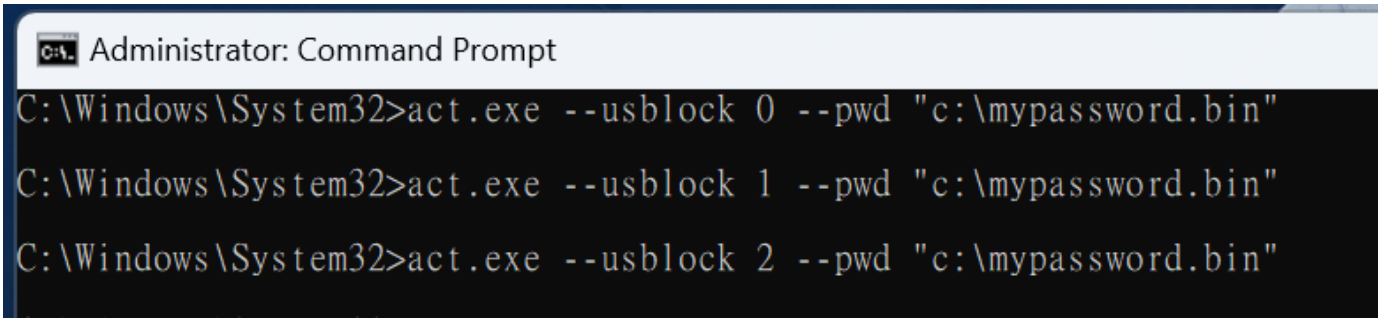
- **Set USB Read-Only**

```
act.exe --usblock 1 --pwd mypassword.bin
```

- **Set USB Peripherals Only**

```
act.exe --usblock 2 --pwd mypassword.bin
```

Example:



*USB Lock has a higher privilege than USB Mass Storage. Setting “USB Peripherals Only” with ACT will change the USB Mass Storage from default enable to disable; setting back to “USB Enable Storage” or “USB Read-Only” will change the USB Mass Storage back to enable.

3.1.2 DVD Lock

Command:

- **Set DVD Enable Storage**

```
act.exe --dvdlock 0 --pwd mypassword.bin
```

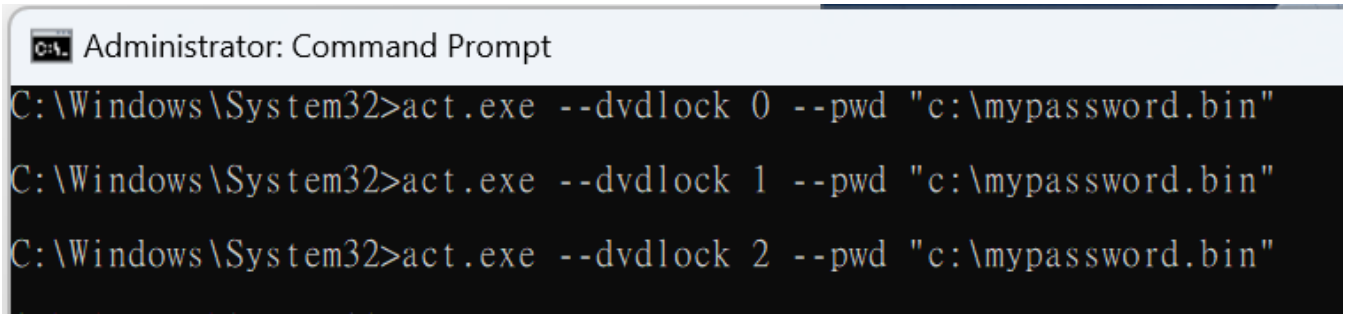
- **Set DVD Read-Only**

```
act.exe --dvdlock 1 --pwd mypassword.bin
```

- **Set DVD Disable**

```
act.exe --dvdlock 2 --pwd mypassword.bin
```

Example:



4.1 BIOS Update

This function is used to update the BIOS firmware. It requires the target device model, firmware version, BIOS firmware file, and the corresponding hash value as input parameters.

Arguments:

`--update_bios`

Example:

This example shows a configuration for updating BIOS firmware for model B9400CBA to version 312 if and only if device's current BIOS is older than 310.

The BIOS firmware file is ASUS_B9400CEA_312_BIOS_Update and the **SHA256 hash value** is B86C79EAF097BA6115CFEB27418A517EB5511218B7C0BF1E3BDC6476C6A81B6A

```
{
  "prerequisite": {
    "model": "B9400CBA",
    "version": 310
  },
  "target": {
    "version": 312,
    "file": "ASUS_B9400CEA_312_BIOS_Update.exe",
    "hash": "B86C79EAF097BA6115CFEB27418A517EB5511218B7C0BF1E3BDC6476C6A81B6A"
  }
}
```

Put all settings in `bios.json` and update BIOS firmware.

- **Device is not password protected**

```
act.exe --update_bios bios.json
```

- **Device is password protected**

```
act.exe --update_bios bios.json --pwd eg5*7jV3N274
```

5.1 Others

- **Reset BIOS to default settings**

This function will reset all BIOS setups to default settings (including items not configured through ACT), and change boot logo back to default, but **will not** clear the BIOS administrator password. If the password is set (see Chapter 2.2), then the password must be provided.

Arguments:

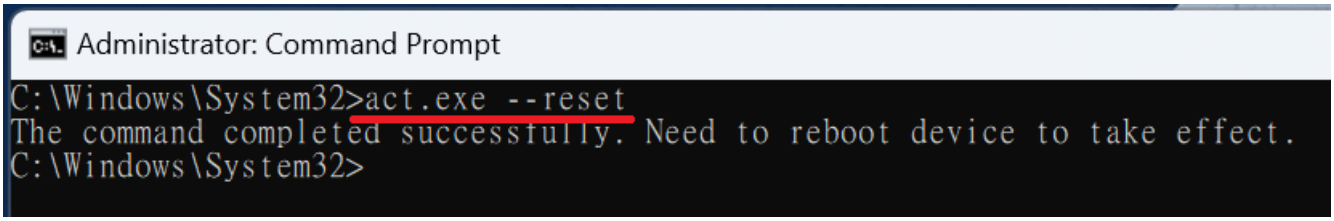
```
--reset
[--pwd, -p <password in plaintext, or a file path to an existing password file>]
```

Command:

```
act.exe --reset
```

Example:

Reset BIOS to default settings where the BIOS administrator password is not set.

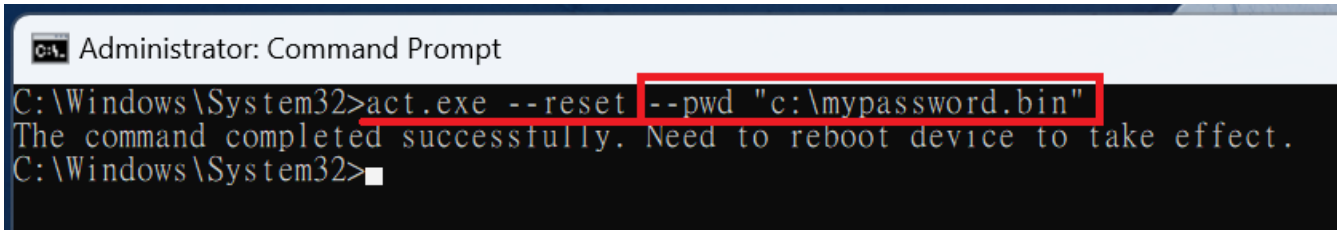


Command:

```
act.exe --reset --pwd mypassword.bin
```

Example:

Reset the BIOS to default settings with BIOS password.



- **Load BIOS to factory default or custom default**

This function will restore all BIOS setups to factory or customer default (including items not configured through ACT) if there is customized default, but **will not** change boot logo back to default and clear the BIOS administrator password.

```
act.exe --factory_default_load --pwd mypassword.bin
```

```
act.exe --customer_default_load --pwd mypassword.bin
```

- **Disable error messages**

This function will not show any error messages on the console.

Arguments:

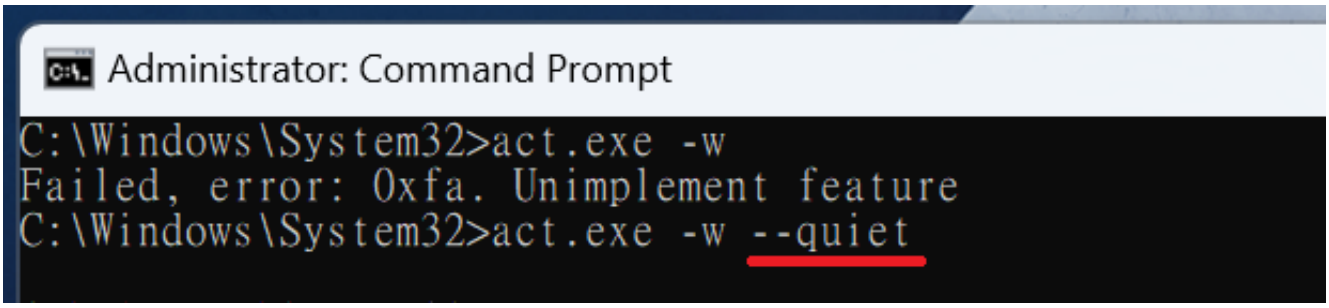
```
--quiet
```

Command:

```
act.exe --quiet
```

Example:

As the figure below, the command with "`--quiet`" will hide error messages.



- **Write Asset Tag**

This function can check or write asset tag for the target device.

Arguments:

```
--assettag <write asset tag for this device>
--signature <signature encoded in base64 for enrolled device>
[--assettag --get] <get the asset tag of this device>
```

```
act.exe --assettag --get
```

Example#1:

Set asset tag `A12345678` with password (under protected mode).

```
act.exe --assettag "A12345678" --pwd mypassword.bin
```

Example#2:

If the target device is enrolled. The asset tag `A12345678` should be signed by the private key first and get the signature encoded in base64, `VjbA…vYiw=`

```
act.exe --assetag "A12345678" --signature VjbA…vYiw=
```

- **Read version information**

This function will read ACT and BIOS versions:

- act.exe revision: ACT application version
- Backend revision: abs.dll library version
- Interface revision: BIOS interface version
- BIOS admin password: BIOS Administration Password is set or not
- BIOS enrollment: BIOS enrollment of public key is set or not

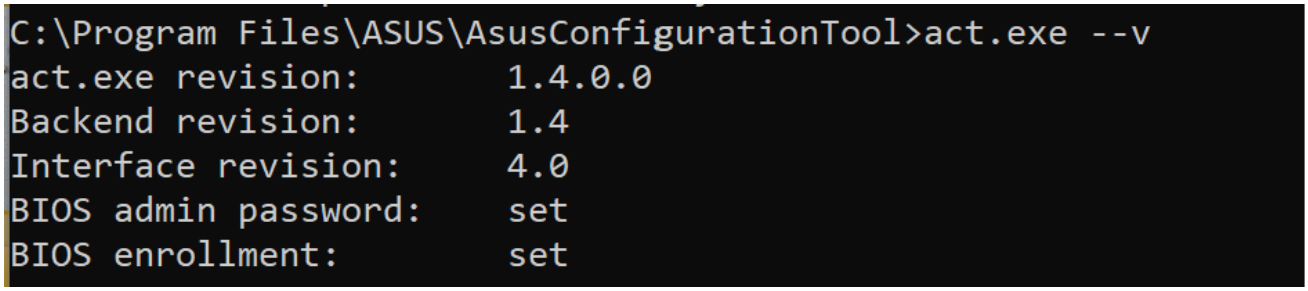
Arguments:

`--version, -v <output version information>`

Command:

```
act.exe --version
```

Example:



4 Trusted Apps

Trusted Apps are required to be signed and certified in order to become trusted, it will be authorized to set administrator password via ACT even when the password does not already exist. After setting a password through the trusted apps, the BIOS configuration and administrator password can be adjusted remotely. The whitelist of these applications are listed below:

- ASUS Control Center

  (Refer to "ASUS Control Center English User Manual" Ch2.2.7 for more information)

- Ciro

5 Error code

The error code and messages are listed below:

#	Error Message
0x1	"Operation fail"
0x2	"Invalid arguments"
0x3	"Invalid platform(BIOS) implementation"
0x4	"File not found"
0x5	"File exists"
0x6	"Invalid file content"
0x7	"Resource busy"
0x8	"Permission denied"
0x9	"Fault error"
0x10	"Untrust application"
0x11	"Incompatible between BIOS and configuration file"
0x12	"Unimplement feature"
0x13	"Logic violation"
0x14	"Error Max"

6 Appendix A – Scope of Settings

6.1 Intel Platform

6.1.1 Notebook

	Intel	Y2023 Platform		Remark
		AlderLake	RaptorLake	
Advanced	Internal Pointing Device (NX only)	X	X	
	Fn Lock Option (NX Only)	X	X	
	Lid Switch (NX only)	X	X	
	Wake On Lid Open (NX only)	X	X	
	Wake On LAN (NX only)	V	V	
	Wake On WLAN	X	X	
	Sign of Life	X	X	
	TPM Device Selection	X	X	
	USB Provisioning of AMT	X	X	vPro support
	Intel Virtualization Technology	V	V	
	Intel (VMX) Virtualization Technology	X	X	
	Hyper-Threading	V	V	
	Intel Total Memory Encryption	X	X	
	VT-d	V	V	
	DVMT Pre-Allocated	X	X	
	SATA Operation	V	V	
	Control Iommu Pre-boot Behavior	X	X	
	DMA Control Guarantee	X	X	
	Security Device Support	X	X	
	Network Stack	V	V	
	IPv4 PXE Support	V	V	
	IPv6 PXE Support	V	V	
	Next Boot with PXE	X	X	
	Restore AC Power Loss	X	X	
	SMART Self Test	V	V	
Boot	Fast Boot	V	V	

	POST Delay Time	X	X	
	Boot Option Priorities	V	V	
Security	Wireless Network Interface	V	V	
	Bluetooth Interface	V	V	
	LAN Network Interface	V	V	
	HD Audio Interface	V	V	
	Internal Speaker	X	X	
	Microphone	X	X	
	USB Interface (NX only)	V	V	
	External Ports (NX only)	V	V	
	CMOS Camera (NX/AIO only)	V	V	
	WWAN	X	X	
	Card Reader	V	V	
	Card Reader Interface (NX/AIO PCIE_only)	X	X	
	Finger Print (NX only)	X	X	
	WWAN USB Interface (NX/AIO only)	X	X	
	M.2 SSD_N	X	X	
	Secure Boot Control	V	V	
	MIPI Camera (NX/AIO only)	X	X	
	GPS	X	X	
	Bluetooth	X	X	
	NFC	X	X	
	SATA ODD Interface (NX/AIO only)	X	X	
Tool	UEFI Capsule Firmware Updates	X	X	
	MAC Address Override (NX/AIO only)	X	X	
	OS Agent Request	X	X	
	Thermal Management	X	X	
	Type-C Output Setting	X	X	
ASUS_Business_Manager	USB Lock	V	V	
	DVD Lock	V	V	
	Change Boot Logo	V	V	

	Intel	Y2024 Platform			Remark
		Raptor Lake	Alder Lake-N	Meteor Lake	
Advanced	Internal Pointing Device (NX only)	V	V	V	
	Fn Lock Option (NX Only)	V	V	V	
	Lid Switch (NX only)	V	V	V	
	Wake On Lid Open (NX only)	V	V	V	
	Wake On LAN (NX only)	V	V	V	
	Wake On WLAN	V	V	V	
	Sign of Life	V	V	V	
	TPM Device Selection	X	X	X	
	USB Provisioning of AMT		X		vPro support
	Intel Virtualization Technology	X	X	X	
	Intel (VMX) Virtualization Technology	V	V	V	
	Hyper-Threading		X		
	Intel Total Memory Encryption	V	V	V	
	VT-d	V	V	V	
	DVMT Pre-Allocated	V	V	V	
	SATA Operation	V	V	V	
	Control Iommu Pre-boot Behavior	V	V	V	
	DMA Control Guarantee	V	V	V	
	Security Device Support	X	X	X	
	Network Stack	V	V	V	
	IPv4 PXE Support	V	V	V	
	IPv6 PXE Support	V	V	V	
	Next Boot with PXE	V	V	V	
	Restore AC Power Loss	V	V	V	
	SMART Self Test	V	V	V	
Boot	Fast Boot	V	V	V	
	POST Delay Time	V	V	V	
	Boot Option Priorities	V	V	V	
Security	Wireless Network Interface	V	V	V	

	Bluetooth Interface	V	V	V	
	LAN Network Interface	V	V	V	
	HD Audio Interface	V	V	V	
	Internal Speaker	V	V	V	
	Microphone	V	V	V	
	USB Interface (NX only)	V	V	V	
	External Ports (NX only)	V	V	V	
	CMOS Camera (NX/AIO only)	V	V	V	
	WWAN	V	V	V	
	Card Reader	V	V	V	
	Card Reader Interface (NX/AIO PCIE_only)	V	V	V	
	Finger Print (NX only)	V	V	V	
	WWAN USB Interface (NX/AIO only)	V	V	V	
	M.2 SSD_N	V	V	V	
	Secure Boot Control	V	V	V	
	MIPI Camera (NX/AIO only)	V	V	V	
	GPS	V	V	V	
	Bluetooth	V	V	V	
	NFC	V	V	V	
	SATA ODD Interface (NX/AIO only)	V	V	V	
Tool	UEFI Capsule Firmware Updates	V	V	V	
	MAC Address Override (NX/AIO only)	V	V	V	
	OS Agent Request	V	V	V	
	Thermal Management	V	V	V	
	Type-C Output Setting	V	V	V	
ASUS_Business_Manager	USB Lock	V	V	V	
	DVD Lock	V	V	V	
	Change Boot Logo	V	V	V	

6.1.2 All in One

	Intel	Y2023 Intel Platform		
		AlderLake	RaptorLake	Remark
Advanced	Wake On WLAN	X	X	
	Sign of Life	X	X	
	TPM Device Selection	X	X	
	Intel Virtualization Technology	V	V	
	Intel (VMX) Virtualization Technology	X	X	
	Hyper-Threading	V	V	
	VT-d	V	V	
	DVMT Pre-Allocated	X	X	
	SATA Operation	V	V	
	Control Iommu Pre-boot Behavior	X	X	
	DMA Control Guarantee	X	X	
	Network Stack	V	V	
	IPv4 PXE Support	V	V	
	IPv6 PXE Support	V	V	
	Next Boot with PXE	X	X	
	Restore AC Power Loss	X	X	
	ErP Support (DT/AIO only)	X	X	
	Power On By PCI-E / Wake on LAN (WOL) (DT/AIO Only)	V	V	
	SMART Self Test	V	V	
	USB Provisioning of AMT	X	X	vPro support
	Intel Total Memory Encryption	X	X	
	Security Device Support	X	X	
Boot	Fast Boot	V	V	
	POST Delay Time	X	X	
	Boot Option Priorities	V	V	
Security	Wireless Network Interface	V	V	
	Bluetooth Interface	V	V	
	LAN Network Interface	V	V	

	HD Audio Interface	V	V	
	Microphone	X	X	
	Internal Speaker	X	X	
	CMOS Camera (NX/AIO only)	V	V	
	Card Reader	V	V	
	Card Reader Interface (NX/AIO PCIE_only)	X	X	
	M.2 SSD_N	X	X	
	Secure Boot Control	V	V	
	SATA ODD Interface (NX/AIO only)	X	X	
	MIPI Camera (NX/AIO only)	X	X	
	WWAN	X	X	
	WWAN USB Interface (NX/AIO only)	X	X	
	GPS	X	X	
	Bluetooth	X	X	
	NFC	X	X	
Tool	UEFI Capsule Firmware Updates	X	X	
	Thermal Management	X	X	
	OS Agent Requests	X	X	
	MAC Address Override (NX/AIO only)	X	X	
	Type-C Output Setting	X	X	
ASUS_Business_ Manager	USB Lock	V		
	DVD Lock	V		
	Change Boot Logo	V		

	Intel	**Y2024 Intel Platform**		
		RaptorLake	**MeteorLake**	**Remark**
Advanced	Wake On WLAN	V	V	
	Sign of Life	V	V	
	TPM Device Selection	X	X	
	Intel Virtualization Technology	X	X	
	Intel (VMX) Virtualization Technology	V	V	
	Hyper-Threading	V	V	
	VT-d	V	V	
	DVMT Pre-Allocated	V	V	Panel≦4k

	SATA Operation	V	V	
	Control Iommu Pre-boot Behavior	X	X	Intel 12th and above
	DMA Control Guarantee	V	V	
	USB Mass Storage Driver Support	V	V	
	Network Stack	V	V	
	IPv4 PXE Support	V	V	
	IPv6 PXE Support	V	V	
	Next Boot with PXE	V	V	
	Automatic Connection (NX/AIO only)	V	V	
	EAP Method (NX/AIO only)	V	V	
	Encryption (NX/AIO only)	V	V	
	Boot from Thunderbolt Port (NX/AIO only)	V	V	
	Restore AC Power Loss	V	V	
	ErP Support (DT/AIO only)	V	V	
	Power On By PCI-E / Wake on LAN (WOL) (DT/AIO Only)	V	V	
	Power On By RTC	V	V	
	Activation Interface Status	V	V	
	SMART Self Test	V	V	
	USB Provisioning of AMT	V	V	vPro support
	Intel Total Memory Encryption	V	V	
	Intel SIPP	V	V	
	Enhanced Intel(R) SpeedStep(tm) Technology	V	V	
	Intel(R) Speed Shift Technology	V	V	
	Intel Turbo Boost Max Technology 3.0	V	V	
	CPU C-states	V	V	
	Active Efficient-Cores	V	V	
	Security Device Support	X	X	
Boot	Fast Boot	V	V	
	POST Delay Time	V	V	
	Boot Option Priorities	V	V	

Security	Password Strength Settings	V	V	
	Allow Non-Admin Password Changes	V	V	
	Bypass Password	V	V	
	Wireless Network Interface	V	V	
	Bluetooth Interface	V	V	
	LAN Network Interface	V	V	
	HD Audio Interface	V	V	
	Microphone	V	V	
	Internal Speaker	V	V	
	CMOS Camera (NX/AIO only)	V	V	
	Card Reader	V	V	
	Card Reader Interface (NX/AIO PCIE_only)	V	V	
	M.2 SSD_N	V	V	
	Secure Boot Control	V	V	
	SATA ODD Interface (NX/AIO only)	V	V	
	MIPI Camera (NX/AIO only)	V	V	
	WWAN	V	V	
	WWAN USB Interface (NX/AIO only)	V	V	
	GPS	V	V	
	Bluetooth	V	V	
	NFC	V	V	
	COM Port N Interface	V	V	PCIE interface
	COM Port N Interface (USB)	V	V	PCIE interface
Monitor	Anti-Tamper Firmware Check	V	V	
Tool	Boot Menu Hotkey	V	V	
	Hotkey Access	V	V	
	UEFI Capsule Firmware Updates	X	X	
	Thermal Management	X	X	
	OS Agent Requests	X	X	
	MAC Address Override (NX/AIO only)	X	X	
	Type-C Output Setting	X	X	
	System Log Support	V	V	

System Log Support	Erase System Log	V	V	
	When Log is Full	V	V	
MEBx	Intel(R) AMT or Intel(R) Standard Manageability	V	V	
ASUS_Business_ Manager	USB Lock	V		
	DVD Lock	V		
	Change Boot Logo	V		

6.1.3 Desktop – OEM projects

			Y2024 Intel Platform	
	Intel	AlderLake	RaptorLake	RaptorLake refresh
Advanced	Hyper-Threading	V	V	V
	Intel Virtualization Technology	V	X	X
	Intel (VMX) Virtualization Technology	X	V	V
	VT-d	V	V	V
	Network Stack	V	V	V
	IPv4 PXE Support	V	V	V
	IPv6 PXE Support	V	V	V
	Intel Lan Controller	V	V	V
	HD Audio Interface	V	V	V
	Connectivity mode	V	V	V
Boot	Fast Boot	V	V	V
	Wait For 'F1' If Error (DT only)	V	V	V
	Boot Option Priorities	V	V	V
Security	OS Type	V	V	V
ASUS_Business_Manager	USB Lock	V	V	V
	DVD Lock	V	V	V
	Change Boot Logo	V	V	V

6.1.4 Desktop – ODM project/OEM D901MDR

		Y2023	Y2024 Platform	
	Intel	RaptorLake	RaptorLake	RaptorLake refresh
Advanced	Wake On WLAN (DT only)	X	V	V
	Sign of Life	X	V	V
	TPM Device Selection	X	X	X
	USB Provisioning of AMT	X	V	V
	PCI Express Native Power Management (DT only)	X	V	V
	Native ASPM (DT only)	X	V	V
	DMI Link ASPM Control (DT only)	X	V	V
	ASPM (DT only)	X	V	V
	L1 Substates (DT only)	X	V	V
	DMI ASPM (DT only)	X	V	V
	DMI Gen3 ASPM (DT only)	X	V	V
	PEG - ASPM (DT only)	X	V	V
	PCI Express Clock Gating (DT only)	X	V	V
	Hyper-Threading	V	V	V
	Intel Virtualization Technology	X	X	X
	Intel (VMX) Virtualization Technology	V	V	V
	Intel Total Memory Encryption	X	V	V
	Intel SIPP	X	V	V
	Enhanced Intel(R) SpeedStep(tm) Technology	X	V	V
	Intel(R) Speed Shift Technology	X	V	V
	Intel Turbo Boost Max Technology 3.0	X	V	V
	Turbo Mode (DT only)	X	V	V
	CPU C-states	X	V	V
	Enhanced C-states (DT only)	X	V	V
	Package C State Limit (DT only)	X	V	V
	Thermal Monitor (DT only)	X	V	V
	Active Efficient-Cores	X	V	V
	VT-d	V	V	V

	iGPU Multi-Monitor (DT only)	X	V	V
	DVMT Pre-Allocated	X	V	V
	Re-Size BAR Support (DT only)	X	V	V
	SATA Operation		V	V
	M.2_1 Link Speed (DT only)	X	V	V
	PCIEX16(G4) Link Speed (DT only)	X	V	V
	Control Iommu Pre-boot Behavior	X	V	V
	DMA Control Guarantee	X	V	V
	USB Mass Storage Driver Support	X	V	V
	Security Device Support	X	X	X
	XHCI Hand-off (DT only)	X	V	V
	Power On By PCI-E / Wake on LAN (WOL) (DT/AIO Only)	V	V	V
	Network Stack	V	V	V
	IPv4 PXE Support	V	V	V
	IPv6 PXE Support	V	V	V
	Next Boot with PXE	X	V	V
	SMART Self Test	V	V	V
	Restore AC Power Loss	V	V	V
	Max Power Saving (DT only)	X	V	V
	ErP Support (DT/AIO only)	X	V	V
	Power On By PS/2 Keyboard (DT only)	X	V	V
	Power On By PS/2 Mouse (DT only)	X	V	V
	Power On By USB Keyboard / Mouse (DT only)	X	V	V
	Power On By RTC	X	V	V
	Activation Interface Status	X	V	V
	CSM Support (DT only)	X	V	V
Boot	Fast Boot	V	V	V
	Boot LOGO Display (DT only)	X	V	V
	Wait For 'F1' If Error (DT only)	X	V	V
	POST Delay Time	X	V	V
	Bootup NumLock State (DT only)	X	V	V
	Boot Option Priorities	V	V	V

Security	Password Strength Settings	X	V	V
	Allow Non-Admin Password Changes	X	V	V
	Bypass Password	X	V	V
	Wireless Network Interface	V	V	V
	Bluetooth Interface	V	V	V
	LAN Network Interface	V	V	V
	HD Audio Interface	V	V	V
	WWAN	X	V	V
	Internal Speaker	X	V	V
	Microphone	X	V	V
	Card Reader	V	V	V
	Card Reader Interface	X	X	X
	Front USB Port(s) (DT only)	X	V	V
	Front USB Port N (DT only)	X	V	V
	Rear USB Port(s) (DT only)	X	V	V
	Rear USB Port N (DT only)	X	V	V
	M.2 SSD_N	X	V	V
	SATA Controller(s) (DT only)	X	V	V
	SATA Port N (DT only)	X	V	V
	SATA Port N Hot Plug (DT only)	X	V	V
	Serial Port 1 (DT only)	X	V	V
	Serial Port 2 (DT only)	X	V	V
	Parallel Port (DT only)	X	V	V
	Device Mode	X	V	V
	GPS	X	V	V
	Bluetooth	X	V	V
	NFC	X	V	V
	Secure Boot Control	V	V	V
	Microsoft UEFI CA (DT only)	X	V	V
Monitor	Chassis Intrusion Detection Support	X	V	V
	Anti-Tamper Firmware Check	X	V	V
Tool	UEFI Capsule Firmware Updates	X	V	V
	OS Agent Requests	X	V	V
	Thermal Management	X	V	V

	Type-C Output Setting	X	V	V
	Boot Menu Hotkey	X	V	V
	Hotkey Access	X	V	V
System Log Support	System Log Support	X	V	V
	Erase System Log	X	V	V
	When Log is Full	X	V	V
MEBx	Intel(R) AMT or Intel(R) Standard Manageability	X	V	V
ASUS_Business_Manager	USB Lock	V	V	V
	DVD Lock	V	V	V
	Change Boot Logo	V	V	V

6.2 AMD Platform

6.2.1 Notebook

	AMD	Y2023	Y2024
		Mendocino	HawkPoint
Advanced	SATA Operation	V	X
	Wake On LAN (NX only)	V	V
	Network Stack	V	V
	IPv4 PXE Support	V	V
	IPv6 PXE Support	V	V
	SMART Self Test	V	V
	Internal Pointing Device (NX only)	X	V
	Fn Lock Option	X	V
	Keyboard Light	X	V
	Lid Switch (NX only)	X	V
	Wake On Lid Open (NX only)	X	V
	Boot Indicator	X	V
	AIM-T Support	X	V
	KVM for Wired Manageability	X	V
	Wireless Manageability	X	V
	KVM for Wireless Manageability		
	TCR for Wireless Manageability		
	RealManage Firmware Control		
	Sign of Life	X	V
	Next Booth with PXE	X	V
	Restore AC Power Loss	X	V
	SVM MODE	X	V
	UMA Frame Buffer Size	X	V
	SMT Control	X	V

	IOMMU	X	V
	SATA Mode Selection	X	V
	USB Mass Storage Driver Support	X	V
	Automatic Connection	X	V
	EAP Method	X	V
	Encryption	X	V
	Boot from Thunderbolt Port	X	V
	Power On By RTC	X	V
	Activation Interface Status	X	V
Boot	Fast Boot	V	V
	POST Delay Time	X	V
	Boot Option Priorities	V	V
Security	Password Strength Settings	X	V
	Allow Non-Admin Password Changes	X	V
	Bypass Password	X	V
	Secure Boot Control	V	V
	LAN Network Interface	V	V
	Wireless Network Interface	V	V
	BlueTooth Interface	V	V
	Wireless Network	V	V
	BlueTooth Interface	V	V
	HD Audio Interface	V	V
	Wireless Network Interface	X	V
	Internal Speaker	X	V
	Microphone	X	V
	USB Interface (NX only)	X	V
	External Ports (NX only)	X	V
	CMOS Camera (NX/AIO only)	X	V

	WWAN	X	V
	Card Reader	X	V
	Card Reader Interface (NX/AIO PCIE_only)	X	V
	Finger Print (NX only)	X	V
	WWAN USB Interface (NX/AIO only)	X	V
	M.2 SSD_N	X	V
	MIPI Camera (NX/AIO only)	X	V
	GPS	X	V
	Bluetooth	X	V
	NFC	X	V
	COM Port N Interface	X	V
	COM Port N Interface (USB)	X	V
	SATA ODD Interface (NX/AIO only)	X	V
Monitor	Chassis Intrusion Detection Support	X	V
	Anti-Tamper Firmware Check	X	V
Tool	UEFI Capsule Firmware Updates	X	V
	Battery Care Mode	X	V
	Instant Full-Charge Mode	X	V
	MAC Address Override (NX/AIO only)	X	V
	OS Agent Request	X	V
	Thermal Management	X	V
	Type-C Output Setting	X	V
	Right Control Key Function Selection	X	V
	Boot Menu Hotkey	X	V
	Hotkey Access	X	V
System Log Support	System Log Support	X	V
	Erase System Log	X	V
	When Log is Full	X	V

ASUS_Business_ Manager	USB Lock	V	V
	DVD Lock	V	V
	Change Boot Logo	V	V

6.2.2 All in One

	AMD	Mendocino	Y2024
Advanced	SVM Mode	V	V
	SATA Operation	V	V
	ErP Support	X	V
	Power On By PCI-E / Wake on LAN (WOL) (DT/AIO Only)	V	V
	Power On By RTC	X	V
	Activation Interface Status	X	V
	Wake On LAN	V	V
	Network Stack	V	V
	IPv4 PXE Support	V	V
	IPv6 PXE Support	V	V
	Next Boot with PXE	X	V
	Automatic Connection	X	V
	EAP Method	X	V
	Encryption	X	V
	Boot from Thunderbolt Port	X	V
	SMART Self Test	V	V
	Restore AC Power Loss	X	V
	AIM-T Support	X	V
	KVM for Wired Manageability	X	V
	Wireless Manageability	X	V
	KVM for Wireless Manageability	X	V
	TCR for Wireless Manageability	X	V
	RealManage Firmware Control	X	V
	SVM MODE	X	V
	UMA Frame Buffer Size	X	V

	SMT Control	X	V
	IOMMU	X	V
	SATA Mode Selection	X	V
	USB Mass Storage Driver Support	X	V
Boot	Fast Boot	V	V
	POST Delay Time	V	V
	Boot Option Priorities	V	V
Security	Password Strength Settings	X	V
	Allow Non-Admin Password Changes	X	V
	Bypass Password	X	V
	Secure Boot Control	V	V
	LAN Network Interface	V	V
	Wireless Network Interface	V	V
	BlueTooth Interface	V	V
	SATA ODD Interface	X	V
	HD Audio Interface	V	V
	Card Reader Interface	X	V
	WWAN	X	V
	GPS	X	V
	NFC	X	V
	COM Port N Interface	X	V
	Internal Speaker	X	V
	Microphone	X	V
	MIPI CameraN	X	V
	Bluetooth	X	V
	CMOS Camera	X	V
	Card Reader	X	V
	WWAN	X	V

	COM Port N Interface (USB)	X	V
	M.2 SSD_N	X	V
	Secure Boot Control	X	V
Monitor	Anti-Tamper Firmware Check	X	V
Tool	UEFI Capsule Firmware Updates	X	V
	MAC Address Override	X	V
	Thermal Management	X	V
	Type-C Output Setting	X	V
	OS Agent Request	X	V
	Boot Menu Hotkey	X	V
	Hotkey Access	X	V
System Log Support	System Log Support	X	V
	Erase System Log	X	V
	When Log is Full	X	V
ASUS_Business_Manager	USB Lock	V	V
	DVD Lock	V	V
	Change Boot Logo	V	V

6.2.3 Desktop – OEM project

	AMD	Mendocino
Advanced	SVM Mode	V
	Network Stack	V
	IPv4 PXE Support	V
	IPv6 PXE Support	V
	HD Audio Interface	V
Boot	Fast Boot	V
	Wait For 'F1' If Error (DT only)	V
	Boot Option Priorities	V
Security	OS Type	V
	Connectivity mode	V
ASUS_Business_Manager	USB Lock	V
	Change Boot Logo	V

6.2.4 Desktop – ODM project

	AMD	Mendocino	Y2024
Advanced	SVM Mode	V	V
	UMA Frame Buffer Size	X	V
	PCI Express Native Power Management	X	V
	Native ASPM	X	V
	ASPM	X	V
	L1 Substates	X	V
	PEG ASPM	X	V
	PCI Express Clock Gating	X	V
	SMT Control	X	V
	IOMMU	X	V
	Wake On LAN	V	V
	Wake On WLAN	V	V
	Power On By PS/2 Keyboard	X	V
	Power On By PS/2 Mouse	X	V
	Power On By USB Keyboard / Mouse	X	V
	Power On By PCI-E / Wake on LAN (WOL) (DT/AIO Only)	V	V
	Power On By RTC	X	V
	Activation Interface Status	X	V
	CSM Support	X	V
	AIM-T Support	X	V
	KVM for Wired Manageability	X	V
	Wireless Manageability	X	V
	KVM for Wireless Manageability	X	V
	TCR for Wireless Manageability	X	V
	SATA Mode Selection	X	V

	USB Mass Storage Driver Support	X	V
	XHCI Hand-off	X	V
	Network Stack	V	V
	IPv4 PXE Support	V	V
	IPv6 PXE Support	V	V
	Next Boot with PXE	X	V
	SMART Self Test	V	V
	Restore AC Power Loss	X	V
	Max Power Saving	X	V
	ErP Support	X	V
Boot	Fast Boot	V	V
	Bootup NumLock State	X	V
	Boot Logo Display	X	V
	POST Delay Time	X	V
	Boot Option Priorities	V	V
	Wait For 'F1' If Error	X	V
Security	Password Strength Settings	X	V
	Allow Non-Admin Password Changes	X	V
	Bypass Password	X	V
	Secure Boot Control	V	V
	LAN Network Interface	V	V
	Wireless Network Interface	V	V
	Wireless Network	V	V
	BlueTooth Interface	V	V
	HD Audio Interface	V	V
	WWAN	X	V
	GPS	X	V
	NFC	X	V
	Internal Speaker	X	V

	Microphone	X	V
	Bluetooth	X	V
	Card Reader	X	V
	Front USB Port(s)	X	V
	Front USB Port N	X	V
	Rear USB Port(s)	X	V
	Rear USB Port N	X	V
	M.2 SSD_N	X	V
	SATA Controller(s)	X	V
	SATA Port N	X	V
	SATA Port N Hot Plug	X	V
	Serial Port 1	X	V
	Serial Port 2	X	V
	Parallel Port	X	V
	Device Mode	X	V
	Secure Boot Control	X	V
	Microsoft UEFI CA	X	V
Monitor	Chassis Intrusion Detection Support	X	V
	Anti-Tamper Firmware Check	X	V
Tool	UEFI Capsule Firmware Updates	X	V
	Thermal Management	X	V
	Type-C Output Setting	X	V
	OS Agent Request	X	V
	Boot Menu Hotkey	X	V
	Hotkey Access	X	V
System Log Support	System Log Support	X	V
	Erase System Log	X	V
	When Log is Full	X	V

ASUS_Business_Manager	USB Lock	V	V
	DVD Lock	V	V
	Change Boot Logo	V	V

7 Appendix B – List of Arguments

Arguments	Definition
-h [--help]	Show help
-v [--version]	output version information and exit
--quite	disable error message
--factory_default_load	Load factory default setting
--newpwd arg	create new password file
--renewpwd arg	renew password file
-p [--pwd] arg	plaintext password or path to password file
-o [--output] arg	specify output filename
-i [--input] arg	specify input filename
-r [--get]	read BIOS settings
-w [--set]	set BIOS settings
-f [--force]	force set BIOS settings
-s [--skip_password_complexity_check]	skip password complexity check
--reset	reset BIOS setting to default
--filter arg	filter for set or get operation
--usblock arg	0: USB_ENABLE_STORAGE 1: USB_READ_ONLY 2: USB_PERIPHERAL_ONLY
--dvdlock arg	0: DVD_ENABLE_DVD 1: DVD_READ_ONLY 2: DVD_DISABLE
--update_firmware_bypass_password_flag arg	0: disable update_firmware_bypass_password 1: enable update_firmware_bypass_password
--changelogo arg	change custom logo The logo format is 24-bit uncompressed BMP, and its size should not exceed 1MB.
--assettag arg	set/get asset tag
--update_bios arg	update BIOS
--no_migration	disable migration
--makemigration	check and do migration if needed
--enroll arg	Enroll device, install public key for signing verification
--revoke	revoke device, remove public key for signing ver.
--signingkey arg	secify a RSA private key for signing request
--signature arg	specify a RSA signature for verification
--sign	sign a file

8 Appendix C – Mapping table of ACT and BIOS interface version

Feature	ACT application version	BIOS interface version	
		NX/AIO	DT
Support password length up to 64 characters	v1.0.2.0 or later	v1.2 or later	v1.1 or later
Read DMI settings	v1.0.8.0 or later	v1.2 or later	v1.1 or later

9 Appendix D – Table of Supported Model List

NX							
B5602CVA	B5602CVN	B5402CVA	B5402FVA	B7402FVA	B2402CVA	B2402FVA	B2502CVA
B2502FVA	BR1402CVA	BR1402FVA	B1402CVA	B1502CVA	B9403CVA	BR1402CGA	BR1402FGA
BR1102CGA	BR1102FGA	B1402CGA	B1502CGA	B1502CBA	B1402CBA	B5602FBN	B5602CBN
B5602FBA	B5602CBA	B5402FBA	B5402CBA	B5302FBA	B5302CBA	B3402FBA	B2402CBA
B2402FBA	B2502CBA	B2502FBA	B7402FBA	B9400CBA	B6602FC2		
Y2024							
B9403CVAR	B3402FVA	BR1204FGA	BR1204CGA	BR1104FGA	BR1104CGA	B5604CVA	B5604CVF
B5404CVA	B5404CVF	B5404CMA	B5604CMA	B3404CVA	B3404CVF	B3604CVA	B3604CVF
B3404CMA	B3604CMA	L5404CHA					
B3405CCA	B5405CCA	B3605CCA	B5605CCA	B3405CVA	B3605CVA	B5405CVA	B5605CVA
BR1204FTA	BR1204CTA	BR1104FTA	BR1104CTA	B1403CVA	B1503CVA	P1403CVA	P1503CVA
B1403CTA	B1503CTA	BM1503CDA	BM1403CDA	P5405CSA			
DT							
D800MDR	D800SDR	D900MDR	D900SDR	D700TE	S500TE	D500TE	D700ME
D700SE	D500ME	D500SE	D700TD	D500TD	S501MD	D500MD	S500SD
D500SD	D700MD	D700SD	D900MD	D900SD	S500SE	S500TD	S502MD
Y2024							
D700MER	D500MER	D700SER	D500SER	D700TER	D500TER	~~S501MER~~	~~S502MER~~
~~S701TER~~	D901MDR	D901SDR					
D501SER	D701SER	D501MER	D701MER	D900MF	D900SF	D700MF	D700SF
P500MV	V500MV						
AIO							
A5702WVA	A5402WVA	A3202WBA	A3402WBA	M3402WFA	M3702WFA		
Y2024							
A3202WVA	A3402WVA	A5402WVAR	A5702WVAR				
P440VA	P470VA	B440VA					

10 Appendix E – Overall function

Groups	BIOS Config Settings	Condition	Definition
General_Advanced	Hyper-Threading	Enable/Disable	Enable or Disable Hyper Threading Technology
	Intel Virtualization Technology	Enable/Disable	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
	VT-d: Enabled	Enable/Disable	VT-d capability
	Wake On LAN	Enable/Disable	Enable or disable the wake-on-LAN function of the onboard LAN controller or other installed PCI-E LAN cards.
	Storage Interface-SATA Operation:	AHCI/RAID	Configures operating mode of the integrated SATA hard drive controller.
	Network Stack Enable	Enable/Disable	Enable/Disable UEFI network Stack
	>> Ipv4 PXE (Only selectable if Network Stack is enabled)	Enable/Disable	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
	>> Ipv6 PXE (Only selectable if Network Stack is enabled)	Enable/Disable	Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.
	SMART Self Test	Enable/Disable	Run SMART Self Test on all HDDs during POST.
	C-States Control	Enable/Disable	Enable/Disable CPU Power Management. Allows CPU to go to C-states when it's not 100% utilized.
	Intel® Speed Shift Technology	Enable/Disable	Enable/Disable Intel(R) Speed Shift Technology support. Enabling will expose the CP PC v2 interface to allow for hardware controlled P-states.
	Intel® SpeedStep Technology	Enable/Disable	Allows more than two frequency ranges to be supported.
	Intel® Turbo Boost Max Technology 3.0	Enable/Disable	Enable/Disable Intel (R) Turbo Boost Max Technology 3.0 support. Disabling will report the maximum ratio of the slowest core in _CPC object.

	Intel Trusted Execution Technology (TXT)	Enable/Disable	Enables utilization of additional hardware capabilities provided by Intel (R) Trusted Execution Technology. Changes require a full power cycle to take effect.
	Keyboard Light (NX)	ON/OFF	Turn on/off keyboard light
	Fn Lock Option (NX)	Enable/Disable	If enabled, lets the hot key combination <Fn>+<Esc> toggle the primary behavior of F1-F12, between their standard and secondary functions. If disabled, you cannot dynamically toggle the primary behavior of these keys.
Boot	Fast Boot:	Enable/Disable	Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.
	Boot Option Priorities	1.HDD/2.LAN/3. USB (Can drag to reorder)	Set the system boot order
Security	Secure Boot Control	Enable/Disable	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled and the System is in User mode. The mode change requires platform reset
	LAN Network Interface	Locked/Unlock	Lock/Unlock LAN Network
	Wireless Network and Bluetooth Interface	Locked/Unlock	Lock/Unlock Wireless Network and Bluetooth
	HD Audio Interface	Locked/Unlock	Lock/Unlock HD AUDIO
	USB Interface (NX)	Enable/Disable	Enable/Disable all hardware accessing the USB interface, including USB storage devices, USB ports, camera, and fingerprint scanners, etc.
	External Ports (NX)	Locked/Unlock	Lock/Unlock External Ports
	CMOS Camera	Locked/Unlock	Lock/Unlock USB CMOS Camera

	Pending Operation	None/TPM Clear	"Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device"
	Active Efficient Cores	All Cores /0/1/2/3/4/5/6/7	Set the count of active efficient cores.
	MAC Address Pass Through	Passthrough MAC Address/Integrate NIC 1 MAC Address/Disabled	Change the type of MAC address.
	ASUS Diagnostic Tool	Enable/Disable	Enable Disable ASUS Diagnostic Tool (ADT)
	ASUS Cloud Recovery	Enable/Disable	Enable Disable ASUS Cloud Recovery
	Microphone (NX/AIO)	Lock/Unlock	Lock/Unlock Microphone
	Internal Speaker	Lock/Unlock	Lock/Unlock Internal Speaker
	WWAN	Lock/Unlock	Lock/Unlock WWAN
	GPS	Lock/Unlock	Lock/Unlock GPS
	Wireless Network Interface	Lock/Unlock	Lock/Unlock Wireless Network
	Bluetooth Interface	Lock/Unlock	Lock/Unlock Bluetooth
	NFC	Lock/Unlock	Lock/Unlock NFC
	Restore AC Power Loss	Power On/ Power Off/ Last State	Select AC power state when power is reapplied after a power failure.
	Secure Erase (Media Sanitization)	Start Device Sanitization	All data will be cleared. This action will take a long time. Please do NOT power off or unplug the target device.
	Boot Protection	Disable/ Enable/ Enable for External Storage only	If enabled, Administrator Password would be required during boot process.
	Load factory defaults	Restore	Restore/Load Default values for all the setup options.
ASUS Business Manager	USB Storage Protection	Enable Storage/ Storage Read-Only/ Peripherals Only	Sets access level for USB storage/peripheral devices. This setting is disabled if USB interface is disabled.

	DVD Lock	DVD_Enable /DVD_READ_ONLY/ DVD_DISABLE	Sets access level for USB storage/peripheral devices. This setting is disabled if USB interface is disabled.
	Change Boot Logo	Upload: Pic	BMP base64 text is required to change logo. The image must be 24bit and uncompressed, with a resolution of bigger than 640x480.

11 Appendix F – Table of DMI settings

Items	description
[Model Name]	Display Project Name.
[System Manufacturer]	Display “ASUSTeK COMPUTER INC.”
[System Language]	
Help String	Choose the system default language
Items	“English”: Default
	“Español”
	“Deutsch”
	“Français”
	“简体中文”
	“繁體中文”
	“Русский”
	“한국어”
	“Українська”
	“日本語”
[User Permissions]	View Only
[BIOS Version]	Display BIOS Version
[Build Date]	YYYY/MM/DD
[GOP Version]	Display GOP Version
[EC Version]	Display EC firmware version(This item will be hidden if not support EC.)
[ME FW Version]	Display ME FW Version
[PCH Stepping]	Display PCH Stepping
[System Date]	YYYY/MM/DD
[System Time]	HH:MM:SS
[Access Level]	Display Access Level
[Brand String]	Display the brand string of the processor
[Core Count]	Display the CPU Core Count. (Big Core and Small Core)
[Processor ID]	Display the CPU ID
[Processor Base Frequency]	Display the base frequency of processor
[Minimum Clock Speed]	Display the Minimum CPU speed (MHz)
[Maximum Clock Speed]	Display the Maximum CPU speed (MHz)
[Processor L2 Cache]	Display the CPU L2 Cache size
[Processor L3 Cache]	Display the CPU L3 Cache size
[Microcode Version]	Display Microcode Version
[Intel® Hyper-Threading Capable]	Display “Yes” or “No” for the capability to support Intel® Hyper-Threading Capable

[64-Bit Technology]	Display “Yes” or “No” for the capability to support 64-Bit Technology
[Total Memory]	Display the size of system memory
[Memory Available]	Display the size of available memory
[Memory Frequency]	Display the frequency of system memory
[Memory Technology]	Display “DDR4” or “DDR5”
[Memory Channel Mode]	Display “Single” or “Dual”
[DIMM SLOT_1]	Display the size of the DIMM on slot 1
[DIMM SLOT_2]	Display the size of the DIMM on slot 2(This item will be hidden if not applicable.)
[MC N1 Ch N2 DIMM N3]	Display the status of system memory
[Serial Number]	Display the Serial Number
[MAC address]	Display MAC Adress(This item will be hidden if not support onboard GLAN.)
[Asset Tag]	Set or Display Asset Tag. If Asset Tag is not filled, it will be display as blank
[Service Tag]	Display Service Tag.
[Manufacture Date]	YYYY/MM/DD
[Operating System Version]	Display Operating System Version(This item only displays on OS-preloaded platform.)