Inspiring Innovation • Persistent Perfection

ASUS Config Manager

User Guide v1.2

Table of Contents

Glossary 2

1. Introduction 3

Supported Microsoft System Center Configuration Manager Versions 3

Supported Client Device Operation System 3

Supported Product Line 3

2. Using ASUS Config Manager 4

Installation 4

Uninstallation 6

Run Application 7

Driver Package Creator 7

Driver Updater 10

BIOS Updater 11

BIOS Admin Password and Authentication 14

BIOS Configuration 20

3. Deploy Result and Error Analysis 24

Error Status of Driver Updater 24

Error Status of BIOS Updater 25

Error Status of BIOS Authentication or BIOS Configuration 26

Error Report 27

4. FAQs 27

5. Appendix – ASUS Commercial Products 28

6. Appendix – Certificate Key 29

Revision History

Version #	Date	Contributor	Changes
1.0	Oct. 2024	Ellen Wu/Rad Yah	First Release
1.1	Mar. 2025	Ellen Wu	Add silent update function of BIOS and drivers
1.2	Aug. 2025	Ellen Wu/Rad Yah	Add 2-4 UNC path for remote control

Glossary

Abbreviation	Terms
SCCM	Microsoft System Center Configuration Manager
Task Sequence	A task sequence is a mechanism used in System Center Configuration Manager for performing multiple steps or tasks on a client computer at the command-line level without requiring user intervention.
Baseline	In Configuration Manager, baselines are used to define the configuration of a system that is established at a specific point in time. Configuration baselines can contain one or more defined set of desired configurations, or Configuration Items.
Distribution Point	A SCCM distribution point (DP) is a Configuration Manager server role where packages are stored for later distribution.

1. Introduction

Concept

ASUS Config Manager is integrated directly into the SCCM console, providing a streamline user experience for administrators of ASUS hardware devices. ASUS Config Manager is to simplify and automate various management tasks, including provisioning, deployment, configuration, and maintenance of ASUS commercial systems within enterprise IT environments.

Supported Microsoft System Center Configuration Manager Versions

ASUS Config Manager can be installed on servers running the following versions of Microsoft SCCM. To determine sever operating system requirements, see the Microsoft SCCM documentation.

- Microsoft System Center Configuration Manager 1602 and later

Supported Client Device Operation System

The ASUS Config Manager client components are supported on the following client operating systems:

- Windows 10/11

Supported Product Line

ASUS Commercial Notebooks, Desktops and All-in-Ones are supported.

Nevertheless, the specific models supported may vary depending on the ASUS Config Manager features. Please refer to the list displayed in the ACM Wizard for details.

**For more information on supported products, refer to the 5 Appendix – ASUS Commercial Products.*

2. Using ASUS Config Manager

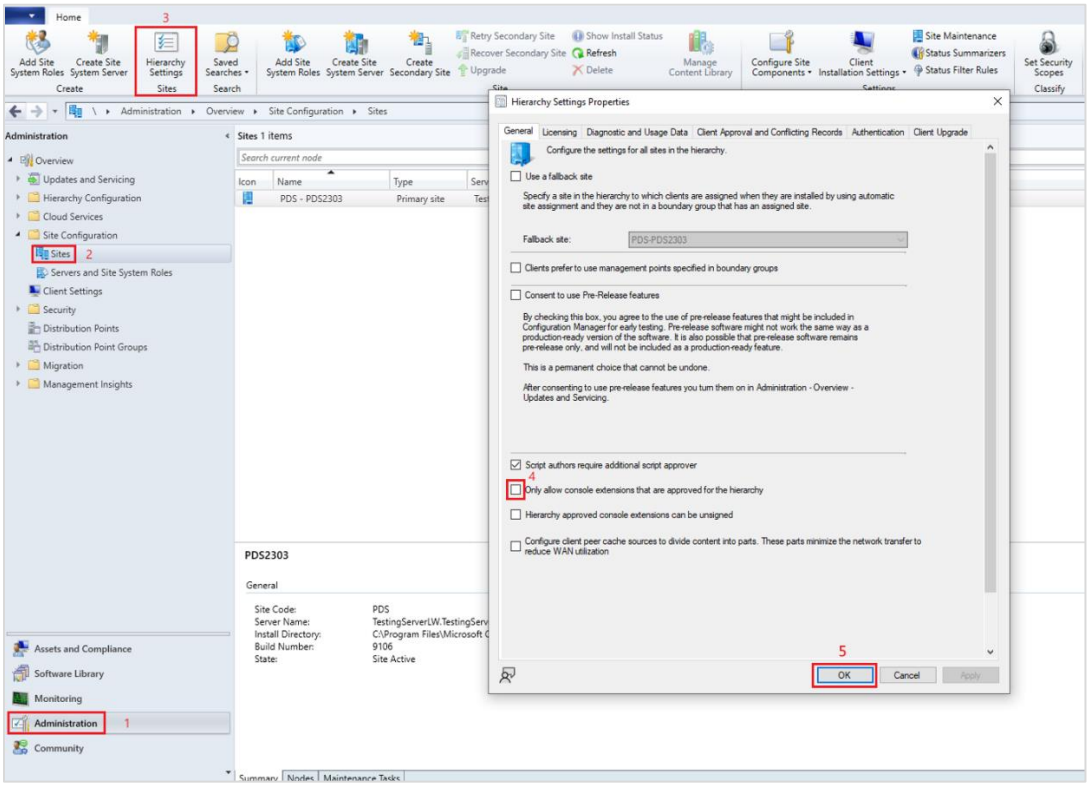
Installation

To download and install the ASUS Config Manger:

1. Go to ASUS support site: [BIOS & Driver Management - Services | Business | ASUS Global]

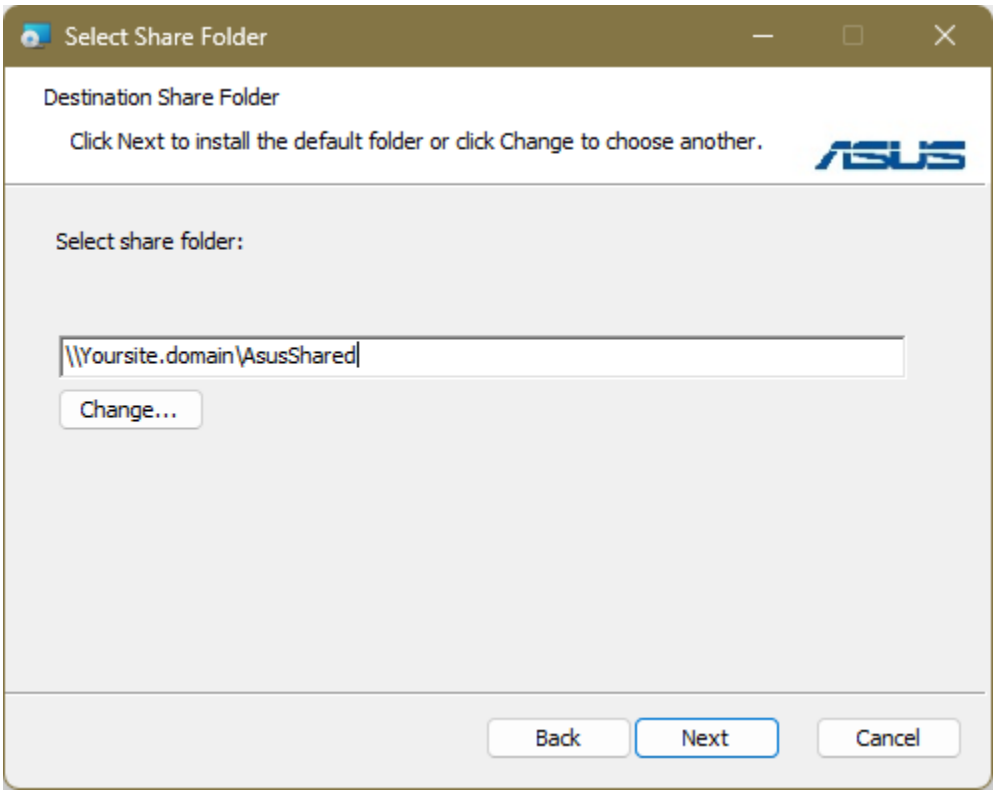
2. Download the latest version of ASUS Config Manger (ACM).

3. **Uncheck the option "Only allow console extensions that are approved for the hierarchy"** in Microsoft SCCM console under Administration > Site Configuration > Sites > Hierarchy Settings.



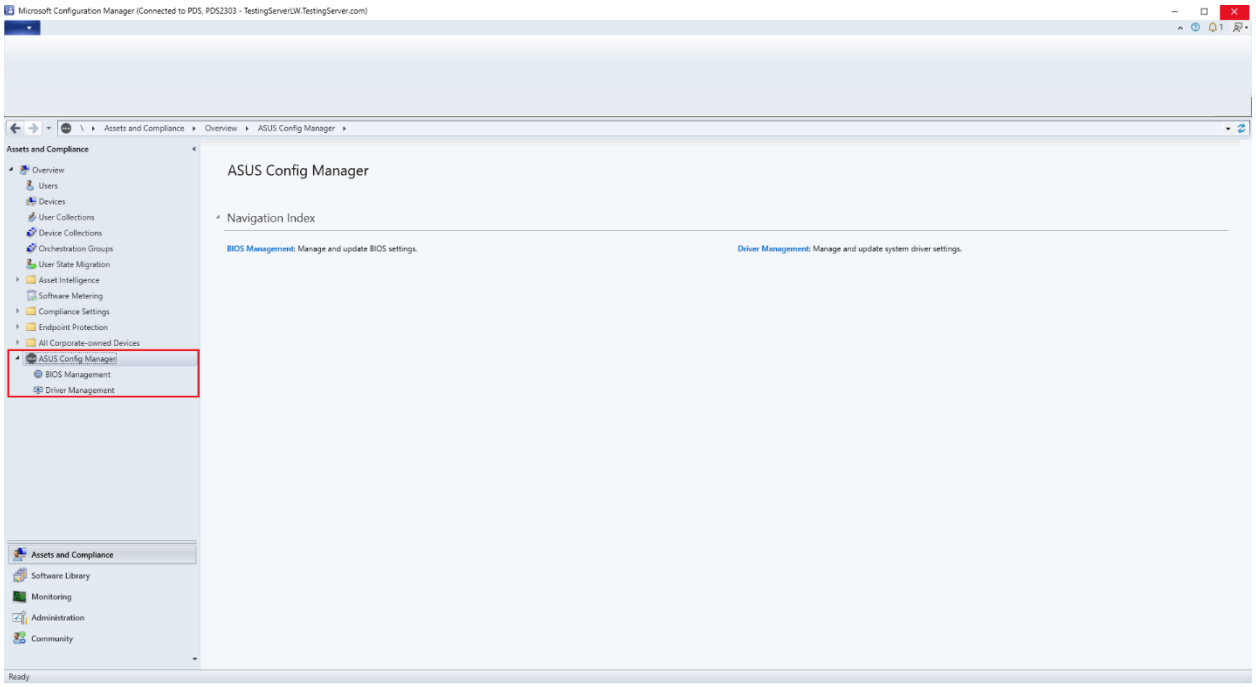
4. Run the downloaded ASUS Config Manger (ACM) for Microsoft System Center Configuration Manager SoftPaq and follow the on-screen instructions to complete the installation.

- We recommend using a UNC path in the *Select Share Folder* step (e.g., \\Yoursite.domain\AsusShared). If the installation is performed on the SCCM server, a local path may be used, and our application will assist in configuring the shared folder.



- To avoid issues related to long file paths, **the total length of the UNC path should be within 45 characters**.

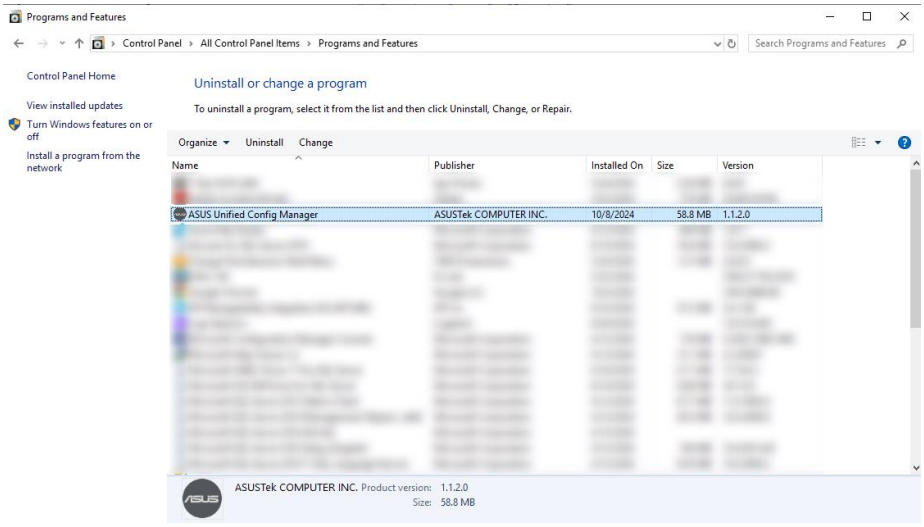
5. Open or **restart** the Microsoft SCCM Console and verify that ASUS Config Manager is displayed under Assets and Compliance.



Uninstallation

To uninstall the ASUS Config Manger:

1. Go to Control Panel > Programs > Uninstallation and choose ASUS Config Manager for uninstallation.



2. Restart the Microsoft SCCM Console to verify that ASUS Config Manager is removed.

Run Application

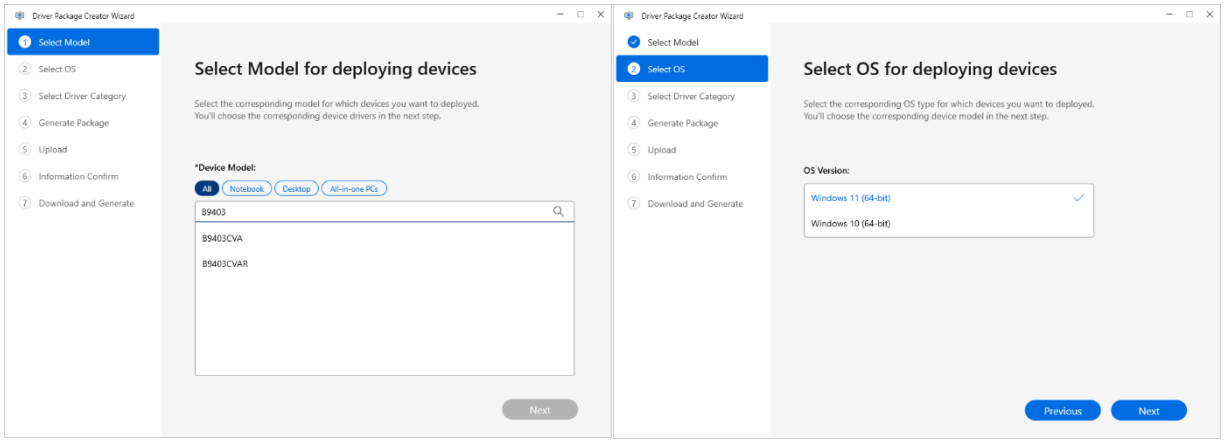
As a standard setting, the installer enhances SCCM functionality by adding various plugins under the ASUS Config Manager node. There is a brief manual for each plugin node in the View section.

Current Plugins: Driver Management, BIOS Management.

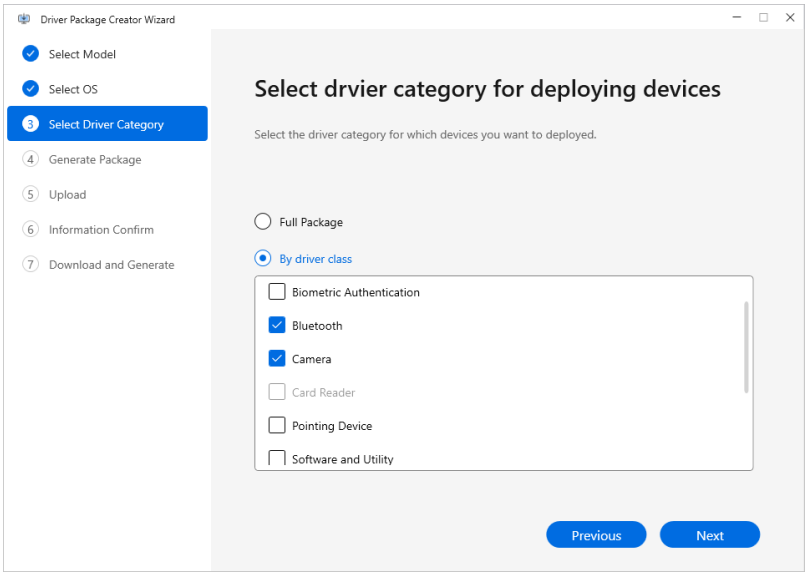
Driver Package Creator

Supports models by syncing the latest drivers from the ASUS Driver Command Website based on the device's operating system. Depending on specific requirements, the downloaded drivers are packaged as a Driver Package **for OS deployment** within a task sequence.

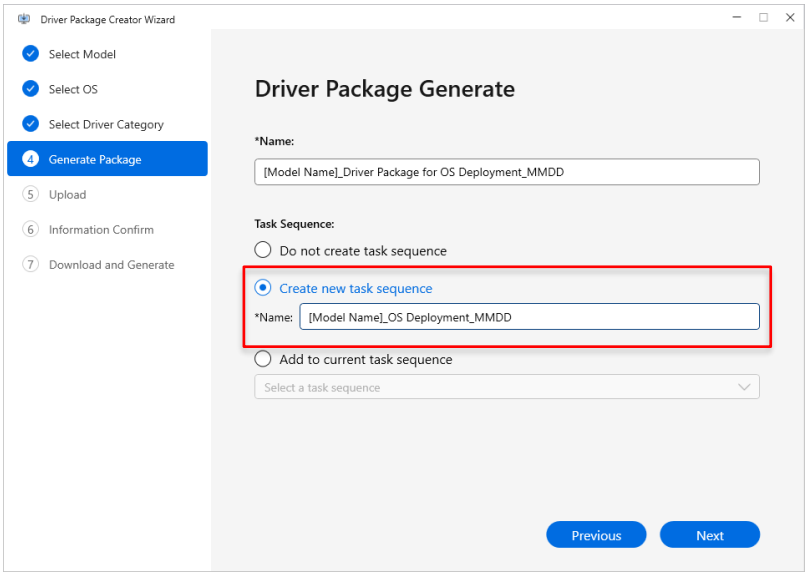
1. Select the particular model and OS version which used for OS deployment.



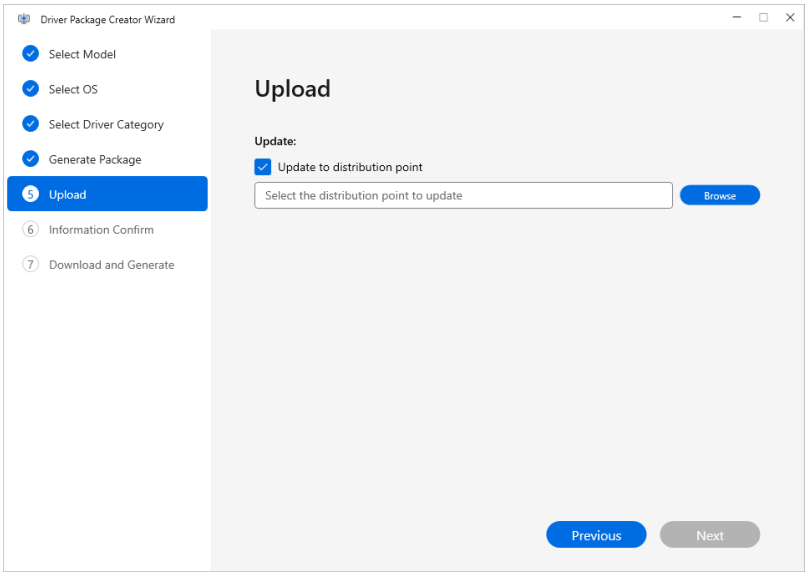
2. Select the drivers: customize the driver package or choose the full package.



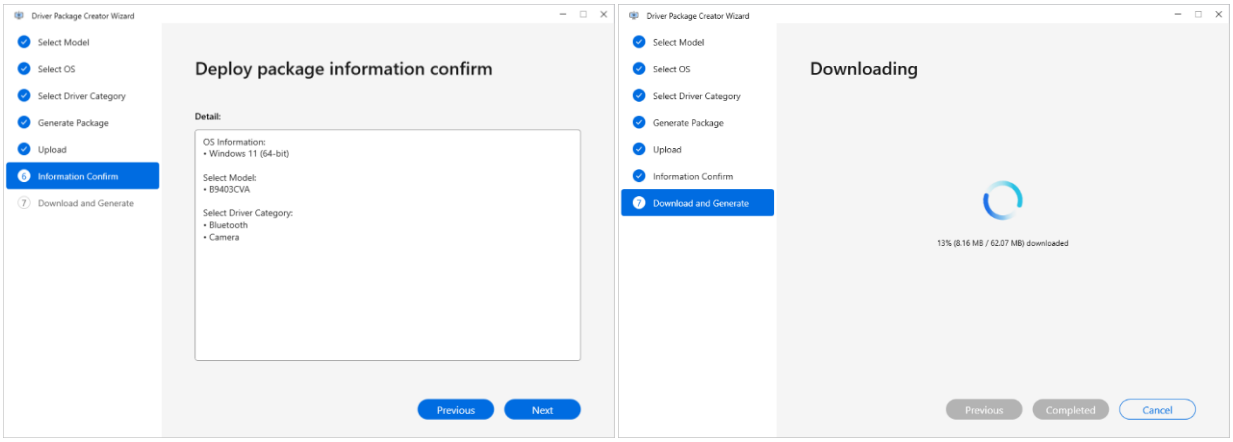
3. Generate a Driver Package: name the package and decide to create a task sequence or not.



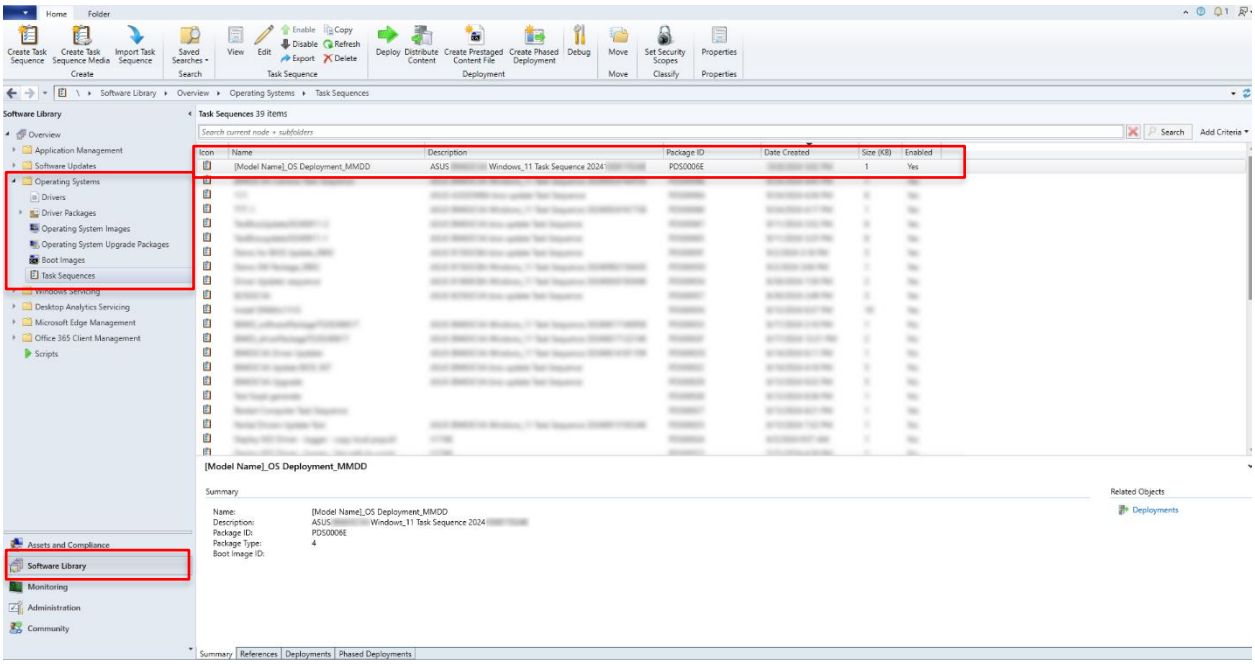
4. Whether to upload to the distribution points.



5. Confirm the driver package information and start downloading and generating.



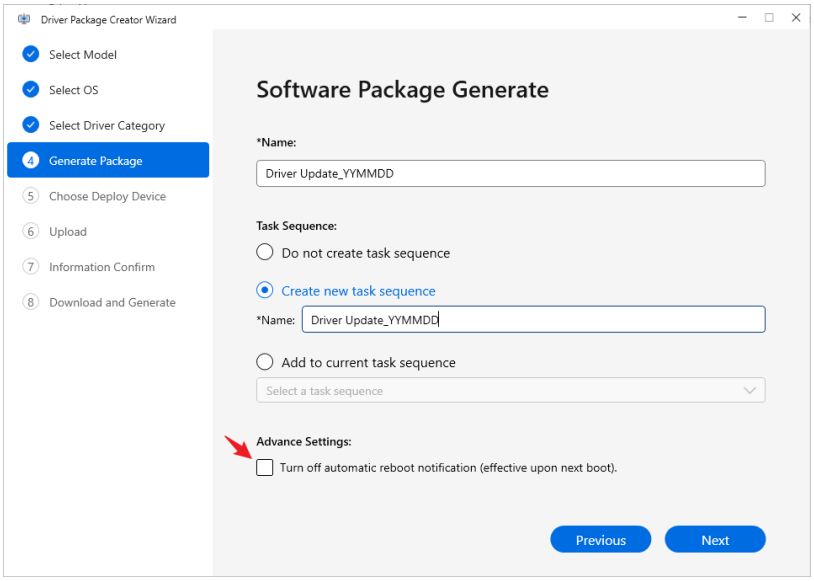
6. After completed, the just generated task sequence can be checked under Task Sequence.
   Software Library > Operating Systems > Task Sequence



Driver Updater

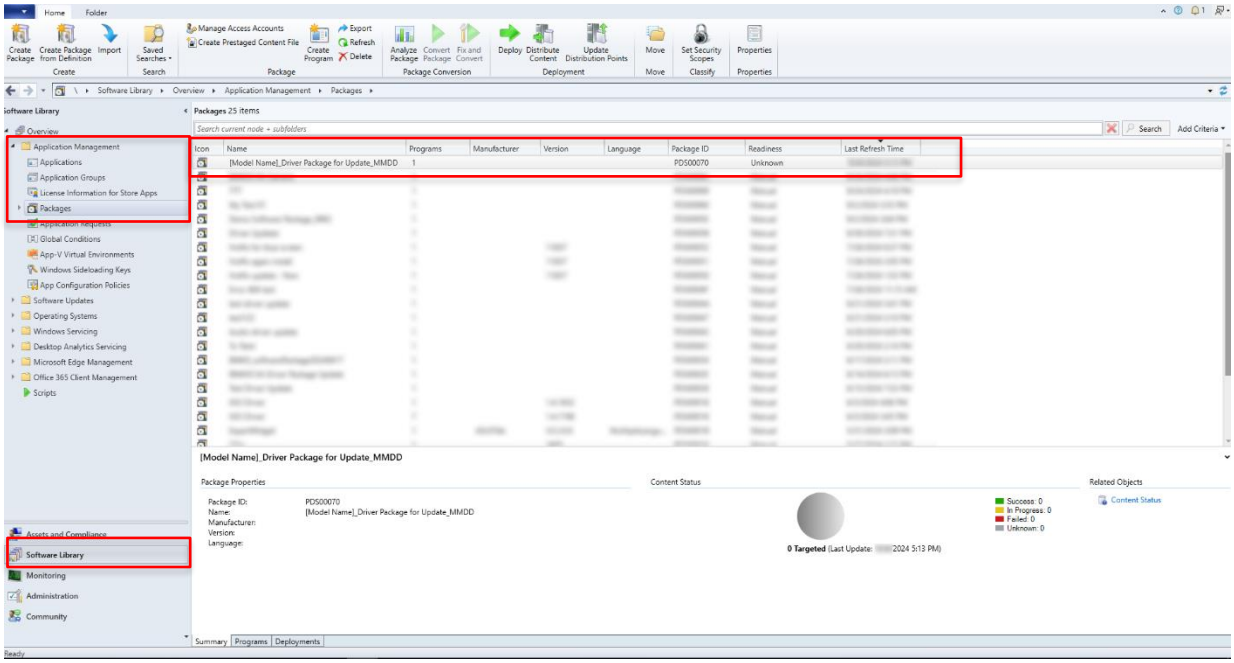
Supports **updating of client device drivers** within OS environment by downloading the latest drivers from the ASUS Driver Command Website based on the device's operating system. The downloaded drivers are packaged as a software package, allowing for easy deployment and updates directly to the client devices as needed.
Updated drivers can be uploaded to the Distribution Points or be deployed directly on clients' devices, catering to urgent fixes or performance optimizations.

1. Select the particular model and its OS version for drivers update.
2. Select the drivers: customize the driver software package or choose the full package.
3. Generate a Driver Software Package: name the package and decide to create a task sequence or not. Choose whether to turn off reboot notification.



4. Whether to upload to the distribution points.
5. Confirm the driver package information and start downloading and generating.
   **If the chosen driver had been downloaded before, ACM wizard will start generating directly.*

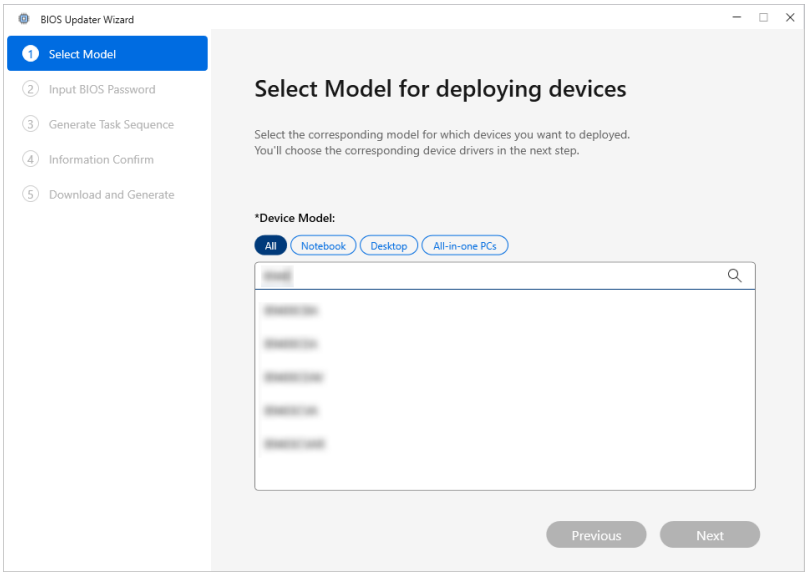
6. After completed, the **software package** can be checked under Application Management. Software Library > Application Management > Packages



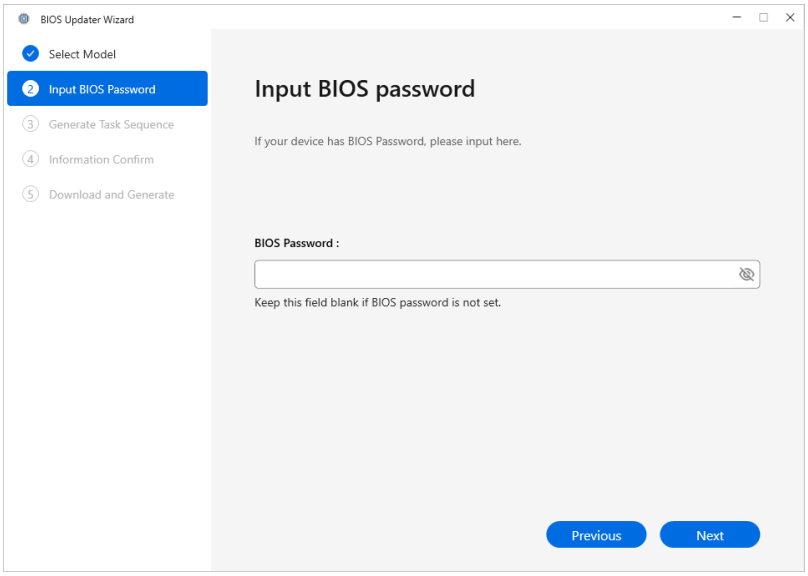
BIOS Updater

Efficiently update and deploy BIOS capsule firmware across multiple devices of **the same model**. Devices sharing the same BIOS admin password can be updated simultaneously, simplifying the process for IT administrators.

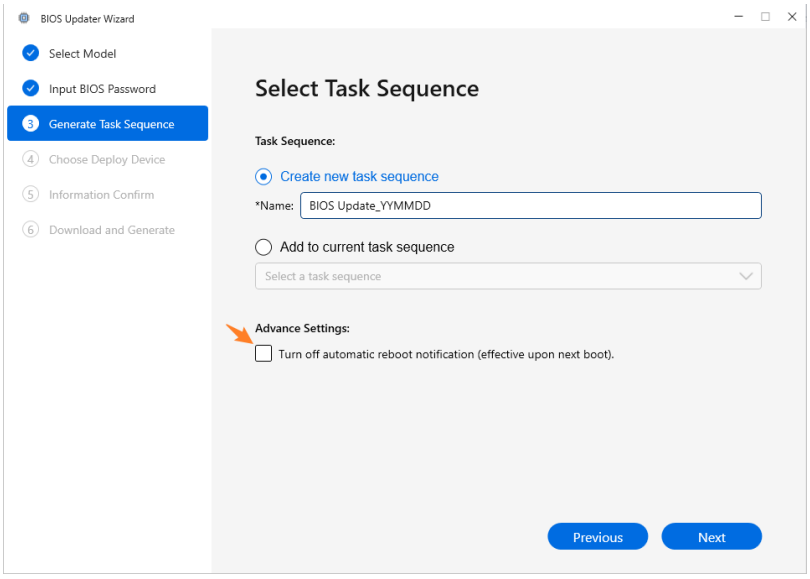
1. Select the particular model for BIOS update deployment.



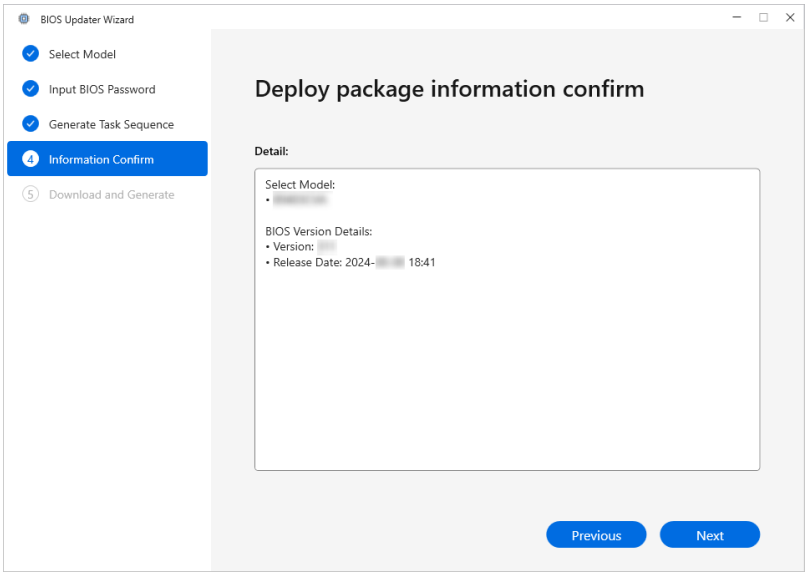
2. Input the BIOS Admin Password if the deployed devices are set.



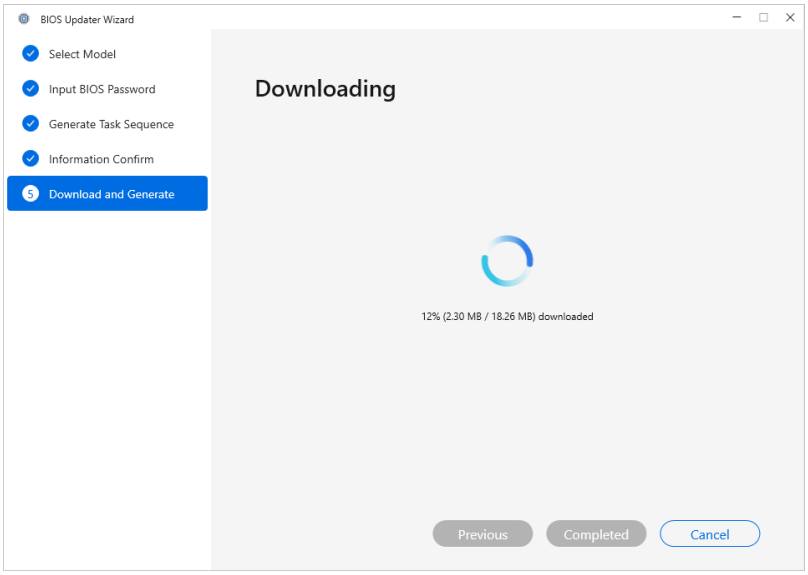
3. Create a task sequence or add to current task sequence for deployment. Remember to select deployed devices collection.



4. BIOS update information confirmation.



5. Start downloading the BIOS and Microsoft SCCM will arrange the deployment accordingly. And this BIOS Update task sequence can also be checked under SCCM Task Sequence. Software Library > Operating Systems > Task Sequence



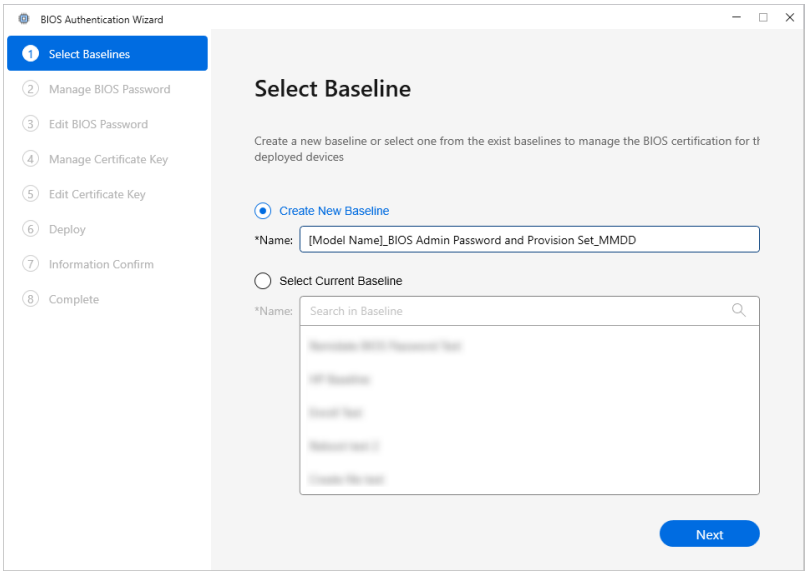
BIOS Admin Password and Authentication

Use BIOS Authentication Wizard to strengthen BIOS security by **enrolling a certificate key** and **setting a BIOS admin password** across multiple devices. The protection ensures only authorized users can modify BIOS settings, enhancing overall security and control.

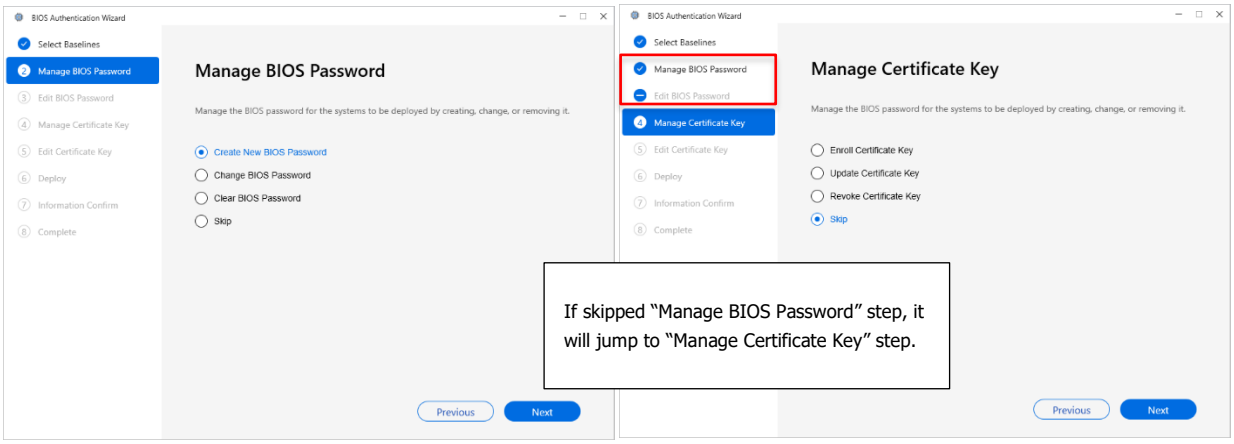
Supported Client Platforms:

- ASUS Commercial Products (2024 or later) for BIOS Provision

1. Create a new baseline or choose a current baseline (for future new devices following).



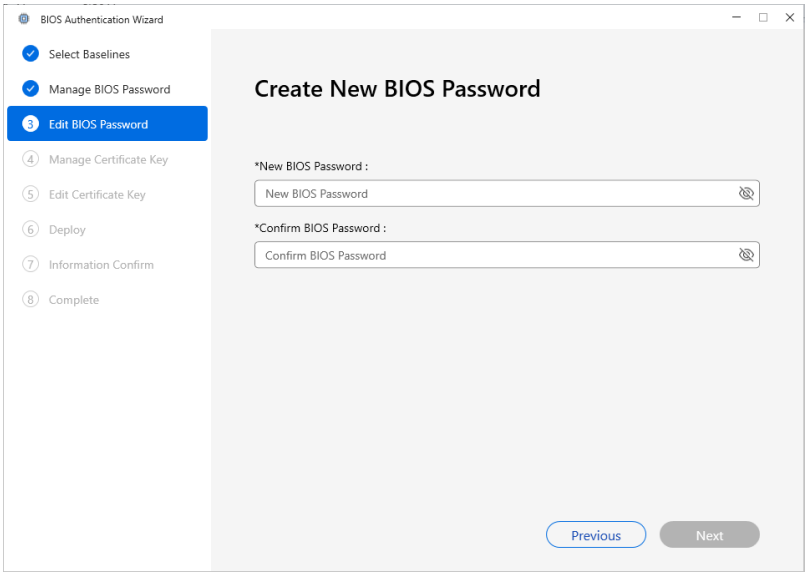
2. Manage BIOS Administrator Password: to create, change, or clear the password. The step can be skipped if the current settings are to be retained.



If skipped "Manage BIOS Password" step, it will jump to "Manage Certificate Key" step.

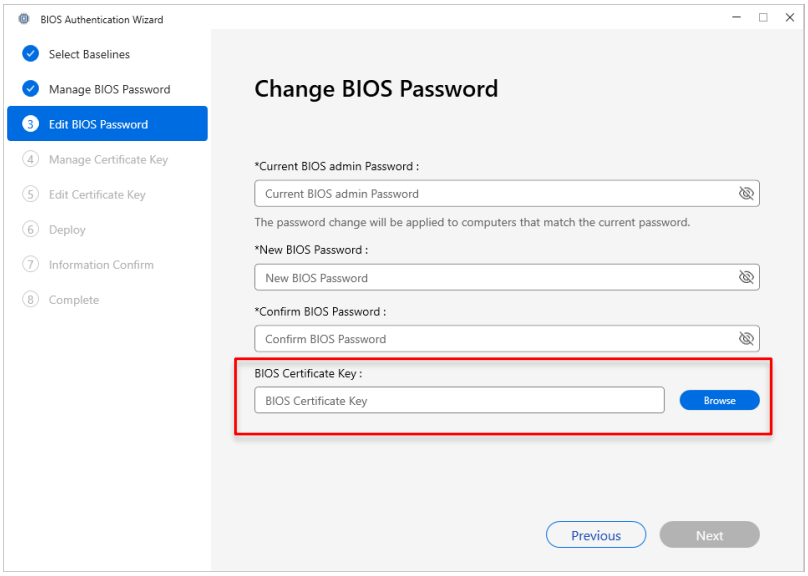
2.1 Create new BIOS admin password

To ensure the password is sufficiently strong, it is recommended to use a complex password that includes a combination of uppercase and lowercase letters, numbers, and symbols. For password strength, please keep password 8-64 digitals.



2.2 Change BIOS admin password

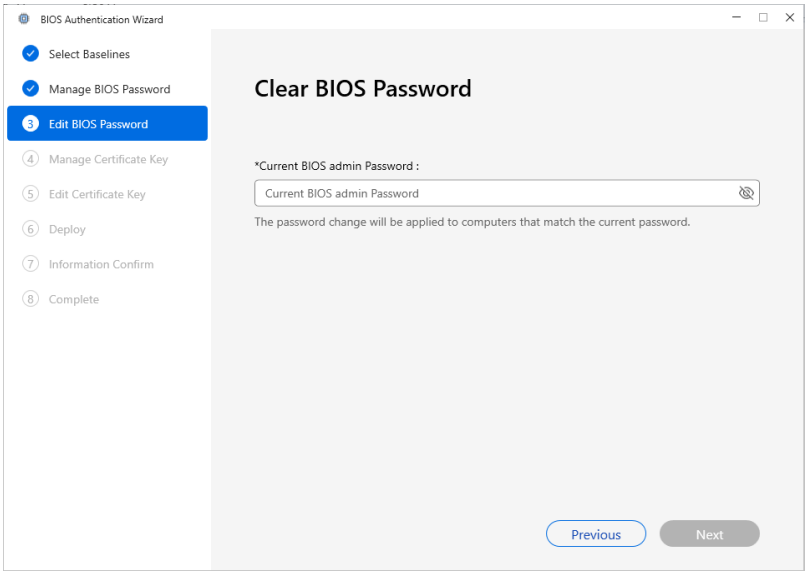
Edit BIOS Admin Password: User should provide the client devices' current BIOS admin password as verification and update the new BIOS admin password.



It may require to input certificate key **if the deployed devices had been enrolled before.** (For more details, please check appendix of certificate keys.)

2.3 Clear BIOS admin password

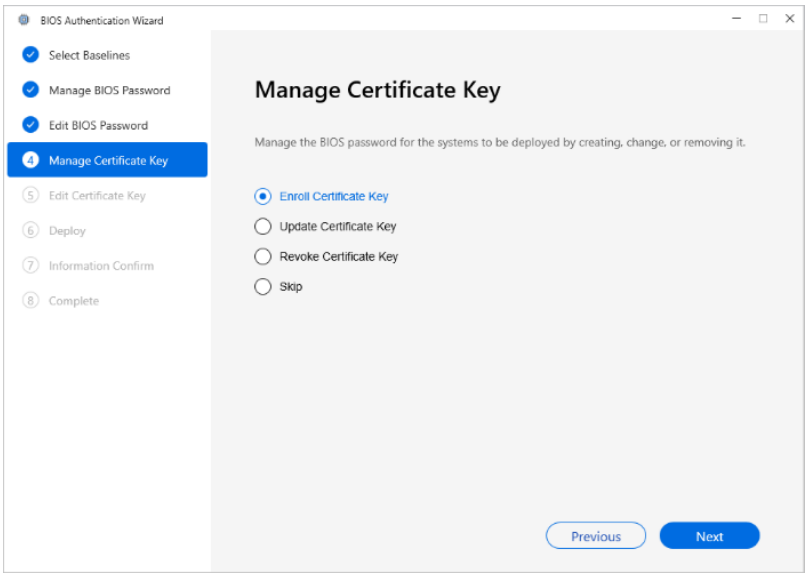
Current BIOS admin password is required to clear the admin password.
If the devices are enrolled, clearing BIOS admin password will also revoke the certificate key.



3. Manage BIOS Certificate Key: to enroll, update, or revoke the provision. The step can be skipped if the current settings are to be retained.

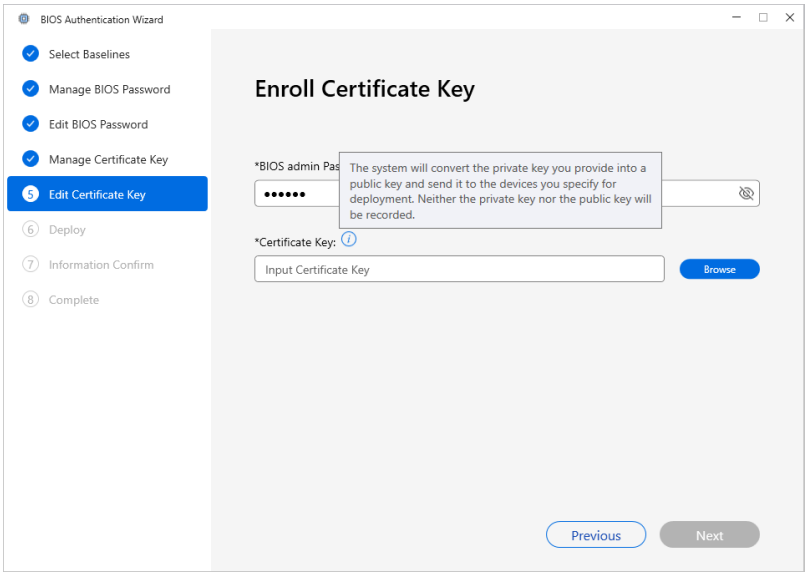
3.1 Enroll certificate key

For BIOS enrollment, BIOS admin password is required.

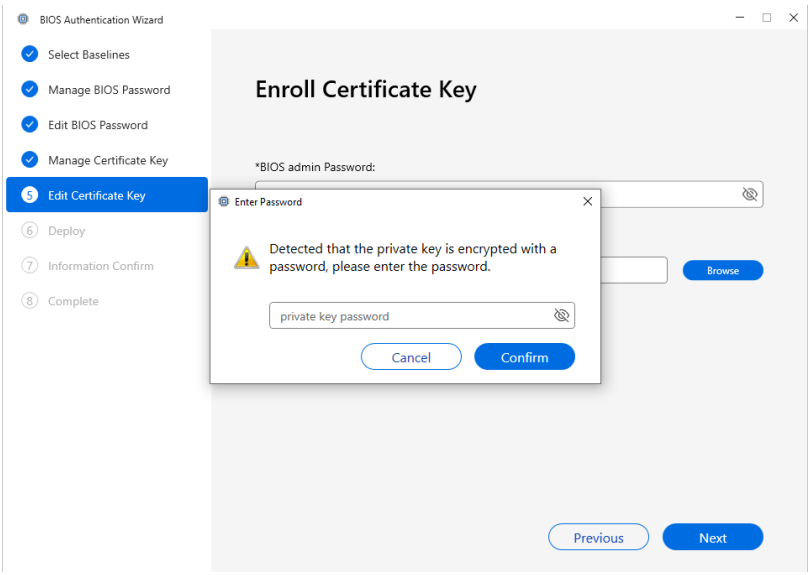


The system will convert the private key user provided into a public key and send it to the devices user specify for deployment.

**Neither the private key nor the public key will be recorded.*

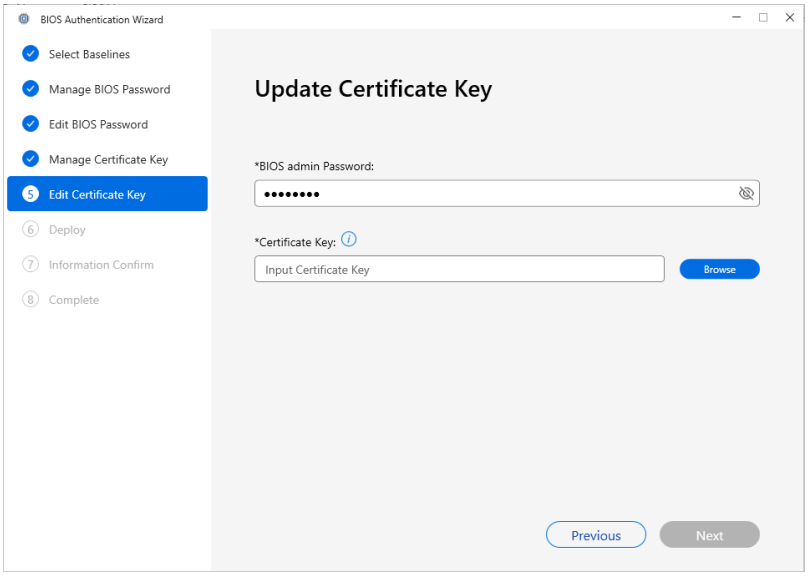


Depending on how the key pair was generated, some keys *may* be encrypted. In such cases, please enter the password used to encrypt the key at the time of its creation.



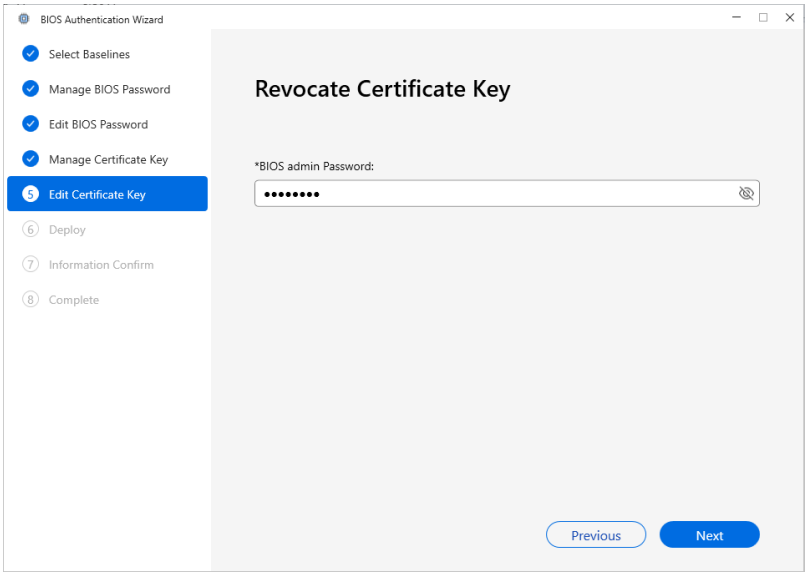
3.2 Update certificate key

If the selected baseline has a BIOS admin password set, ASUS ACM will use this password for the certificate key update. Otherwise, the current BIOS admin password is required to update the certificate key.

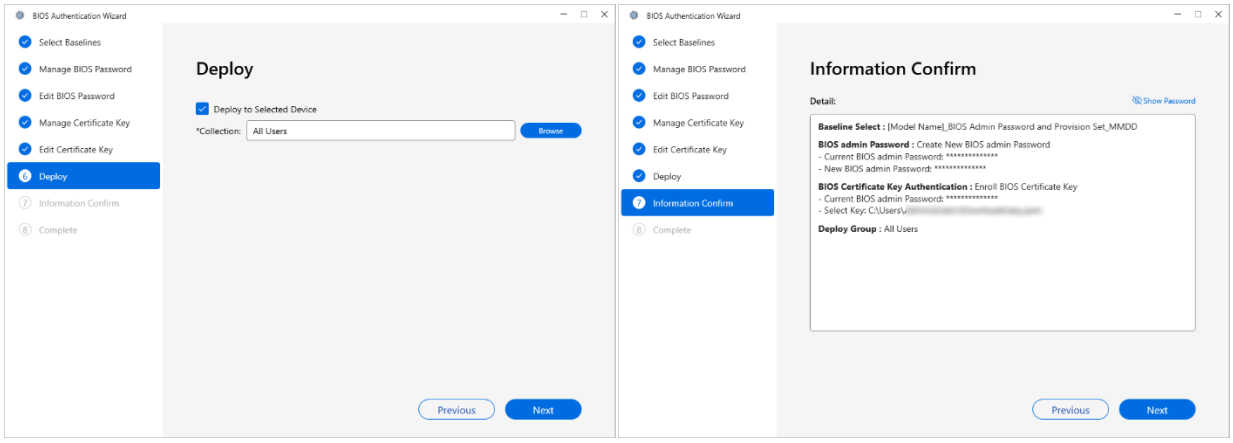


3.3 Revoke Certificate

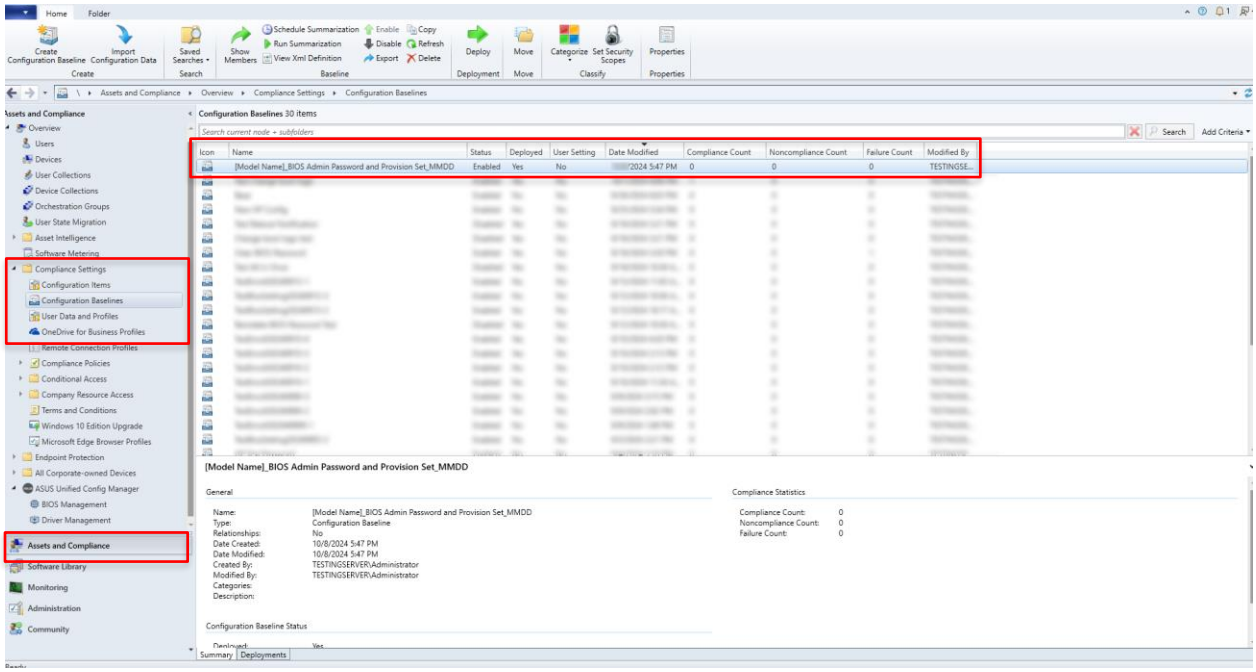
To revoke the certificate key, the BIOS admin password used for enrollment is required.



4. Select the target collection for deployment and review the baseline settings information before proceeding.



5. Once completed, the baseline can be viewed under Compliance Settings.
   Assets and Compliance > Compliance Settings > Configuration Baseline



BIOS Configuration

Effortlessly configure BIOS settings with a user-friendly GUI and deploy them to multiple devices. BIOS Configuration also allows to customize and change the boot logo as needed.

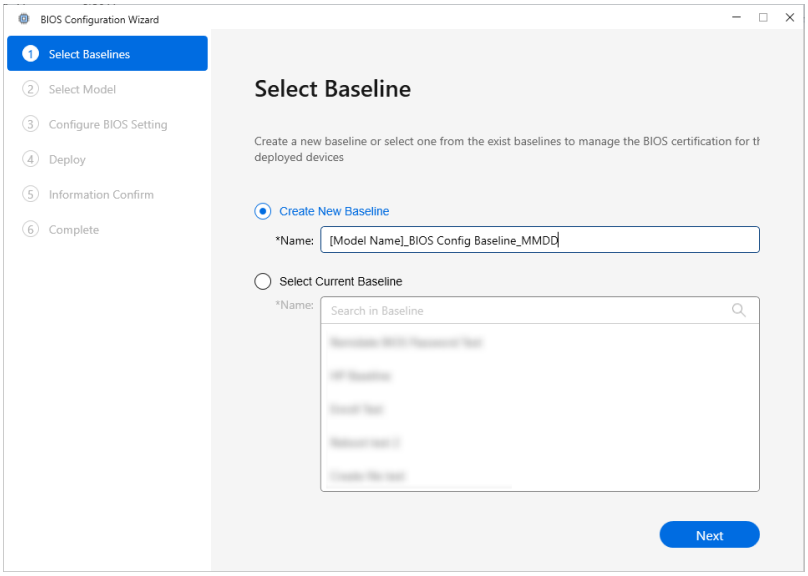
The following three scenarios allow BIOS configuration changes:
1. Client device with no BIOS admin password and no key set.
2. Client device with a BIOS admin password set.
3. Client device with both BIOS admin password and key set.

This authorization mechanism ensures that only properly authorized users can modify BIOS settings, enhancing the overall security of the device.

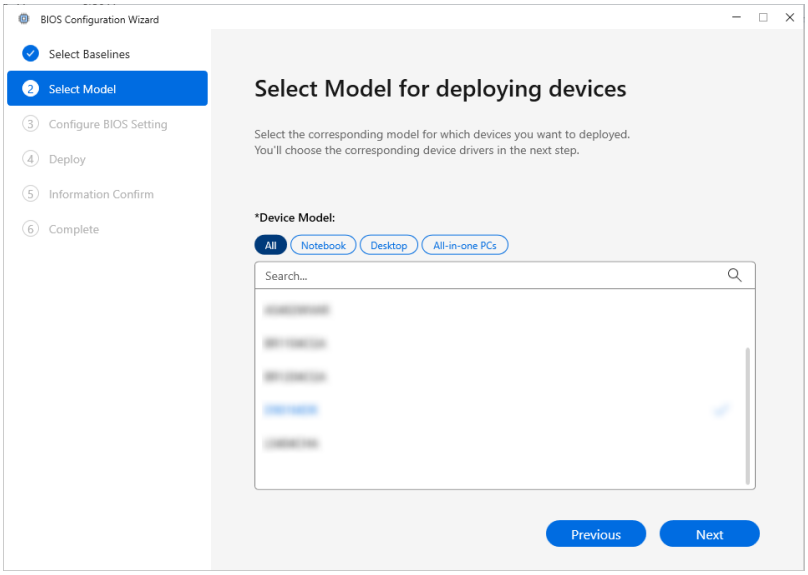
Supported Client Platforms:

- ASUS Commercial Products (2024 or later)

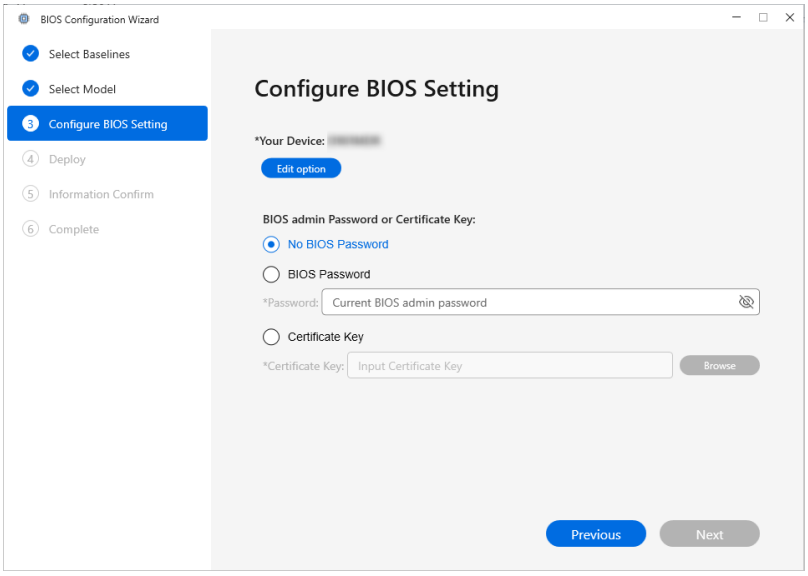
1. Create a new baseline or choose a current baseline (for future new devices following).



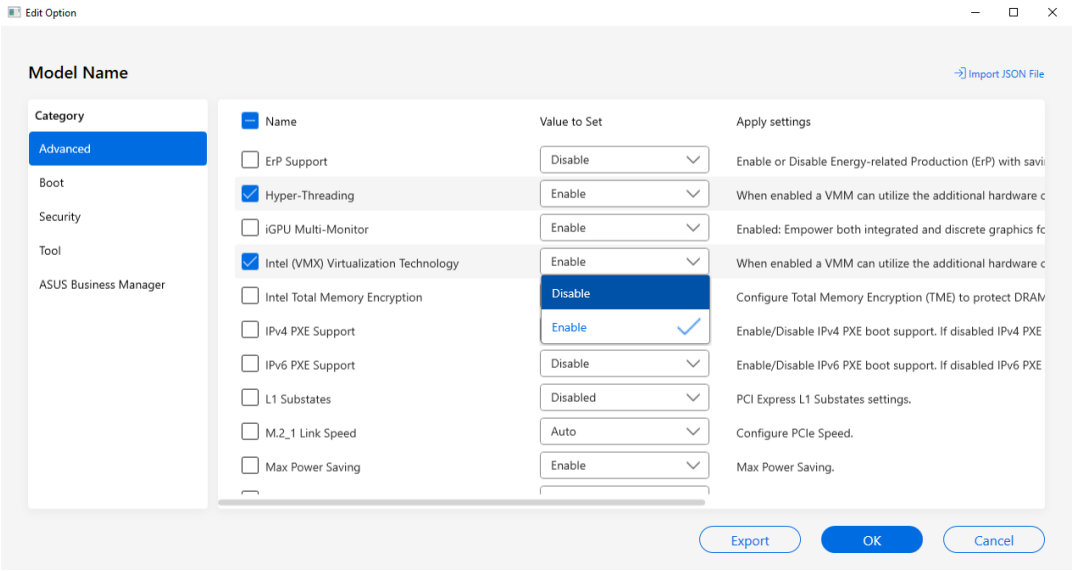
2. Select a model as the reference for the configuration items, and prepare it for deployment.



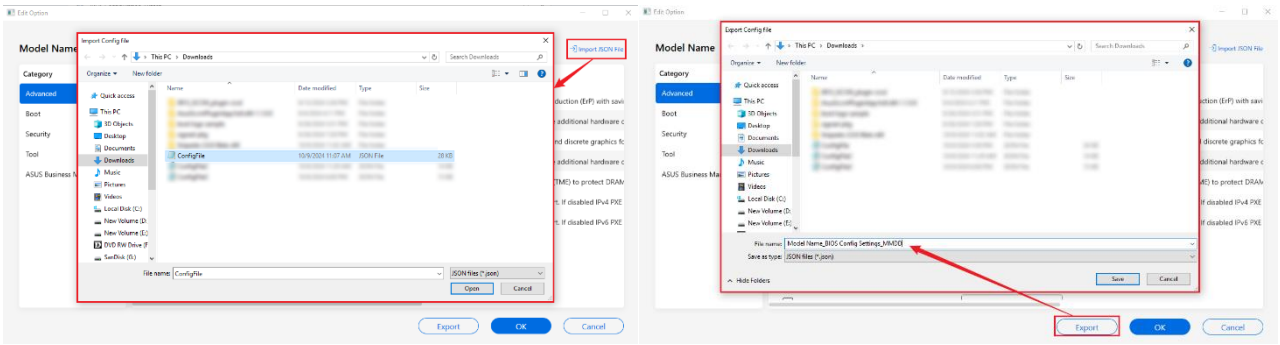
3. Edit the BIOS Configuration Settings: Click "Edit Option" to change the setting with user interface, and remember to provide BIOS admin password or certificate key as the authentication verification.



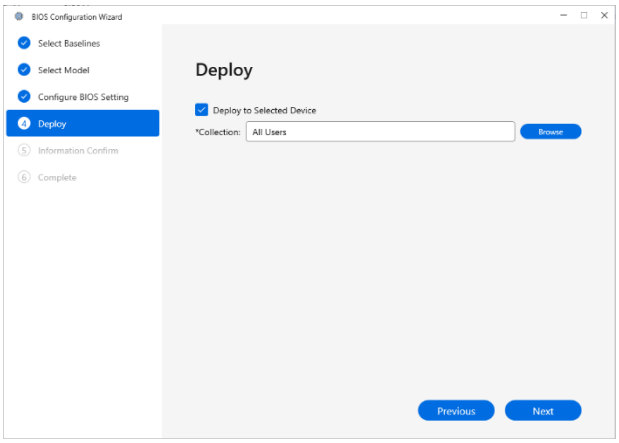
Ensure to tick the checkbox of any options that have been modified

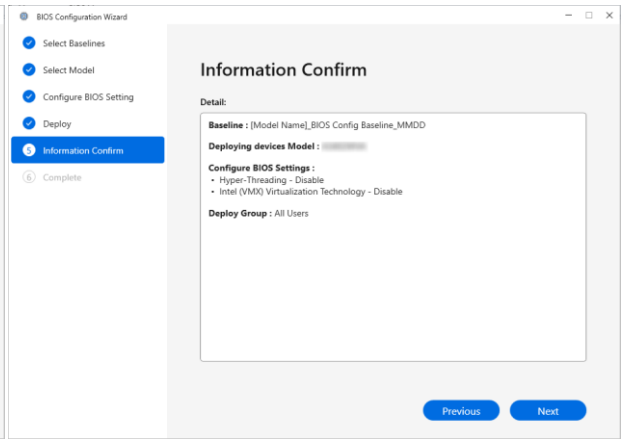


Import a JSON settings file as a reference sample, or export it to save the current configuration.



4. Choose the collection for deployment and make the final confirmation.





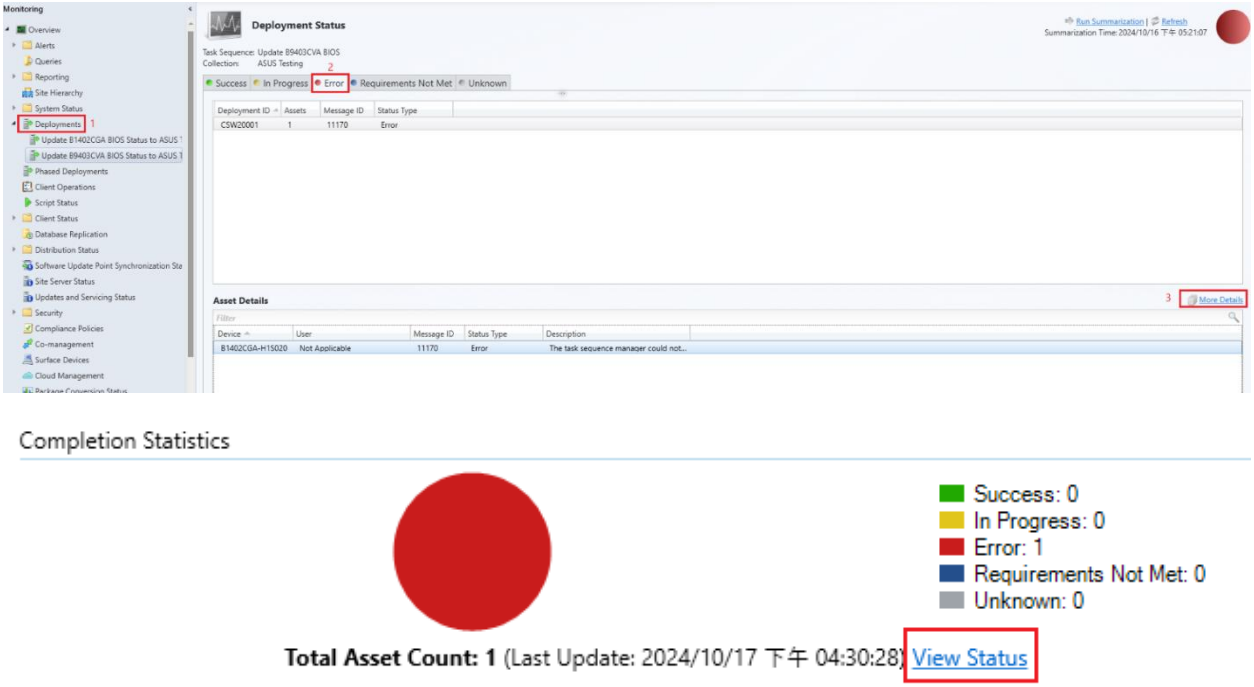
5. The baseline of configuration can be viewed under Compliance Settings.
   Assets and Compliance > Compliance Settings > Configuration Baseline

3. Deploy Result and Error Analysis

Deploy results can be checked from Monitor > Deployments.

Error Status of Driver Updater

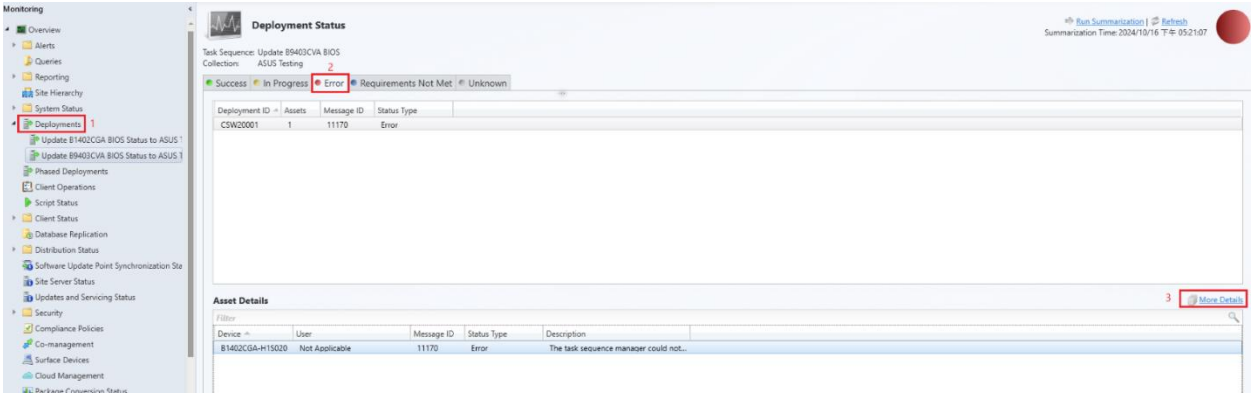
Click on the pie chart, then select View Status > Error > (Choose 1 failed device) > More Details to check the reasons for each device's failure.

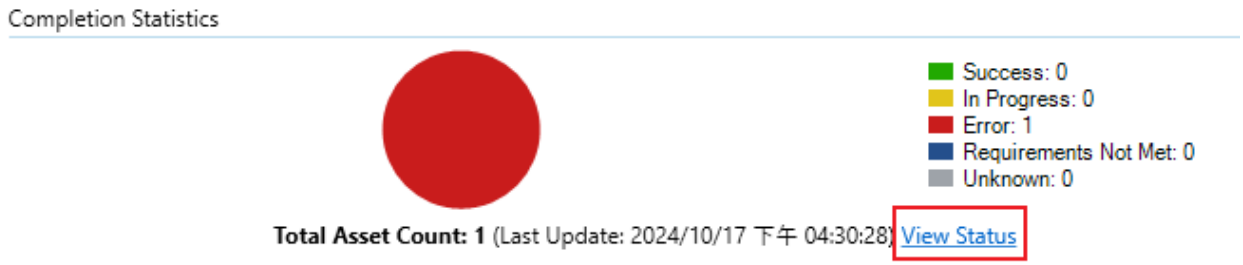


The error code can be obtained from the Exit Code of the "Install Package" step in Status. Please refer to the error code from Microsoft.
https://learn.microsoft.com/en-us/windows-hardware/drivers/devtest/pnputil-return-values

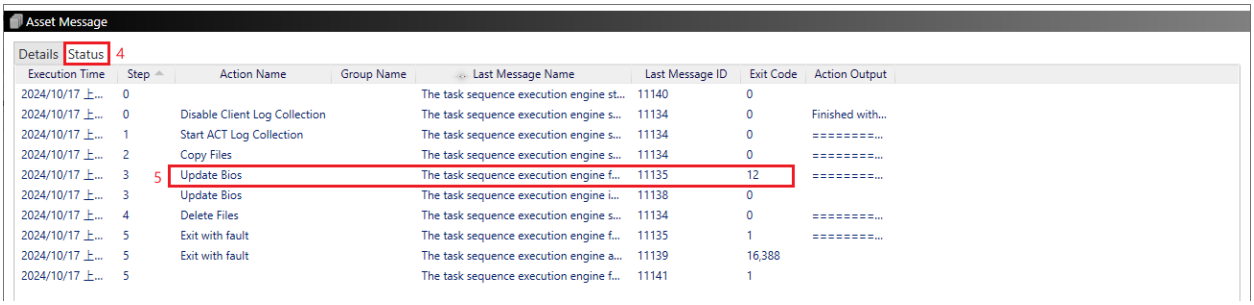
Error Status of BIOS Updater

Click on the pie chart, then select View Status > Error > (Choose 1 failed device) > More Details to check the reasons for each device's failure.





The error code can be obtained from the Exit Code of the "Update Bios" step in Status.
In the example below, the code is 12.



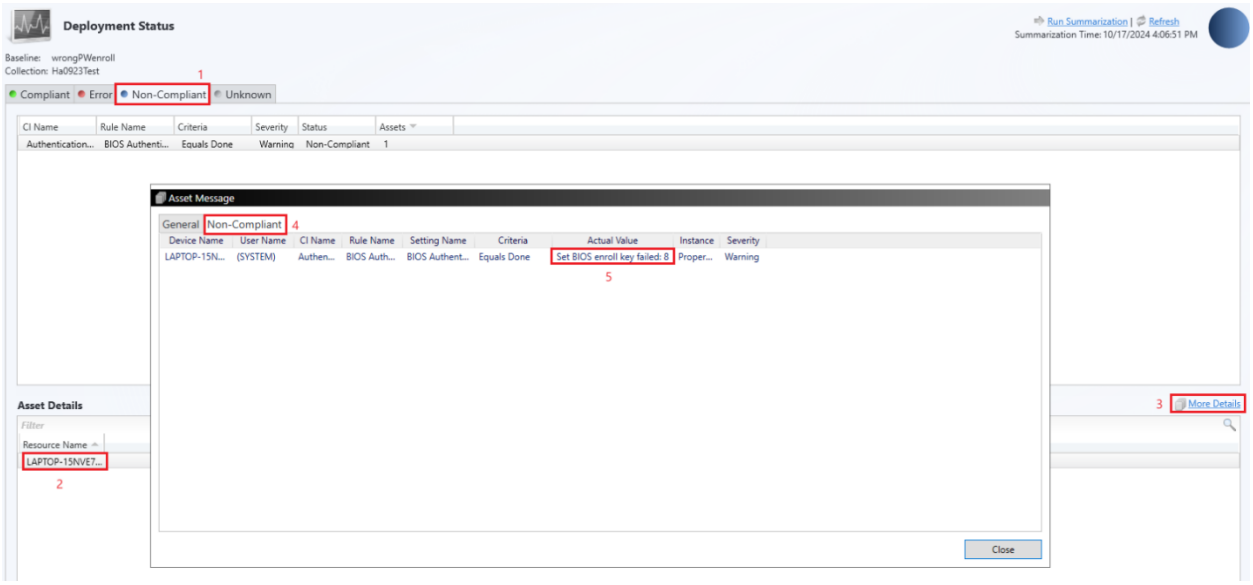
The common error codes are as below:

Error Code	Description
kSuccess(0)	BIOS firmware is updated successfully.
kFail(1)	BIOS firmware update is failed. The reasons may vary; it might be caused by invalid BIOS firmware file, incorrect hash value, firmware file is corrupted or not signed by ASUS, among other possibilities.
kPermissionDenied(8)	The client device is locked by BIOS admin password, but the given password is incorrect.
kModelMismatch(12)	The chosen BIOS firmware model name is mismatched the device.
kSkip(13)	The BIOS version of the client device is equal to or greater than the specified version, so this update would be skipped.

Error Status of BIOS Authentication or BIOS Configuration

Click on the pie chart, then select View Status > Non-Compliant > (Choose 1 failed device) > More Details to check the reasons for each device's deployment failure.
The failure reason will be shown on Non-Compliant > Actual Value and the last number means the error code.

For example, the error occurred during the 'Set BIOS enroll key' step, and the error code is 8.



The common error codes are as below:

Error Code	Description
kSuccess(0)	BIOS authentication / configuration is deployed and updated successfully.
kFail(1)	BIOS authentication / configuration update is failed. The reasons may vary; it could be that the devices are already equipped with an old password, preventing the creation of a new one, or the BIOS password has not taken effect before rebooting, among other possibilities.
kInvalidArguments(2)	BIOS admin password strength requirements have not been met.
kInvalidBiosImpl(3)	The platform is not supported.
kPermissionDenied(8)	BIOS admin password or certificate key does not match the devices being deployed.
kFault(9)	Unhandled error.

Error Report

If an error occurs that requires assistance from ASUS, please provide the files `C:\windows\temp\AsusSccmxxxxx.etl` and `C:\windows\temp\AsusSccmExecution.log` for analysis.

4. FAQs

5. Appendix – ASUS Commercial Products

Check Supported Model List:
https://dlcdnccls.asus.com/data/acm/ASUS_Config_Manager_Supported_Models.pdf

	Commercial Models	Limitation
Driver Package, Driver Updater	Y2020 and newer	
BIOS Update	Y2020 and newer	Y2024 and later supported for update with password set
BIOS Authentication, BIOS Configuration	Y2024 and newer	Support WMI 4.0 interface models

6. Appendix – Certificate Key

BIOS Authentication implements certificate to ensure secure communication and data encryption. IT managers can enroll key pair to BIOS to authenticate devices, ensuring that only authorized hardware can interact with the BIOS.

- It is IT's responsibility to create, maintain, and protect the private key.
- ASUS ACM will create correspond public key automatically according to the private key user provided, and enroll the client devices with the public key.
- Neither the private key nor the public key will be recorded.

How to Prepare A Key Pair

The key pair needs to be a **RSA** key pair with **2048-bit** length created by **OpenSSL** utility.
User is responsible to keep the private key protected.

Example:
To prepare a 2048-bit RSA key pair by OpenSSL.
Creating a private key using passphrase `private.2048.pem` to protect the private key.

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

If a key pair is needed, 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 there is a key pair: private.2048.pem(private key) and public.2048.pem(public key).