

# ASUS Config Manager

User Guide v1.1



# 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.....	5
Run Application .....	6
Driver Package Creator .....	6
Driver Updater.....	9
BIOS Updater.....	10
BIOS Admin Password and Authentication .....	13
BIOS Configuration .....	19
3. Deploy Result and Error Analysis.....	23
Error Status of Driver Updater .....	23
Error Status of BIOS Updater .....	24
Error Status of BIOS Authentication or BIOS Configuration .....	25
Error Report .....	26
4. FAQs .....	26
5. Appendix – ASUS Commercial Products .....	27
6. Appendix – Certificate Key .....	28

## 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

## 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 server 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.

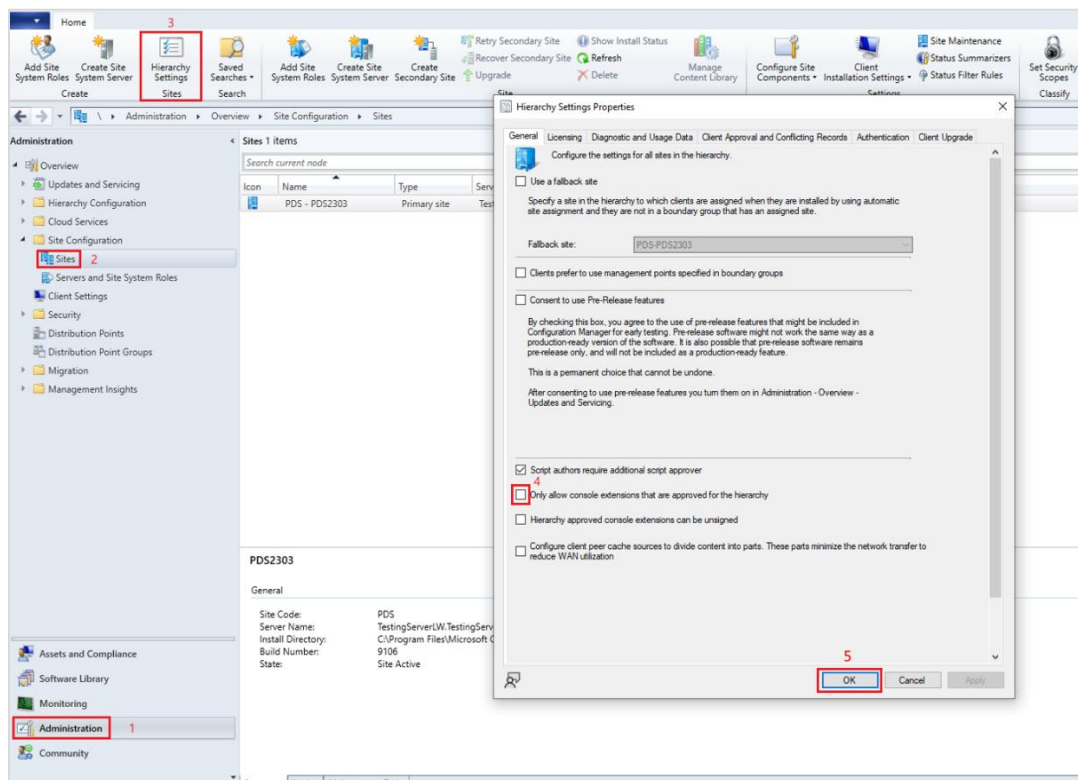
*\*For more information on supported products, refer to the 5 Appendix – ASUS Commercial Products.*

## 2. Using ASUS Config Manager

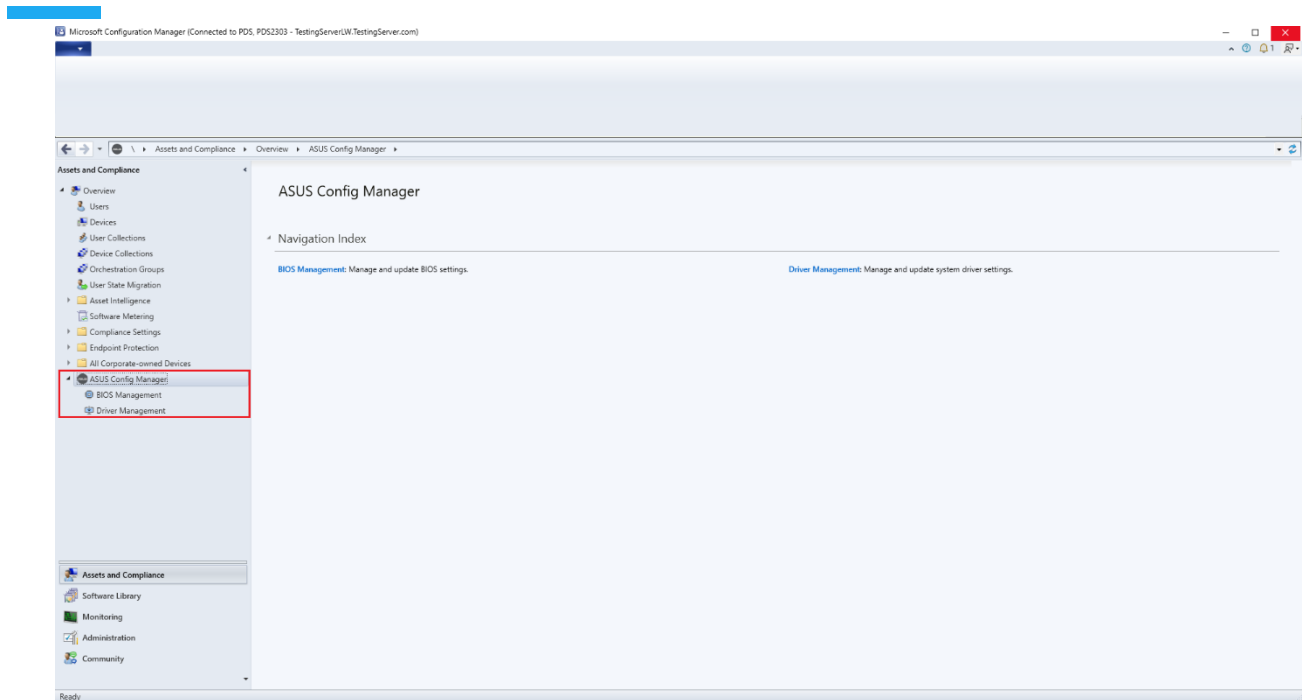
### Installation

To download and install the ASUS Config Manger:

1. Go to ASUS support site: [Centralized 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.



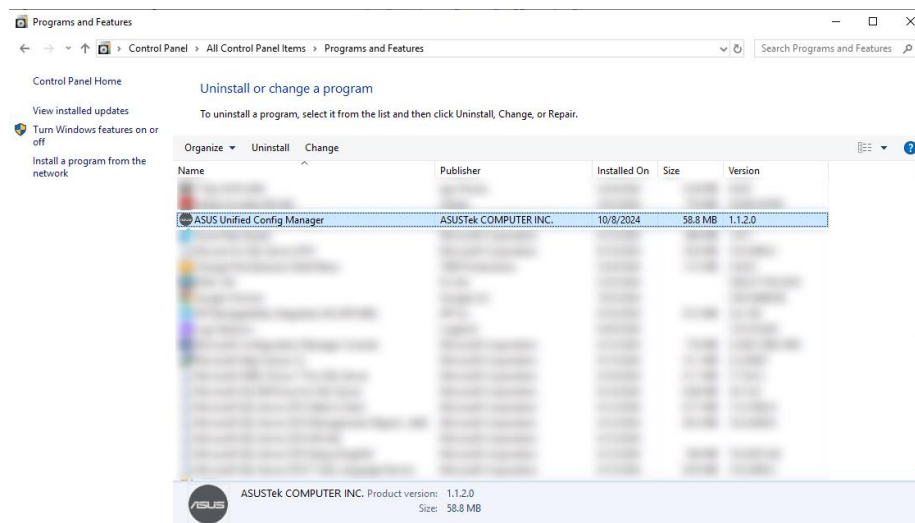
4. Run the downloaded ASUS Config Manger (ACM) for Microsoft System Center Configuration Manager SoftPaq and follow the on-screen instructions to complete the installation.
5. Open or **restart** the Microsoft SCCM Console and verify that ASUS Config Manager is displayed under Assets and Compliance.



## 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.

The first screenshot shows the 'Select Model' step of the Driver Package Creator Wizard. The left sidebar lists the steps: 1. Select Model (active), 2. Select OS, 3. Select Driver Category, 4. Generate Package, 5. Upload, 6. Information Confirm, and 7. Download and Generate. The main area is titled 'Select Model for deploying devices' and includes a search bar and a list of device models: B9403, B9403CVA, and B9403CVAR. Below the list are tabs for 'All', 'Notebook', 'Desktop', and 'All-in-one PCs'. A 'Next' button is at the bottom right.

The second screenshot shows the 'Select OS' step. The left sidebar is the same, but step 2 'Select OS' is now active. The main area is titled 'Select OS for deploying devices' and includes a dropdown menu for 'OS Version'. The dropdown shows 'Windows 11 (64-bit)' selected with a checkmark, and 'Windows 10 (64-bit)' as an option. 'Previous' and 'Next' buttons are at the bottom right.

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

The screenshot shows the 'Select Driver Category' step of the Driver Package Creator Wizard. The left sidebar lists the steps: 1. Select Model, 2. Select OS, 3. Select Driver Category (active), 4. Generate Package, 5. Upload, 6. Information Confirm, and 7. Download and Generate. The main area is titled 'Select driver category for deploying devices' and includes a section for 'Full Package' and 'By driver class'. Under 'By driver class', there are checkboxes for 'Biometric Authentication', 'Bluetooth', 'Camera', 'Card Reader', 'Pointing Device', and 'Software and Utility'. The 'Bluetooth' and 'Camera' checkboxes are checked. 'Previous' and 'Next' buttons are at the bottom right.

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

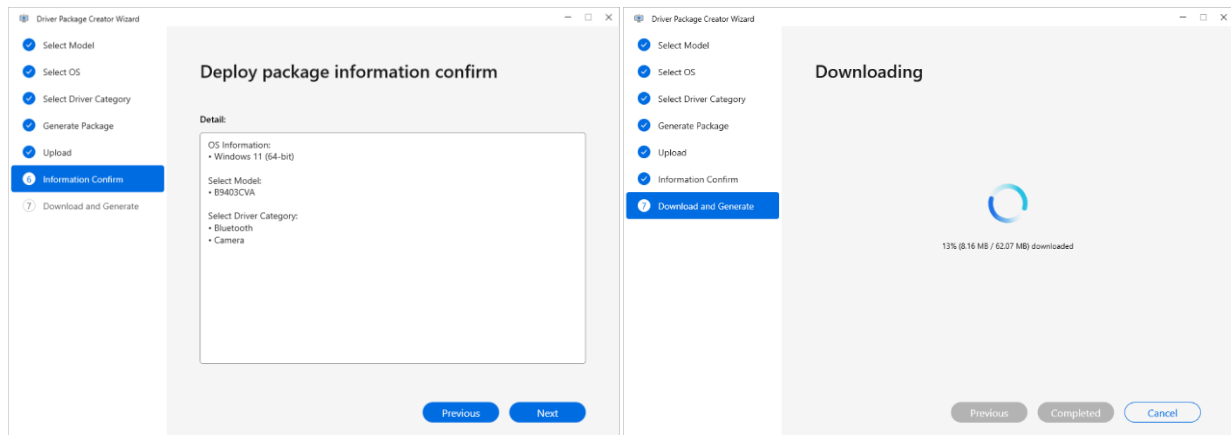
The screenshot shows the 'Driver Package Creator Wizard' window at the 'Generate Package' step. The left sidebar lists steps 1 through 7, with 'Generate Package' (step 4) highlighted in blue. The main area is titled 'Driver Package Generate'. It contains a text field for '\*Name:' with the value '[Model Name]\_Driver Package for OS Deployment\_MMDD'. Below this, the 'Task Sequence:' section has two radio buttons: 'Do not create task sequence' and 'Create new task sequence'. The 'Create new task sequence' option is selected and highlighted with a red rectangle. Below the radio buttons, there is another text field for '\*Name:' with the value '[Model Name]\_OS Deployment\_MMDD'. At the bottom right, there are 'Previous' and 'Next' buttons.

4. Whether to upload to the distribution points.

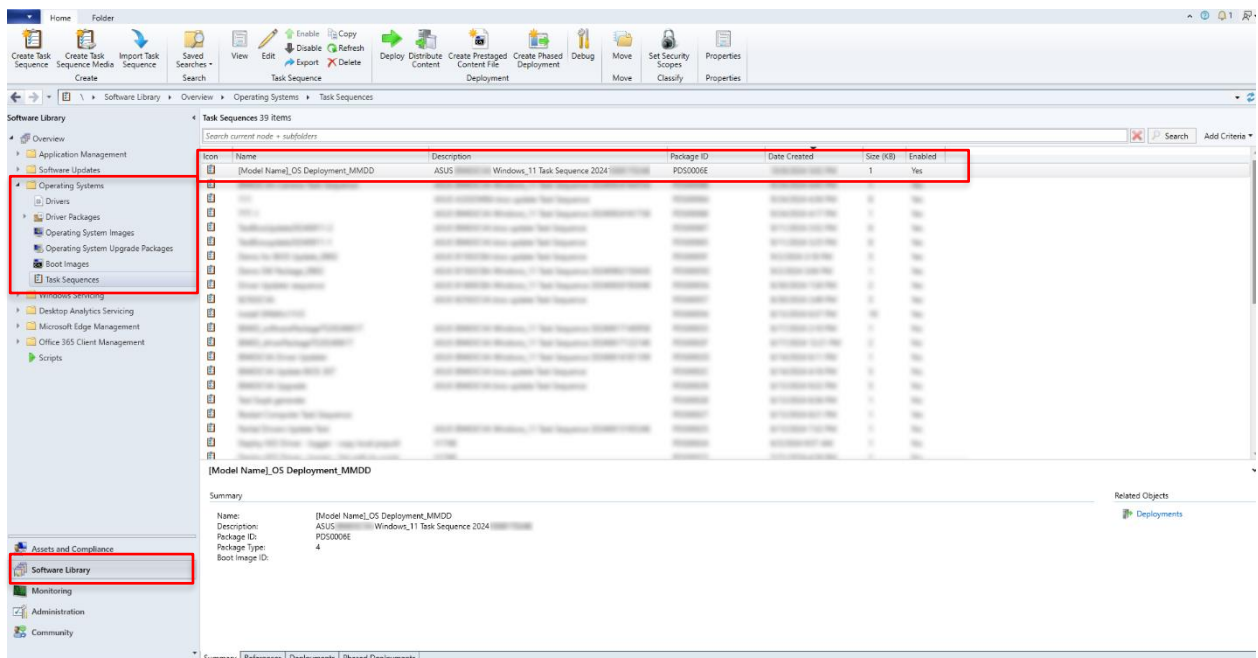
The screenshot shows the 'Driver Package Creator Wizard' window at the 'Upload' step. The left sidebar lists steps 1 through 7, with 'Upload' (step 5) highlighted in blue. The main area is titled 'Upload'. It contains a section for 'Update:' with a checked checkbox for 'Update to distribution point'. Below this, there is a text field for 'Select the distribution point to update' and a 'Browse' button. At the bottom right, there are 'Previous' and 'Next' buttons.



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.

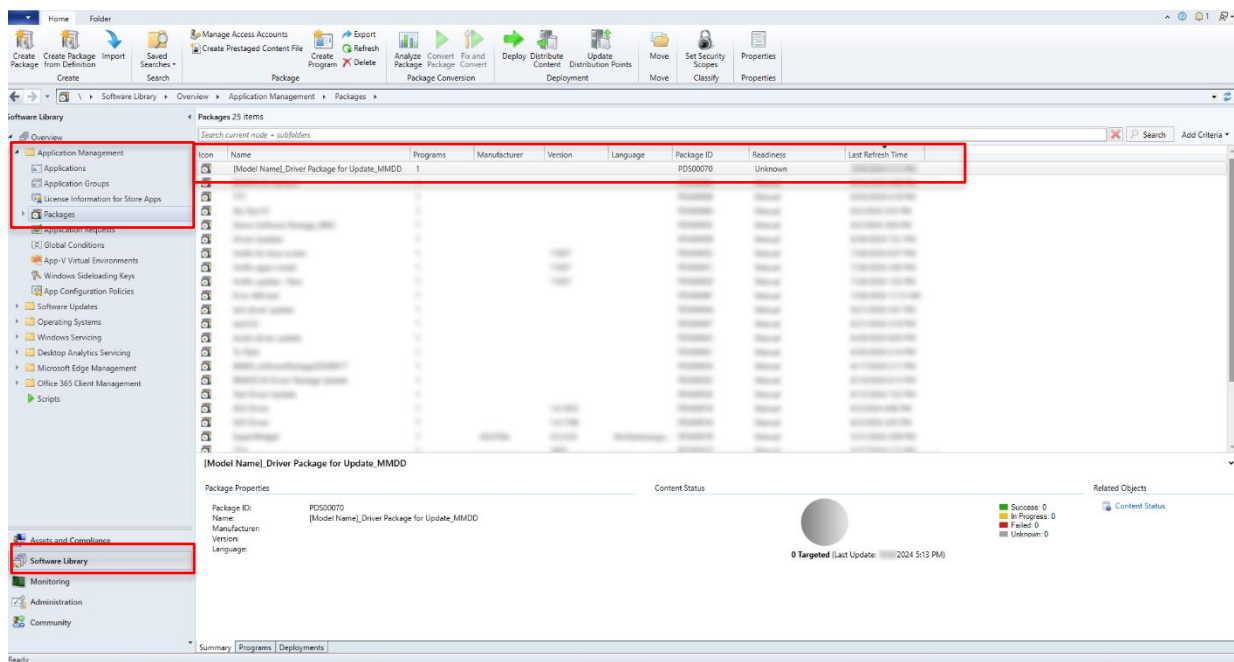
1. Select the particular model and its OS version for drivers update.
2. Select the drivers: customize the driver software package or choose the full package.
3. Generate a Driver Software Package: name the package and decide to create a task sequence or not. Choose whether to turn off reboot notification.

The screenshot shows the 'Driver Package Creator Wizard' window, specifically the 'Software Package Generate' step. On the left, a vertical list of steps is shown: 'Select Model', 'Select OS', 'Select Driver Category', '4 Generate Package' (highlighted in blue), '5 Choose Deploy Device', '6 Upload', '7 Information Confirm', and '8 Download and Generate'. The main area contains the following fields and options:

- \*Name:** A text box containing 'Driver Update\_YYMMDD'.
- Task Sequence:** Two radio buttons: 'Do not create task sequence' and 'Create new task sequence' (selected).
- \*Name:** A text box containing 'Driver Update\_YYMMDD'.
- Advance Settings:** A checkbox labeled 'Turn off automatic reboot notification (effective upon next boot)' is shown with a red arrow pointing to it.
- At the bottom right are 'Previous' and 'Next' buttons.

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.*

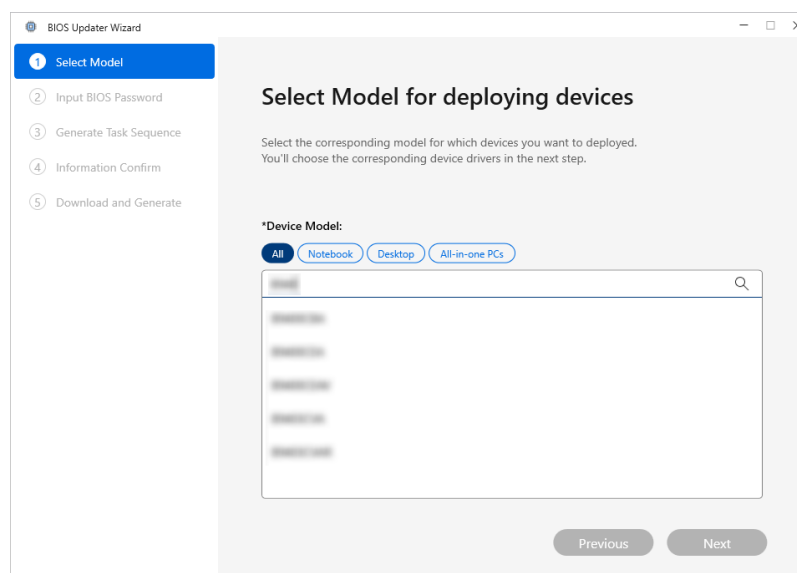
- After completed, the **software package** can be checked under Application Management.  
Software Library > Application Management > Packages



## 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.

- Select the particular model for BIOS update deployment.



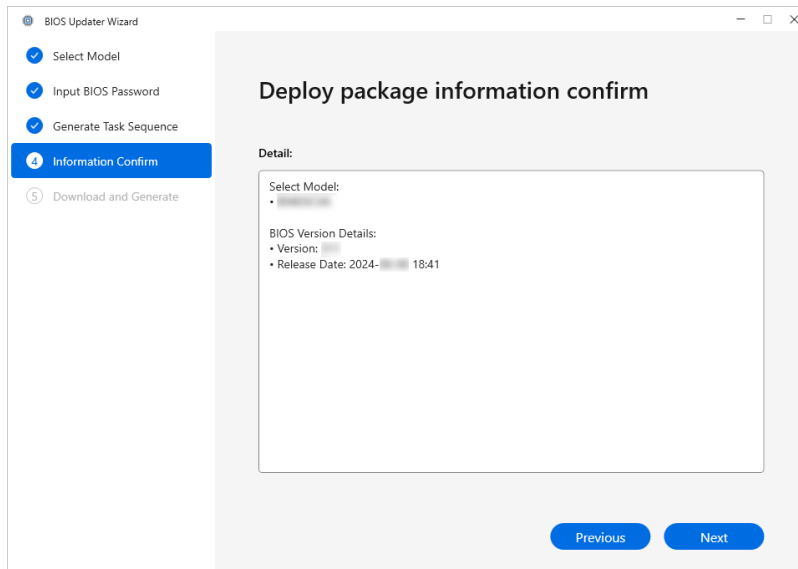
2. Input the BIOS Admin Password if the deployed devices are set.

The screenshot shows the 'BIOS Updater Wizard' window. The left sidebar has five steps: 1. Select Model (checked), 2. Input BIOS Password (highlighted in blue), 3. Generate Task Sequence, 4. Information Confirm, and 5. Download and Generate. The main area is titled 'Input BIOS password' and contains the text 'If your device has BIOS Password, please input here.' Below this is a text input field labeled 'BIOS Password :'. A small icon of a crossed-out eye is to the right of the field. Below the field is the text 'Keep this field blank if BIOS password is not set.' At the bottom right are two blue buttons: 'Previous' and 'Next'.

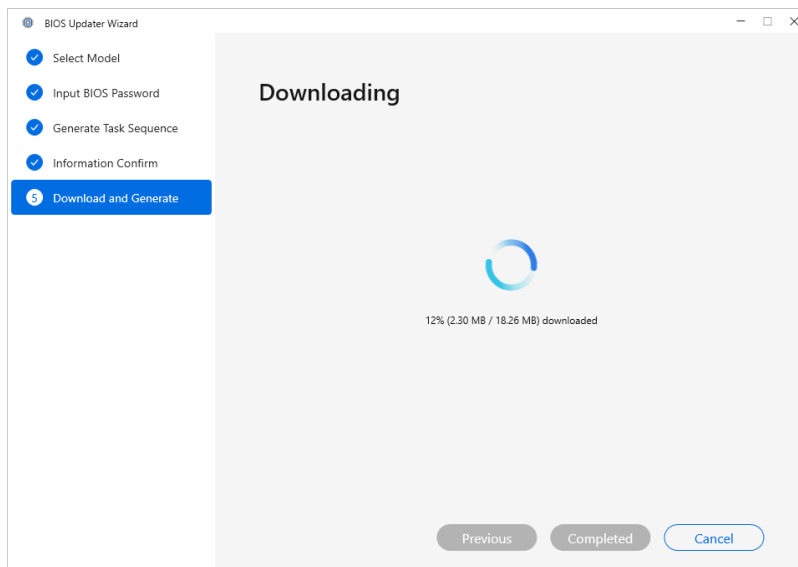
3. Create a task sequence or add to current task sequence for deployment.  
Remember to select deployed devices collection.

The screenshot shows the 'BIOS Updater Wizard' window. The left sidebar has six steps: 1. Select Model (checked), 2. Input BIOS Password (checked), 3. Generate Task Sequence (highlighted in blue), 4. Choose Deploy Device, 5. Information Confirm, and 6. Download and Generate. The main area is titled 'Select Task Sequence'. It has two sections: 'Task Sequence:' and 'Advance Settings:'. Under 'Task Sequence:', there are two radio buttons: 'Create new task sequence' (selected) and 'Add to current task sequence'. Below the 'Add to current task sequence' radio button is a dropdown menu with the text 'Select a task sequence'. Under 'Advance Settings:', there is a checkbox labeled 'Turn off automatic reboot notification (effective upon next boot.)'. An orange arrow points to this checkbox. At the bottom right are two blue buttons: 'Previous' and 'Next'.

#### 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).

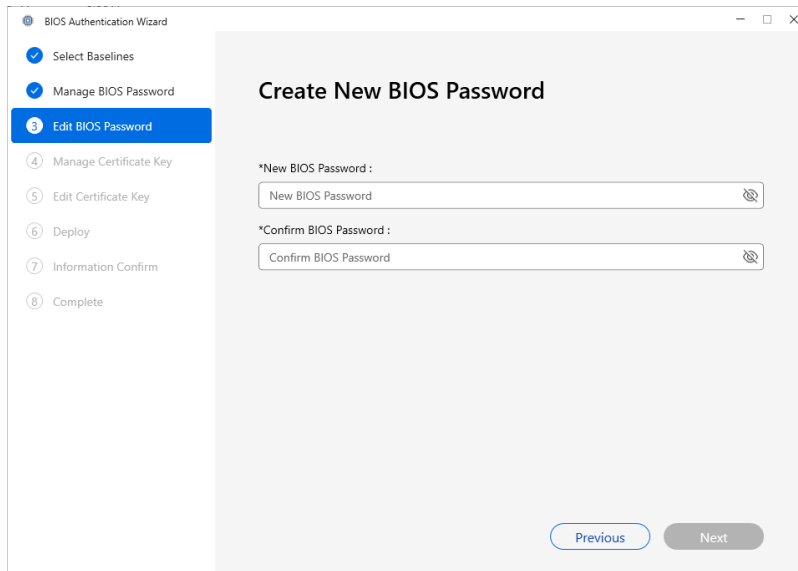
The screenshot shows the 'Select Baseline' step of the BIOS Authentication Wizard. On the left is a vertical sidebar with steps 1 through 8. Step 1, 'Select Baselines', is highlighted in blue. The main area has the title 'Select Baseline' and a subtitle 'Create a new baseline or select one from the exist baselines to manage the BIOS certification for ti deployed devices'. There are two radio button options: 'Create New Baseline' (selected) and 'Select Current Baseline'. Below 'Create New Baseline' is a text input field with the placeholder text '[Model Name]\_BIOS Admin Password and Provision Set\_MMDD'. Below 'Select Current Baseline' is a search input field with the placeholder 'Search in Baseline' and a magnifying glass icon. Below the search field is a list of baseline names, including 'Baseline\_001', 'Baseline\_002', 'Baseline\_003', 'Baseline\_004', and 'Baseline\_005'. At the bottom right is a blue 'Next' button.

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.

The image shows two side-by-side screenshots of the BIOS Authentication Wizard. The left screenshot is the 'Manage BIOS Password' step, with step 2 highlighted in the sidebar. It has three radio button options: 'Create New BIOS Password' (selected), 'Change BIOS Password', and 'Clear BIOS Password'. There is also a 'Skip' option. The right screenshot is the 'Manage Certificate Key' step, with step 4 highlighted in the sidebar. It has four radio button options: 'Enroll Certificate Key', 'Update Certificate Key', 'Revoke Certificate Key', and 'Skip' (selected). A red box highlights the 'Manage BIOS Password' step in the sidebar of the right screenshot. A text box at the bottom center of the right screenshot contains the text: 'If skipped "Manage BIOS Password" step, it will jump to "Manage Certificate Key" step.' Both screenshots have 'Previous' and 'Next' buttons at the bottom.

## 2.1 Create new BIOS admin password

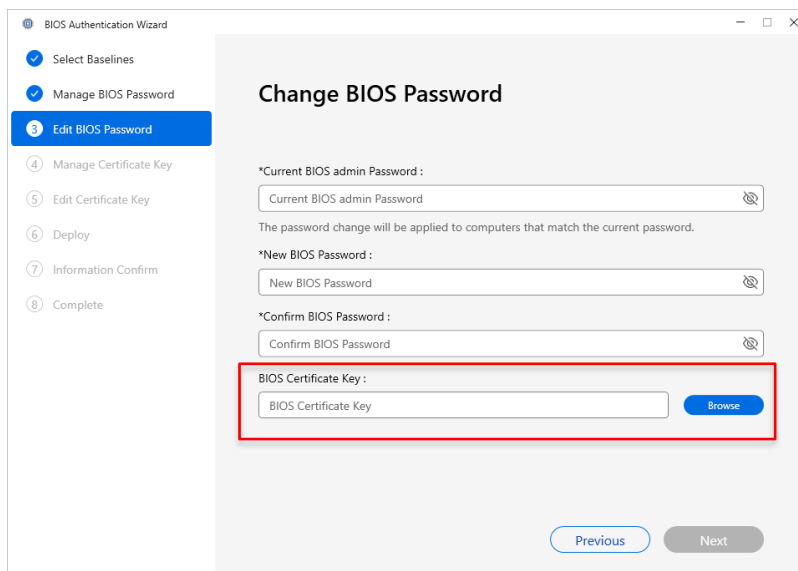
To ensure the password is sufficiently strong, it is recommended to use a complex password that includes a combination of uppercase and lowercase letters, numbers, and symbols. For password strength, please keep password 8-64 digitals.



The screenshot shows the 'BIOS Authentication Wizard' window. On the left, a vertical list of steps is shown: 1. Select Baselines, 2. Manage BIOS Password, 3. Edit BIOS Password (highlighted in blue), 4. Manage Certificate Key, 5. Edit Certificate Key, 6. Deploy, 7. Information Confirm, and 8. Complete. The main area is titled 'Create New BIOS Password'. It contains two input fields: '\*New BIOS Password :' and '\*Confirm BIOS Password :'. Each field has a text input area and a small icon to the right. At the bottom right, there are 'Previous' and 'Next' buttons.

## 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.



The screenshot shows the 'BIOS Authentication Wizard' window. On the left, a vertical list of steps is shown: 1. Select Baselines, 2. Manage BIOS Password, 3. Edit BIOS Password (highlighted in blue), 4. Manage Certificate Key, 5. Edit Certificate Key, 6. Deploy, 7. Information Confirm, and 8. Complete. The main area is titled 'Change BIOS Password'. It contains three input fields: '\*Current BIOS admin Password :', '\*New BIOS Password :', and '\*Confirm BIOS Password :'. Each field has a text input area and a small icon to the right. Below these fields, there is a section for 'BIOS Certificate Key' with a text input area and a 'Browse' button. This section is highlighted with a red rectangle. At the bottom right, there are 'Previous' and 'Next' buttons.

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.*

The screenshot shows the 'BIOS Authentication Wizard' window. On the left, a vertical list of steps is shown: 1. Select Baselines, 2. Manage BIOS Password, 3. Edit BIOS Password (highlighted in blue), 4. Manage Certificate Key, 5. Edit Certificate Key, 6. Deploy, 7. Information Confirm, and 8. Complete. The main area is titled 'Clear BIOS Password'. It contains a label '\*Current BIOS admin Password :' followed by a text input field labeled 'Current BIOS admin Password'. Below the input field, a note states: 'The password change will be applied to computers that match the current password.' At the bottom right, there are two buttons: 'Previous' and 'Next'.

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 screenshot shows the 'BIOS Authentication Wizard' window. On the left, the steps are: 1. Select Baselines, 2. Manage BIOS Password, 3. Edit BIOS Password, 4. Manage Certificate Key (highlighted in blue), 5. Edit Certificate Key, 6. Deploy, 7. Information Confirm, and 8. Complete. The main area is titled 'Manage Certificate Key'. Below the title, a subtitle reads: 'Manage the BIOS password for the systems to be deployed by creating, change, or removing it.' There are four radio button options: 'Enroll Certificate Key' (selected), 'Update Certificate Key', 'Revoke Certificate Key', and 'Skip'. At the bottom right, there are two buttons: 'Previous' and 'Next'.



**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.*

The screenshot shows the 'Enroll Certificate Key' step in the BIOS Authentication Wizard. On the left, a sidebar lists steps: Select Baselines, Manage BIOS Password, Edit BIOS Password, Manage Certificate Key (highlighted), Deploy, Information Confirm, and Complete. The main area has a title 'Enroll Certificate Key'. Below it, there's a field for '\*BIOS admin Password' with a masked input and a 'Browse' button. A tooltip explains: 'The system will convert the private key you provide into a public key and send it to the devices you specify for deployment. Neither the private key nor the public key will be recorded.' Below this is a field for '\*Certificate Key:' with a 'Browse' button. At the bottom are 'Previous' and 'Next' buttons.

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.

This screenshot shows the same 'Enroll Certificate Key' screen as before, but with a modal dialog box titled 'Enter Password' overlaid. The dialog contains a warning icon and the text: 'Detected that the private key is encrypted with a password, please enter the password.' Below the text is a 'private key password' input field with a 'Browse' button. At the bottom of the dialog are 'Cancel' and 'Confirm' buttons. The background wizard interface is partially visible behind the dialog.

### 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.

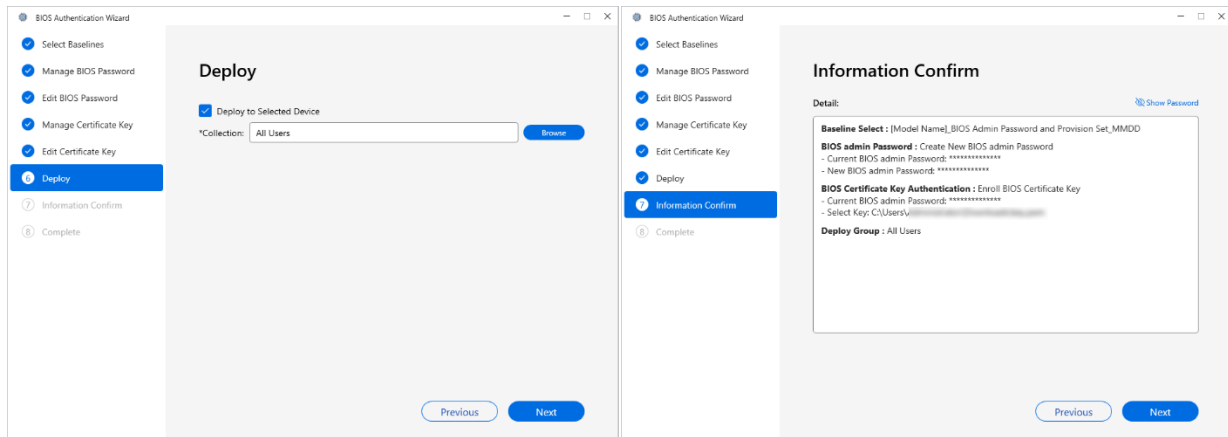
The screenshot shows the 'BIOS Authentication Wizard' window. On the left, a sidebar lists the steps: 1. Select Baselines, 2. Manage BIOS Password, 3. Edit BIOS Password, 4. Manage Certificate Key, 5. Edit Certificate Key (highlighted), 6. Deploy, 7. Information Confirm, and 8. Complete. The main area is titled 'Update Certificate Key'. It contains two input fields: '\*BIOS admin Password:' with a masked password '\*\*\*\*\*' and a 'Show/Hide' icon, and '\*Certificate Key:' with a '1' icon, an 'Input Certificate Key' field, and a 'Browse' button. At the bottom right are 'Previous' and 'Next' buttons.

### 3.3 Revoke Certificate

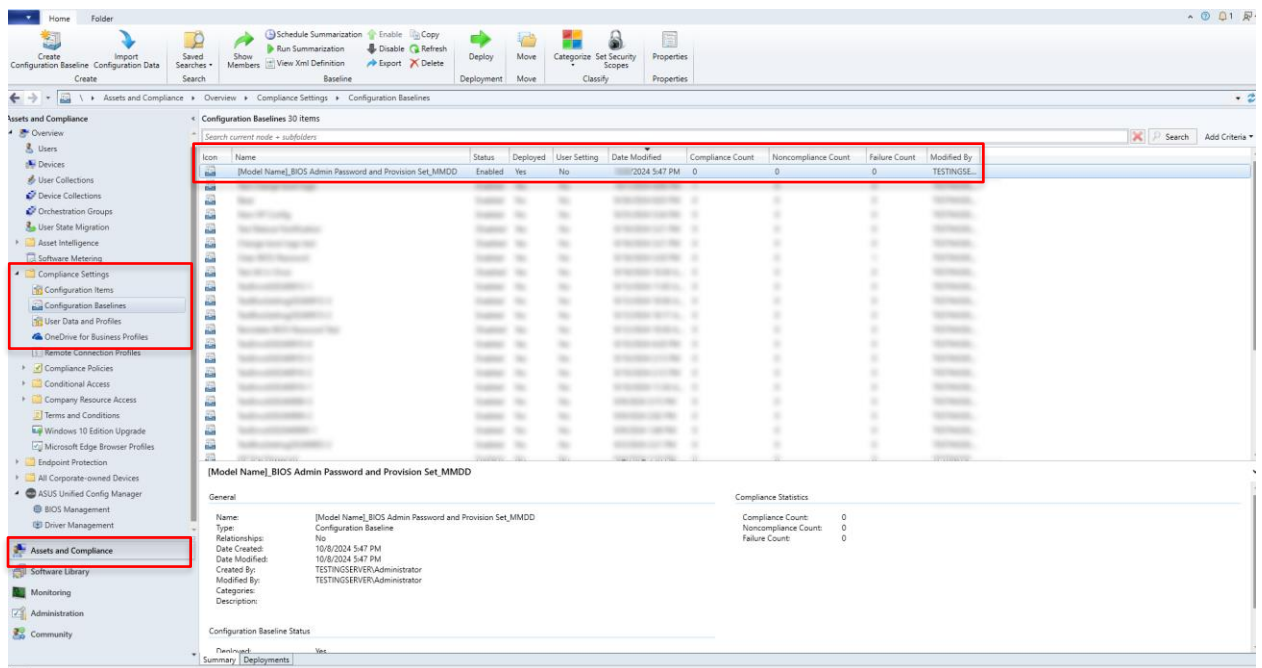
To revoke the certificate key, the BIOS admin password used for enrollment is required.

The screenshot shows the 'BIOS Authentication Wizard' window. On the left, a sidebar lists the steps: 1. Select Baselines, 2. Manage BIOS Password, 3. Edit BIOS Password, 4. Manage Certificate Key, 5. Edit Certificate Key (highlighted), 6. Deploy, 7. Information Confirm, and 8. Complete. The main area is titled 'Revoke Certificate Key'. It contains one input field: '\*BIOS admin Password:' with a masked password '\*\*\*\*\*' and a 'Show/Hide' icon. At the bottom right are 'Previous' and 'Next' buttons.

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.

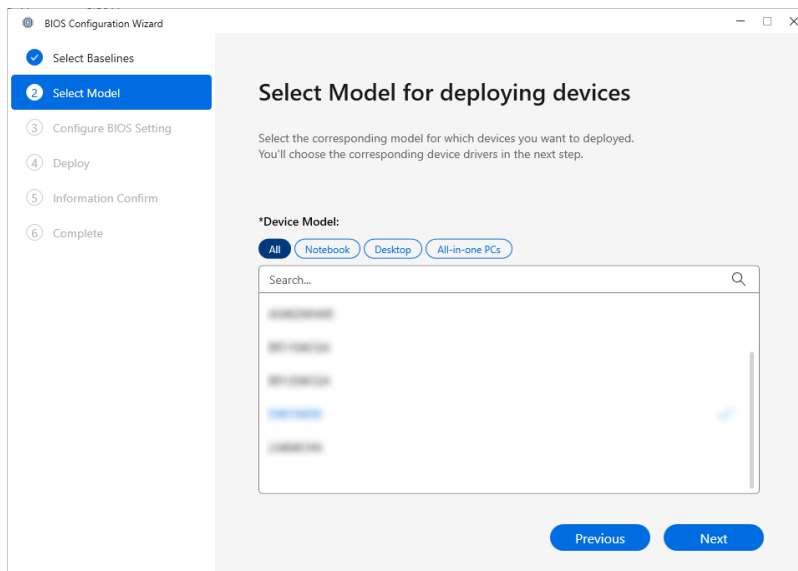
This authorization mechanism ensures that only properly authorized users can modify BIOS settings, enhancing the overall security of the device.

Supported Client Platforms:

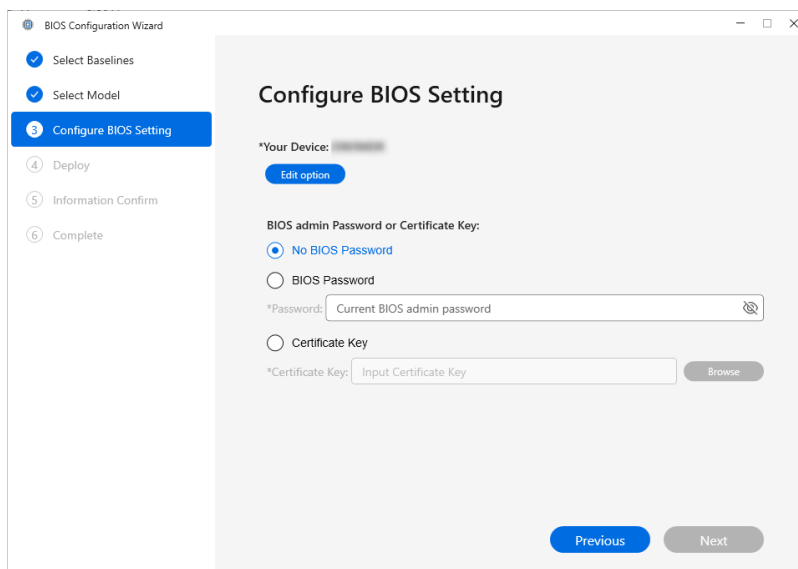
- ASUS Commercial Products (2024 or later)
1. Create a new baseline or choose a current baseline (for future new devices following).

The screenshot shows the 'BIOS Configuration Wizard' window. On the left is a vertical sidebar with six steps: 1. Select Baselines (highlighted in blue), 2. Select Model, 3. Configure BIOS Setting, 4. Deploy, 5. Information Confirm, and 6. Complete. The main area is titled 'Select Baseline' and contains the instruction: 'Create a new baseline or select one from the exist baselines to manage the BIOS certification for the deployed devices'. There are two radio button options: 'Create New Baseline' (which is selected) and 'Select Current Baseline'. Under 'Create New Baseline', there is a text field labeled '\*Name:' with the placeholder text '[Model Name]\_BIOS Config Baseline\_MMDD'. Under 'Select Current Baseline', there is a text field labeled '\*Name:' with a search icon and a dropdown list showing several baseline names. A blue 'Next' button is located at the bottom right of the main area.

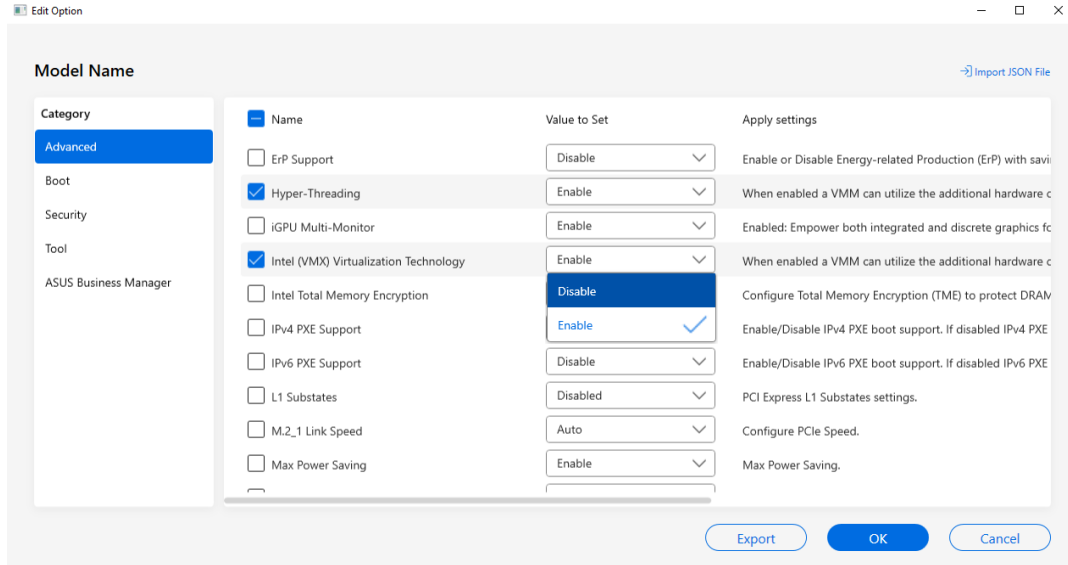
2. Select a model as the reference for the configuration items, and prepare it for deployment.



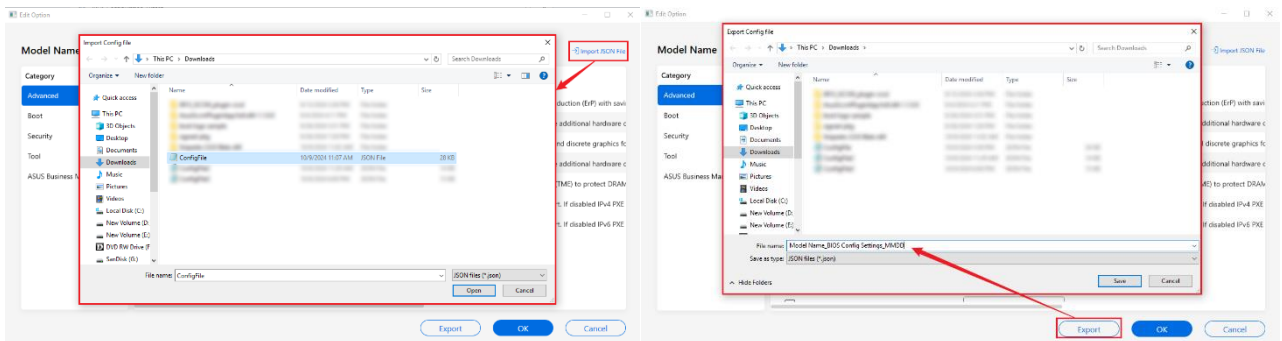
3. Edit the BIOS Configuration Settings: Click "Edit Option" to change the setting with user interface, and remember to provide BIOS admin password or certificate key as the authentication verification.



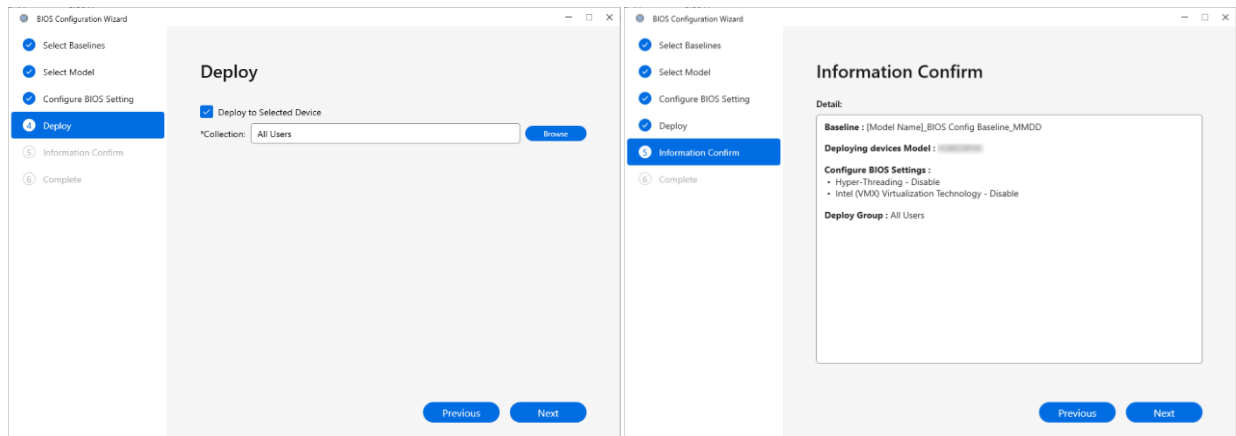
Ensure to tick the checkbox of any options that have been modified



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

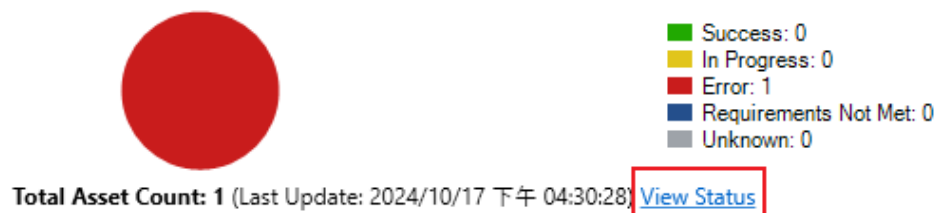
Click on the pie chart, then select View Status > Error > (Choose 1 failed device) > More Details to check the reasons for each device's failure.

The screenshot shows the 'Deployment Status' window. On the left is a navigation pane with 'Deployments' selected. The main area displays a table with columns: Deployment ID, Assets, Message ID, Status Type, and Description. One row is visible with Deployment ID 'CSW20001', Assets '1', Message ID '11170', and Status Type 'Error'. Below the table is an 'Asset Details' section with a table showing details for device 'B1402CGA-H13020', including User 'Net Applicable', Message ID '11170', Status Type 'Error', and Description 'The task sequence manager could not...'. A red circle highlights the 'Error' status in the top summary bar, and a red box highlights the 'More Details' link in the Asset Details section.

Deployment ID	Assets	Message ID	Status Type	Description
CSW20001	1	11170	Error	

Device	User	Message ID	Status Type	Description
B1402CGA-H13020	Net Applicable	11170	Error	The task sequence manager could not...

#### Completion Statistics



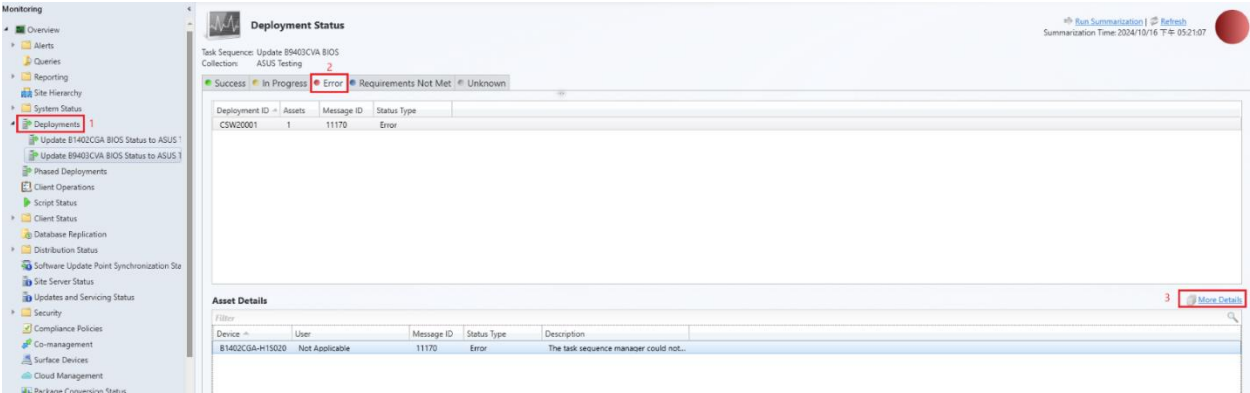
The error code can be obtained from the Exit Code of the "Install Package" step in Status. Please refer to the error code from Microsoft.

<https://learn.microsoft.com/en-us/windows-hardware/drivers/devtest/pnputil-return-values>

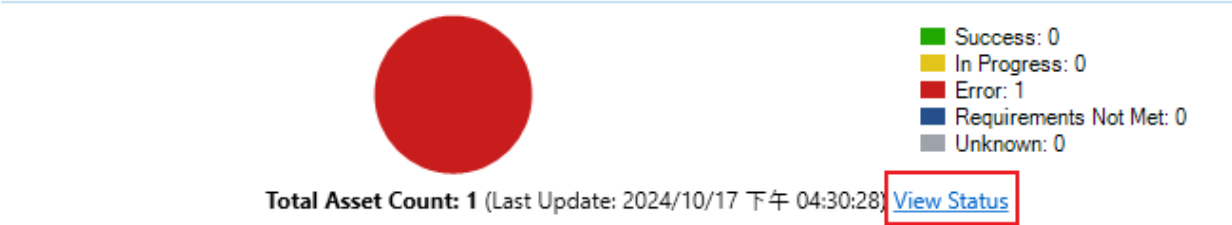


# Error Status of BIOS Updater

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.



## Completion Statistics



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.

Asset Message							
Details		Status					
Execution Time	Step	Action Name	Group Name	Last Message Name	Last Message ID	Exit Code	Action Output
2024/10/17 上午 10:00	0			The task sequence execution engine st...	11140	0	
2024/10/17 上午 10:00	0	Disable Client Log Collection		The task sequence execution engine s...	11134	0	Finished with...
2024/10/17 上午 10:00	1	Start ACT Log Collection		The task sequence execution engine s...	11134	0	=====...
2024/10/17 上午 10:00	2	Copy Files		The task sequence execution engine s...	11134	0	=====...
2024/10/17 上午 10:00	3	Update Bios		The task sequence execution engine f...	11135	12	=====...
2024/10/17 上午 10:00	3	Update Bios		The task sequence execution engine l...	11138	0	
2024/10/17 上午 10:00	4	Delete Files		The task sequence execution engine s...	11134	0	=====...
2024/10/17 上午 10:00	5	Exit with fault		The task sequence execution engine f...	11135	1	=====...
2024/10/17 上午 10:00	5	Exit with fault		The task sequence execution engine a...	11139	16,388	
2024/10/17 上午 10:00	5			The task sequence execution engine f...	11141	1	

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 screenshot displays the 'Deployment Status' window. At the top, it shows 'Baseline: wrongPWenroll' and 'Collection: Ha0923Test'. Below this, there are tabs for 'Compliant', 'Error', 'Non-Compliant' (selected), and 'Unknown'. A table lists deployment items, with one item in a 'Warning' state and 'Non-Compliant' status. An 'Asset Message' dialog box is open, showing details for a device named 'LAPTOP-15NVE7...'. The dialog has a 'General' tab and a 'Non-Compliant' status. It lists the device name, user name, and the specific error: 'Set BIOS enroll key failed: 8'. The number '8' is highlighted with a red box. At the bottom of the dialog, there is a 'Close' button. On the right side of the main window, there is a 'More Details' link, also highlighted with a red box.

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://dlcdncls.asus.com/data/acm/ASUS\\_Config\\_Manager\\_Supported\\_Models.pdf](https://dlcdncls.asus.com/data/acm/ASUS_Config_Manager_Supported_Models.pdf)

	Commercial Models	Limitation
<b>Driver Package, Driver Updater</b>	Y2020 and newer	
<b>BIOS Update</b>	Y2020 and newer	Y2024 and later supported for update with password set
<b>BIOS Authentication, BIOS Configuration</b>	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).