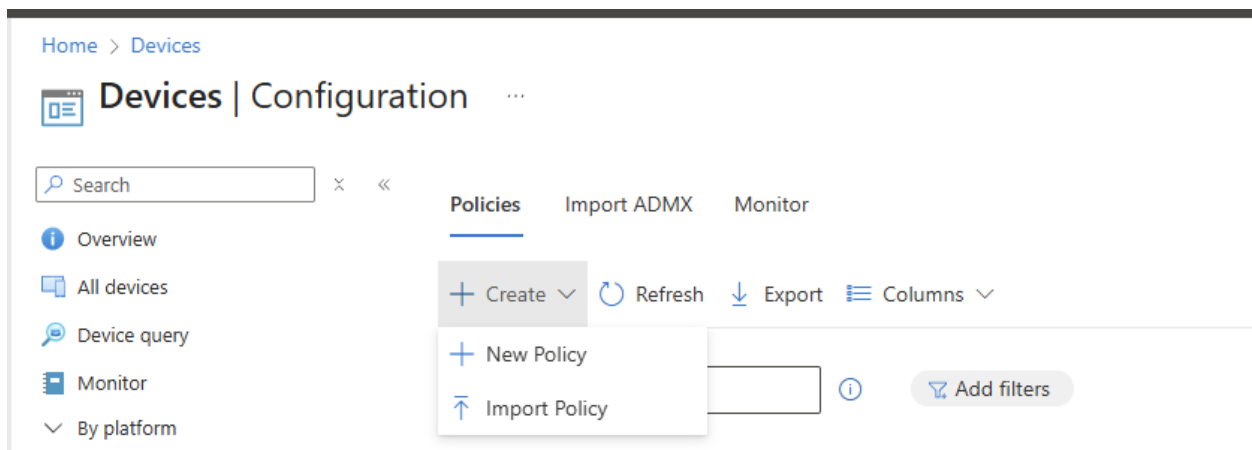


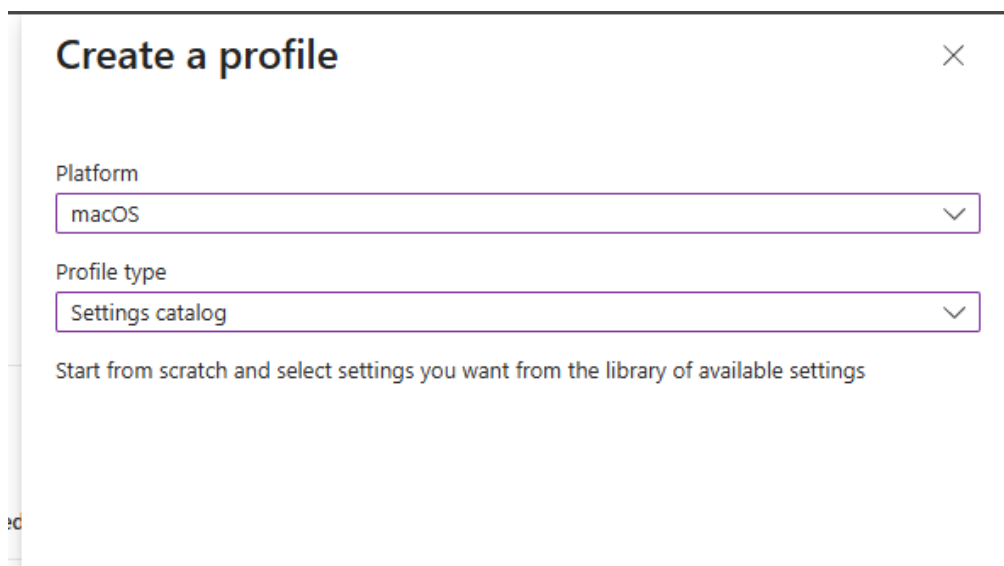
Please read entire document before starting the upgrade process. There are helpful tips and points at the end.

Section 1: Deploying the Tamper Protection Exclusion configuration profile

- 1) As an Intune administrator, log into **endpoint.microsoft.com**
- 2) Navigate to **Devices > Configuration** > Select **+ Create** > Select **+ New Policy**



- 3) In the Create a profile blade, select **macOS** under **Platform** and select **Settings catalog** under **Profile Type** then select **Create** on the bottom



- 4) Name your new profile so it's easy to distinguish, add a description, and click **Next** on the bottom
 - a. Name: TP Exclusion for com.microsoft.wdav.upgrade
 - b. Description: Exclusion for com.microsoft.wdav.upgrade

[Home](#) > [Devices | Configuration](#) >

Create profile

macOS - Settings catalog

1 Basics 2 Configuration settings 3 Scope tags 4 Assignments 5 Review + create

Name *

TP Exclusion for com.microsoft.wdav.upgrade

Description

Exclusion for com.microsoft.wdav.upgrade

Platform

macOS

Previous

Next

- 5) Under the **Configuration settings** tab, click **+Add Settings(1)**, select **Microsoft Defender(2)** from the settings picker on the right, in the drop down select **Tamper Protection(3)**, select **Signing Identifier(4)** and **Process Team Identifier(5)**

[Home](#) > [Devices | Configuration](#) >

Create profile

macOS - Settings catalog

1 Basics 2 Configuration settings 3 Scope tags 4 Assignments 5 Review + create

+ Add settings 1

Microsoft Defender Remove category

Tamper protection Remove subcategory

2 of 6 settings in this subcategory are not configured

Process exclusions

Process path	Process's arguments	Process's Signing Identifier	Process's TeamIdentifier	Cor
Not configured	Not configured	Not configured	Not configured	Ed

Settings picker

Use commas "," among search terms to lookup settings by their keywords

Search for a setting

Browse by category

- Microsoft Autologon (Mach)
- Microsoft Defender 2
 - Antivirus engine
 - Cloud delivered protection preferences
 - Endpoint Detection and Response (EDR) preferences
 - Features
 - Network protection
 - Tamper protection 3
 - User interface preferences
 - Microsoft Edge
 - Microsoft Office
 - Networking
 - Recent Products

6 settings in "Tamper protection" subcategory

Select all these settings

Setting name	
Enforcement level	
Process exclusions	
Process exclusions <ul style="list-style-type: none">Process pathProcess's argumentsProcess's Signing Identifier 4Process's TeamIdentifier 5	

- 6) Under the settings that were created, use the horizontal scroll bar to scroll to the right and **edit the instance(1)** which will open a blade on the right with the **process TeamIdentifier** and the **process Signing Identifier**. Fill in with values below and save:

a. Process's TeamIdentifier: UBF8T346G9

b. Process's Signing Identifier: com.microsoft.wdav.upgradehelper

The screenshot displays the Microsoft Defender configuration interface. On the left, the 'Create profile' blade is active, showing the 'Configuration settings' tab. Under 'Microsoft Defender', the 'Tamper protection' subcategory is expanded, indicating that 2 of 6 settings are not configured. Below this, the 'Process exclusions' section shows a table with columns for 'Process's arguments', 'Process's Signing Identifier', and 'Process's TeamIdentifier', all marked as 'Not configured'. A red circle labeled '1' highlights the '+ Edit instance' button. On the right, the 'Configure instance' blade is open, showing the 'Tamper protection' subcategory. It contains two input fields: 'Process's TeamIdentifier' with the value 'UBF8T346G9' (marked with a red circle labeled '2') and 'Process's Signing Identifier' with the value 'com.microsoft.wdav.upgradehelper' (marked with a red circle labeled '3'). Both fields have a checkmark icon to their right.

- 7) Skip the **scope tags** tab by clicking **next** on the bottom

- 8) Under the **assignments tab**, click **Add Groups**(1) under the **Included groups** section and **select the group**(2) which contains your macOS devices then click **select**(3) and click next at the bottom. **Please note that Microsoft recommends testing this on a set of devices before deploying to the entire fleet of macOS devices**

Home > Devices | Configuration >
Create profile ...
macOS - Settings catalog

Basics Configuration settings Scope tags **Assignments** Review + create

Included groups

1 Add groups Add all users Add all devices

Groups Group Members Filter Filter mode Edit filter

No groups selected

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more about excluding groups.](#)

+ Add groups

Groups Group Members Remove

No groups selected

Select groups to include
Azure AD Groups

Try changing or adding filters if you don't see what

Search
macos
2 results found

All Groups

Name

☐ macOS - Users

☒ macOS - Devices 2

Previous Next 4

Select 3

- 9) On **Review + create** tab, review your settings and click **create** at the bottom.

Section 2: Deploying the package to upgrade to 25072 with Intune

- 1) Obtain the upgrade helper package by downloading it from this public Microsoft CDN link:
https://officecdn-microsoft-com.akamaized.net/pr/C1297A47-86C4-4C1F-97FA-950631F94777/MacAutoupdate/upgrade_from_25062_helper.pkg
- 2) As an Intune administrator, log into **endpoint.microsoft.com**

- 3) Navigate to **Apps**(1) > **All Apps**(2) > click **+ Create**(3) > in the blade on the right, **scroll down** and select **macOS app (PKG)**(4), and click select on the bottom

The screenshot shows the Microsoft Intune 'All Apps' page. On the left, the 'Apps' menu item is highlighted with a red circle (1). The 'All Apps' tab is selected with a red circle (2). The '+ Create' button is highlighted with a red circle (3). On the right, the 'Select app type' dialog is open, showing a list of app types. 'macOS app (PKG)' is highlighted with a red circle (4).

Name	Platform	Type	Version	VPP token name	Assigned	Developer
ApowerMirror- Screen Mirroring	iOS	iOS store app			Yes	
ApowerMirror- Screen Mirroring	Android	Managed Google Play st...			Yes	
Intune Company Portal	Android	Managed Google Play st...			No	
Managed Home Screen	Android	Managed Google Play st...			No	
Microsoft Authenticator	iOS	iOS store app			Yes	
Microsoft Authenticator	Android	Managed Google Play st...			No	
Microsoft Defender: Antivirus	Android	Managed Google Play st...			Yes	
Microsoft Defender: Security	iOS	iOS store app			Yes	
Microsoft Edge: AI browser	Android	Managed Google Play st...			Yes	
Microsoft Intune	Android	Managed Google Play st...			No	
Microsoft Launcher	Android	Managed Google Play st...			No	
Microsoft Outlook	iOS	iOS store app			Yes	
Microsoft Teams	iOS	iOS store app			Yes	
Windows App	Android	Managed Google Play st...			Yes	

- 4) Upload the package that was obtained from section 2, step 1 by clicking **Select app package file**(1), click the **Folder icon**(2), and add the package, then select **Ok** on the bottom

The screenshot shows the 'Add App' wizard in Microsoft Intune. The 'App information' step is selected, and the 'Select app package file' button is highlighted with a red circle (1). On the right, the 'App package file' dialog is open, showing a text box for the file path and a folder icon button highlighted with a red circle (2).

- 5) Once the package is added, fill in the **Publisher** field with **Microsoft** and click next on the bottom

Home > Apps | All Apps >

Add App

macOS app (PKG)

1 App information 2 Program 3 Requirements 4 Detection rules 5 Assignments 6 Review + create

Select file * ⓘ upgrade_from_25062_helper.pkg

Name * ⓘ upgrade_from_25062_helper.pkg

Description * ⓘ upgrade_from_25062_helper.pkg

Publisher * ⓘ Microsoft

Category ⓘ 0 selected

Information URL ⓘ Enter a valid url

Privacy URL ⓘ Enter a valid url

Developer ⓘ

Owner ⓘ

Notes ⓘ

Logo ⓘ Select image

- 6) Under the **Program** tab simply click **Next** on the bottom.
- 7) Under the **Requirements** tab, specify the minimum operation system version for this script and click next.
- 8) Under the **Detection Rules** tab, simply click **Next** on the bottom and do not alter any fields
- 9) Under the **Assignments** tab, select **+Add Group**(1) under the Required section and **specify the group**(2) containing your macOS devices, then click **select**(3), and **Next**(4)

Home > Apps | All Apps >

Add App

macOS app (PKG)

✓ App information ✓ Program ✓ Requirements ✓ Detection rules **5** Assignments 6 Review + create

ⓘ Any macOS app deployed using Intune agent will not automatically be removed from the device when the device is retired. The app and data it contains will remain on the device. If the

Required ⓘ

Group mode Group

No assignments

+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ

1

Available for enrolled devices ⓘ

Group mode Group

No assignments

+ Add group ⓘ + Add all users ⓘ

Previous **Next** **4**

Select groups

Microsoft Entra groups

Try changing or adding filters if you don't

Search

macos

2 results found

All **Groups**

	Name
<input type="checkbox"/>	macOS - Users
<input checked="" type="checkbox"/>	macOS - Devices 2

Select **3**

10) Under the **Review + Create** tab, review your settings then click **Create**.

More info and key points

- **Note:** If admins have an existing configuration profile it can be edited to add the TP exclusion there or a separate configuration profile can be deployed for the test devices.
- **Note 2:** Microsoft always recommends testing on a smaller sample before deploying to production
- Section 1 involves a configuration profile deployment where we utilize a configuration profile to provide a TP exclusion for our helper agent
- Section 2 utilizes a separate Microsoft signed package to manually upgrade the platform.

- TP will be set to audit and then reverted back to block for the time the custom package is ran
- Ensure there are no white spaces before and after your TeamIdentifier and Signing Process Identifier values
- How do I know if the exclusions are applied on a device from my profile?
 - Open a terminal and run **mdatp health --details tamper_protection** then look for the TeamIdentifier and Signing Process Identifier values in the second line
 - **The exclusions line needs to be exactly the same as below output or the configuration will not work:**

```
dkadmin@Doykos-MacBook-Pro ~ % mdatp health --details tamper_protection
tamper_protection      : "block" [managed]
exclusions              : [{"path":null,"team_id":"UBF8T346G9","signing_id":"com.microsoft.wdav.upgradehelper","args":null}] [managed]
feature_enabled_protection : true
feature_enabled_portal  : true
configuration_source    : "mdm"
configuration_local     : "block"
configuration_portal    : "block"
configuration_default   : "audit"
configuration_is_managed : true
dkadmin@Doykos-MacBook-Pro ~ %
```

- How can I easily check if I am updated and TP is still set to block?
 - Open a terminal and run **mdatp health | egrep "app_version|tamper_protection"**
- **Once all of your fleet is upgraded you can remove the Tamper Protection exclusions from your devices by removing the configuration profile**