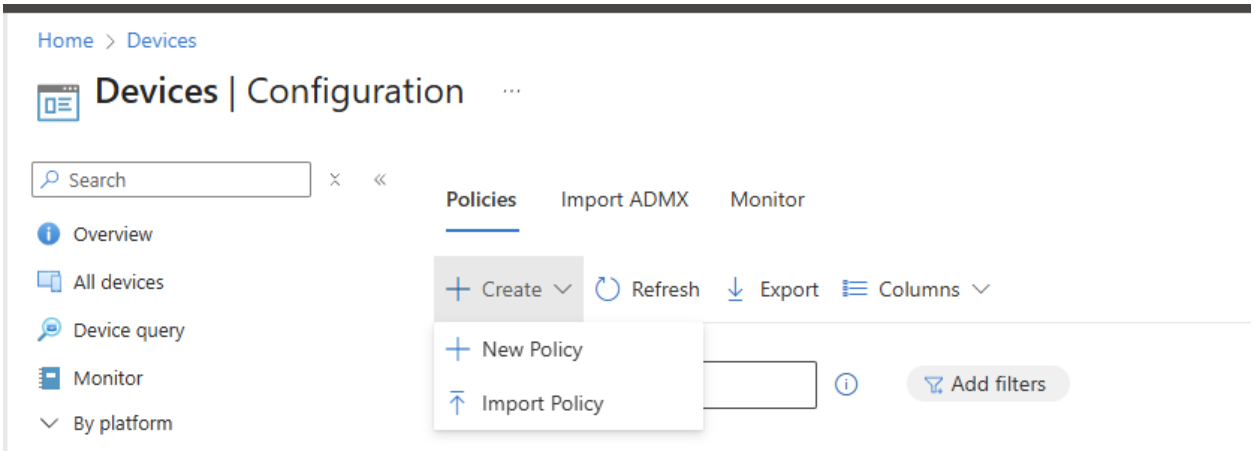
MacOS Upgrade 25072 Helper – Intune Deployment

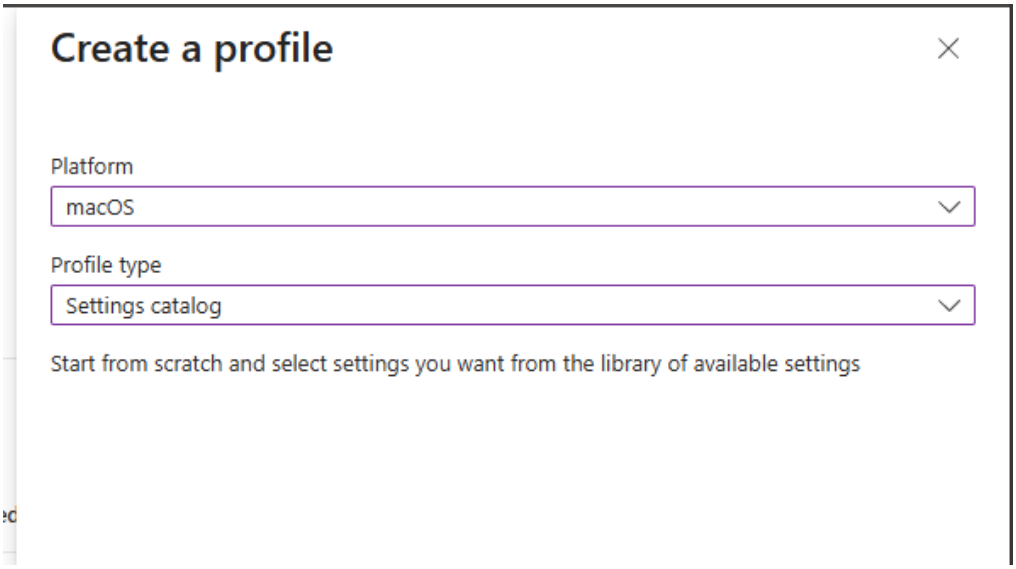
Please read entire document before starting the upgrade process. There are helpful tips and points at the end.

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**

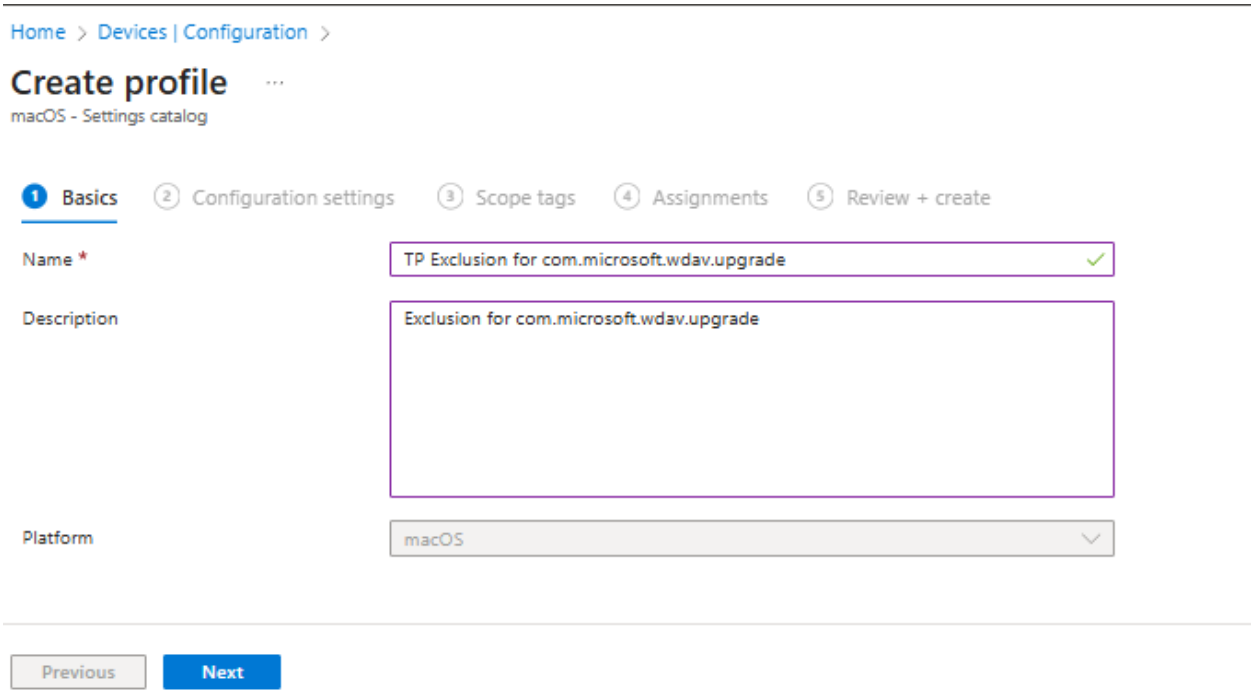


3) In the Create a profile blade, select **macOS** under **Platform** and select **Settings catalog** under **Profile Type** then select **Create** on the bottom

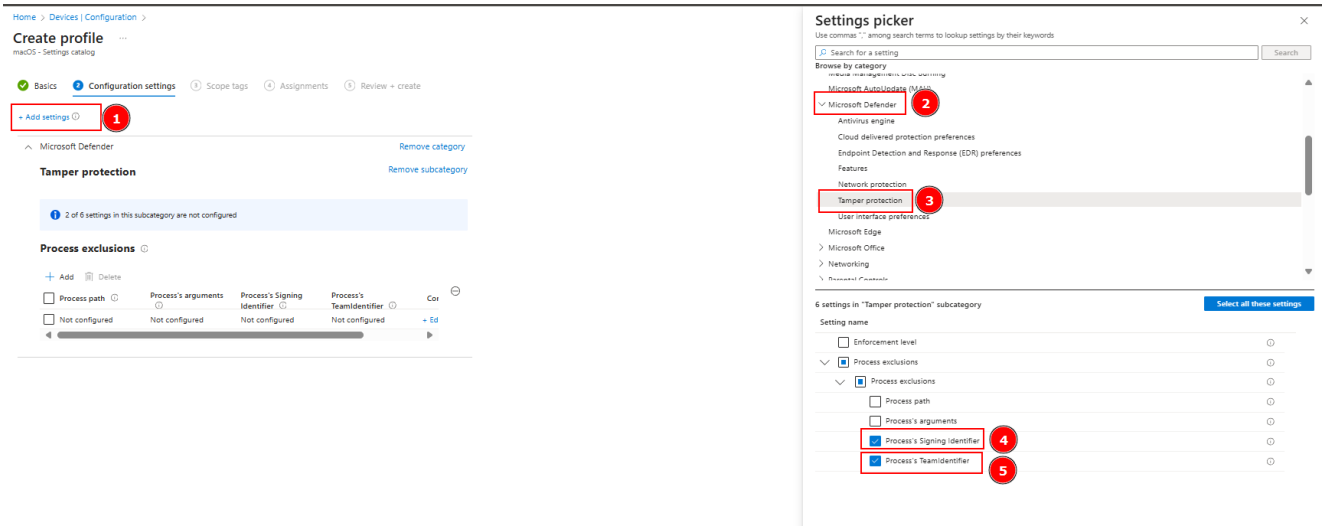


4) Name your new profile so it's easy to distinguish, add a description, and click **Next** on the bottom

   a. Name: TP Exclusion com.microsoft.wdav.upgrade
   b. Description: Exclusion for com.microsoft.wdav.upgrade



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)

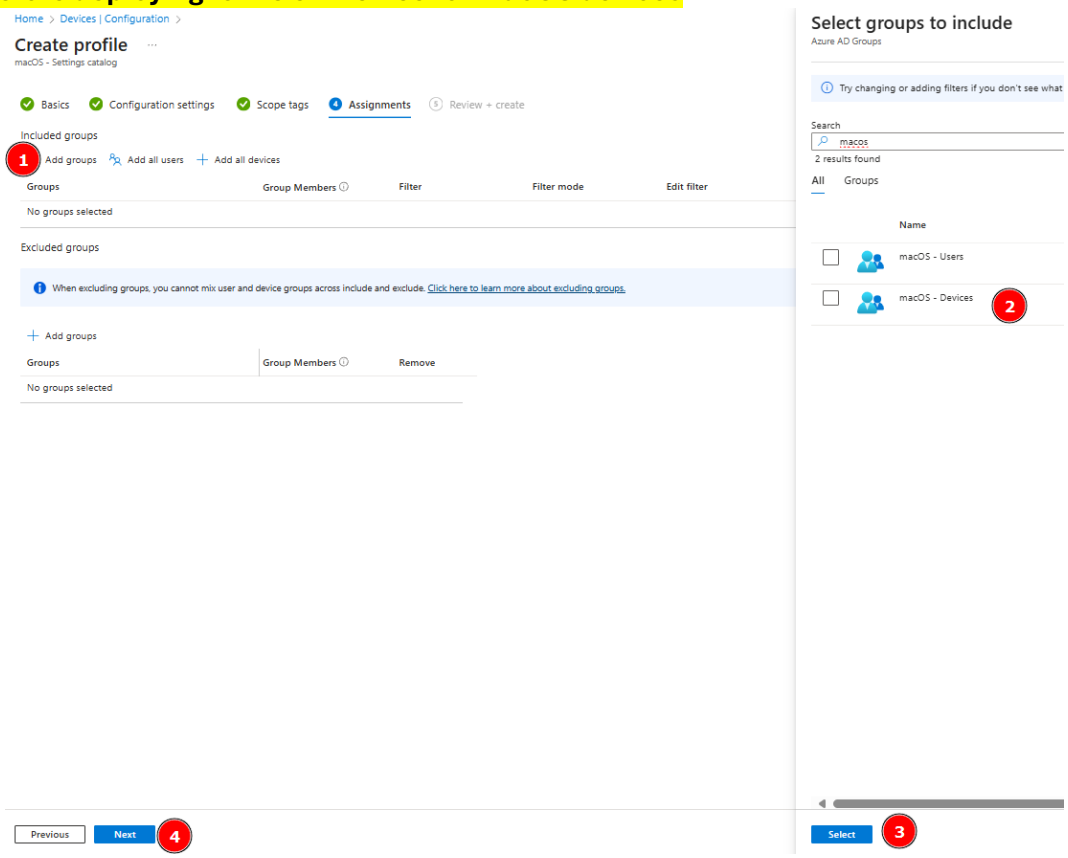


6) Under the settings that were created, use the horizontal scroll bar to scroll to the right and **edit the instance**(1) which will open a blade on the right with the **process TeamIdentifier** and the **process Signing Identifier**. Fill in with values below and save:

   a. **Process's TeamIdentifier: UBF8T346G9**
   b. **Process's Signing Identifier: com.microsoft.wdav.upgradehelper**

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**



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

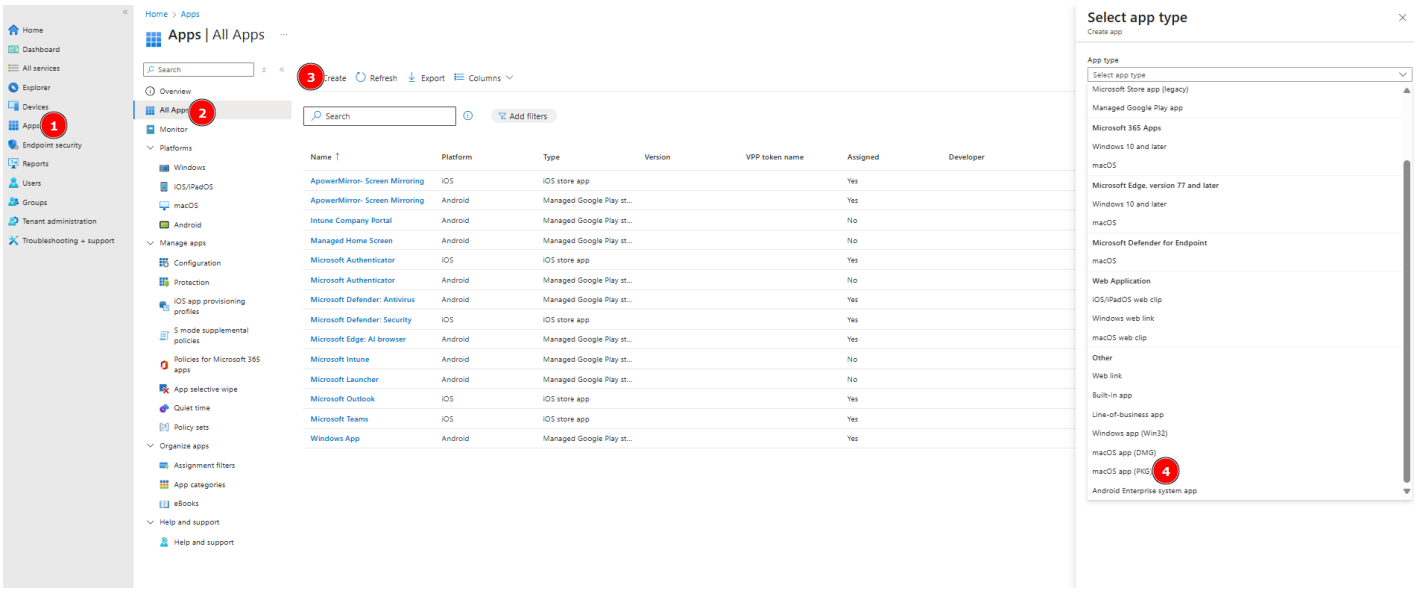
Section 2: Deploying the package to upgrade to 25072 with Intune

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

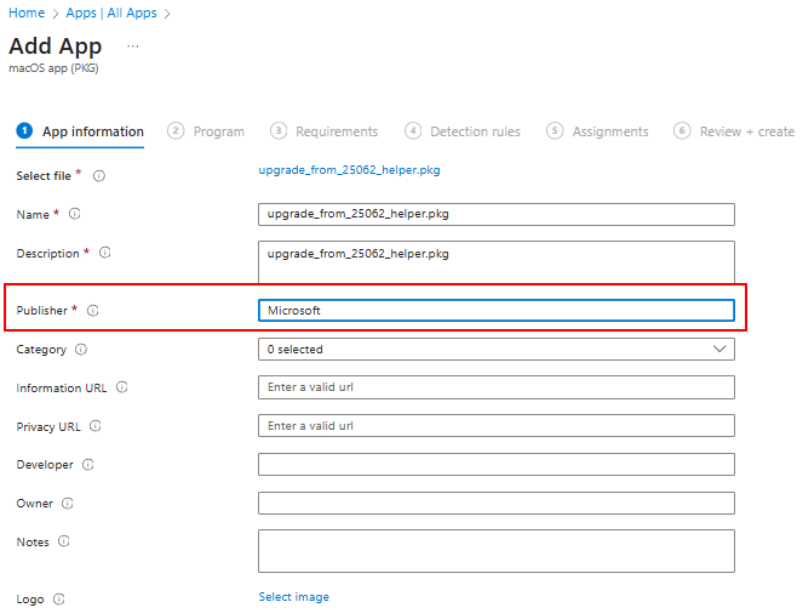
2) As an Intune administrator, log into **endpoint.microsoft.com**

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



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

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

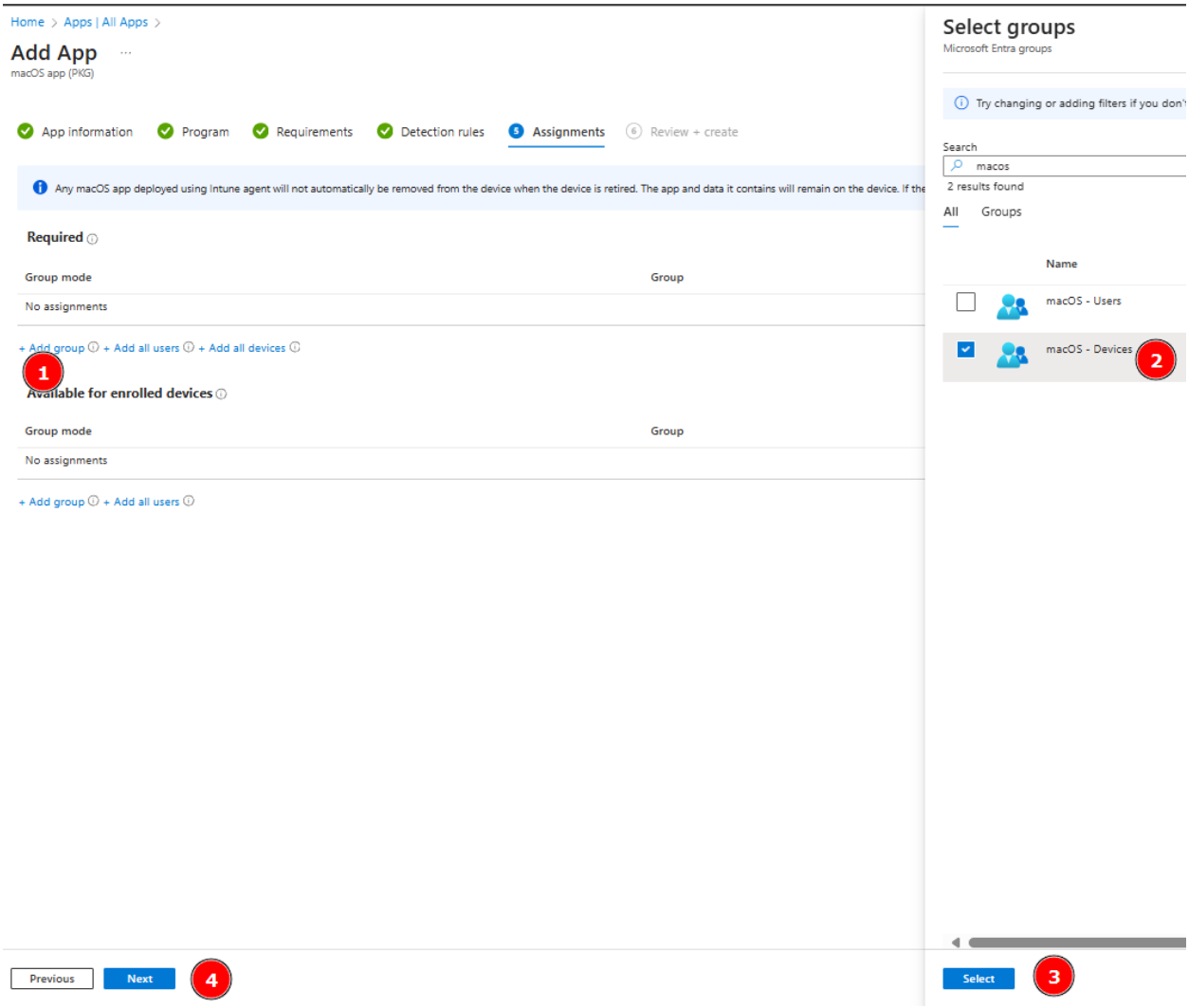


6) Under the **Program** tab simply click **Next** on the bottom.

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)

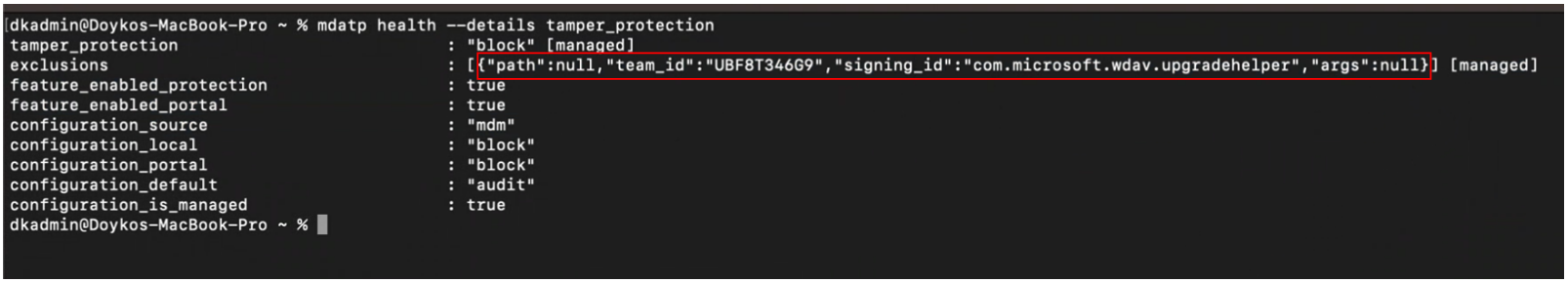


10) Under the **Review + Create** tab, review your settings then click **Create**.

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 TeamIdentifer 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:**



- 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**