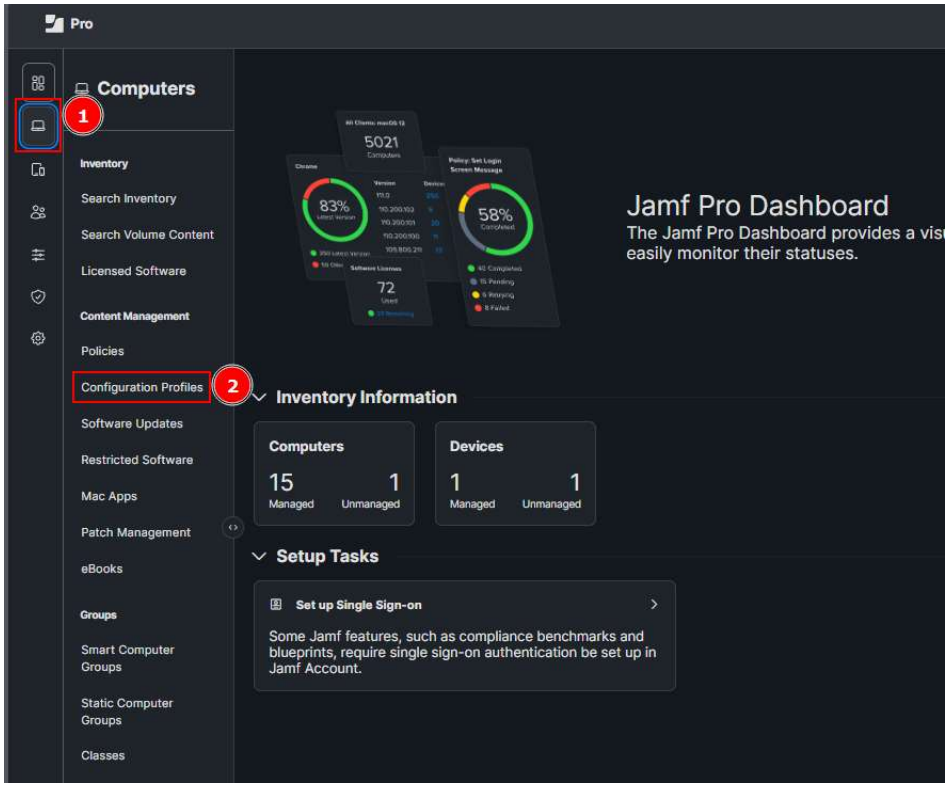
MacOS 25072 Upgrade Helper – JAMF Deployment

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

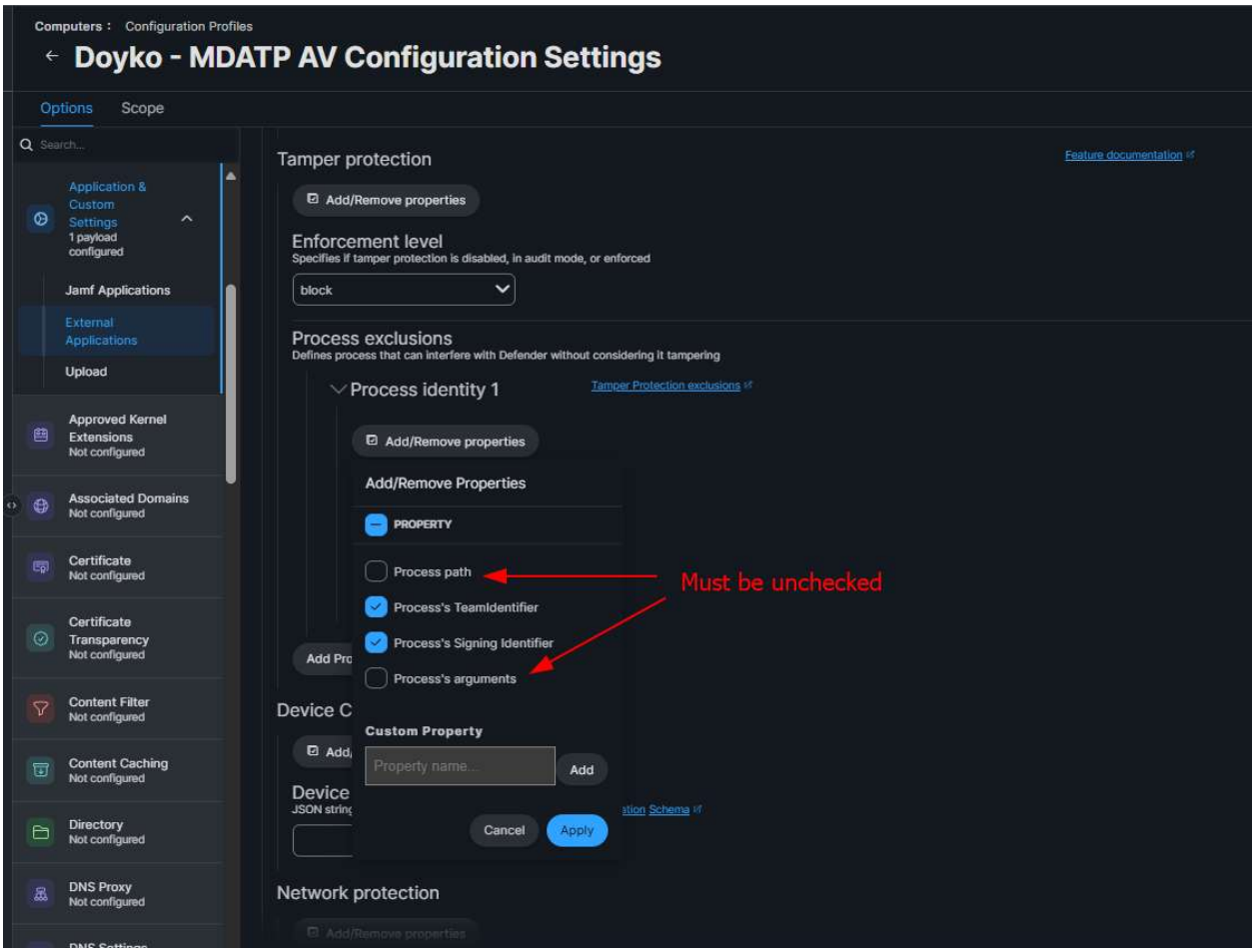
1) Log into JAMF as an administrator
2) From your home page, click on **computers**(1) > **Configuration Profiles**(2)

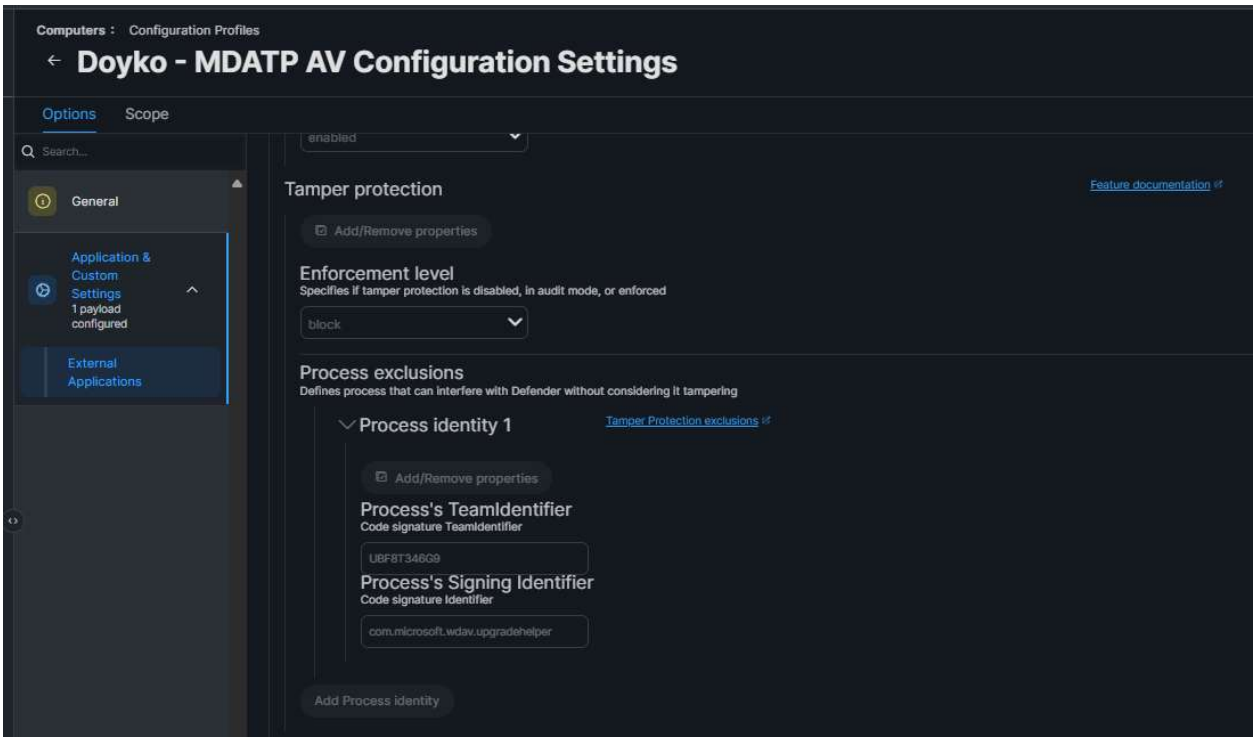


3) On the configuration profile page, **JAMF administrators will need to locate the configuration profile responsible for deploying MDE AV settings on their macOS machine.** If using the Form Editor, administrators need to add the Process Exclusions property under Tamper Protections and add the two values as seen below.

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

You MUST ensure that ONLY Process's TeamIdentifier and Process's Signing Identifer are un-checked or your exclusion will not be honored. Review the two images below for correct configuration


Computers : Configuration Profiles
Doyko - MDATP AV Configuration Settings
Options
Scope
Search...
Application & Custom Settings
1 payload configured
Jamf Applications
External Applications
Upload
Approved Kernel Extensions
Not configured
Associated Domains
Not configured
Certificate
Not configured
Certificate Transparency
Not configured
Content Filter
Not configured
Content Caching
Not configured
Directory
Not configured
DNS Proxy
Not configured
Tamper protection
Feature documentation
Add/Remove properties
Enforcement level
Specifies if tamper protection is disabled, in audit mode, or enforced
block
Process exclusions
Defines process that can interfere with Defender without considering it tampering
Process identity 1
Tamper Protection exclusions
Add/Remove properties
Add/Remove Properties
PROPERTY
Process path
Process's TeamIdentifier
Process's Signing Identifier
Process's arguments
Must be unchecked
Custom Property
Property name...
Add
Cancel
Apply
Network protection


Computers : Configuration Profiles
Doyko - MDATP AV Configuration Settings
Options
Scope
Search...
General
Application & Custom Settings
1 payload configured
External Applications
enabled
Tamper protection
Feature documentation
Add/Remove properties
Enforcement level
Specifies if tamper protection is disabled, in audit mode, or enforced
block
Process exclusions
Defines process that can interfere with Defender without considering it tampering
Process identity 1
Tamper Protection exclusions
Add/Remove properties
Process's TeamIdentifier
Code signature TeamIdentifier
UBF8T346G9
Process's Signing Identifier
Code signature Identifier
com.microsoft.wdav.upgradehelper
Add Process identity

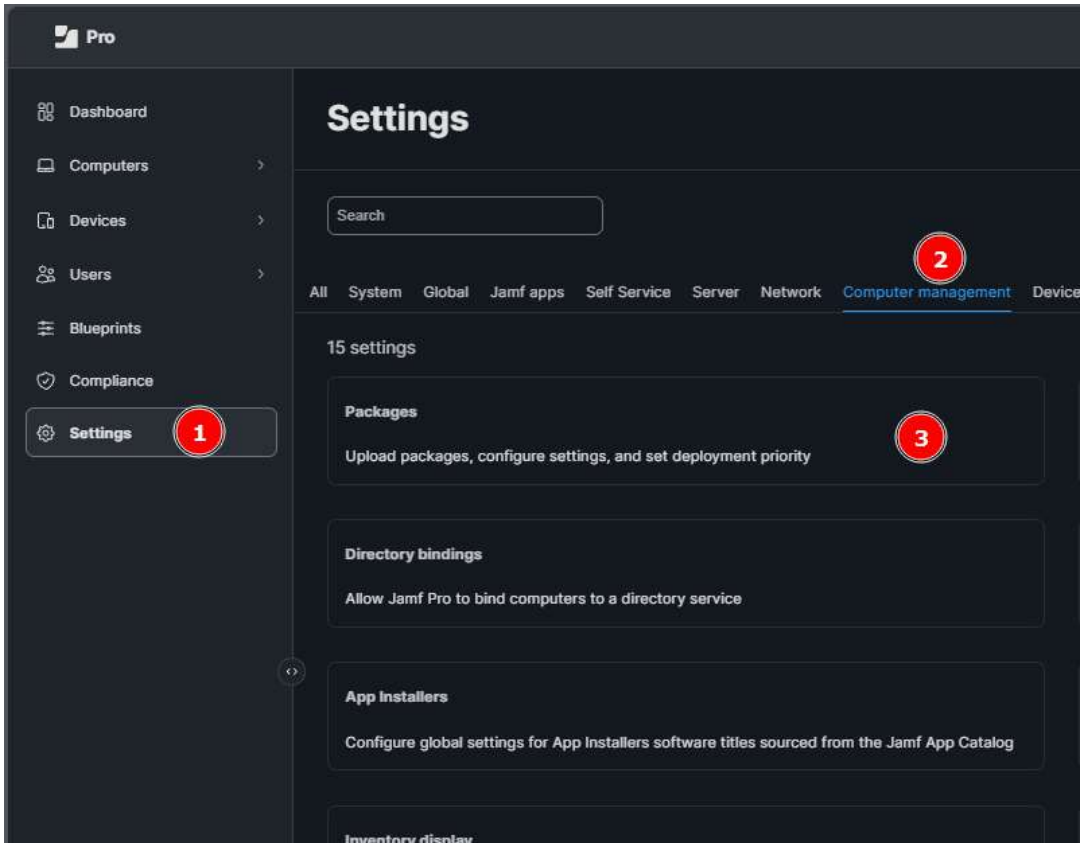
If using a specific PLIST to deploy settings then JAMF administrators need to add the following string:

```
<key>tamperProtection</key>
  <dict>
   <key>enforcementLevel</key>
   <string>block</string>
   <key>exclusions</key>
   <array>
    <dict>
     <key>teamId</key>
     <string>UBF8T346G9</string>
     <key>signingId</key>
     <string>com.microsoft.wdav.upgradehelper</string>
    </dict>
   </array>
  </dict>
```

Once the changes are made, save the configuration profile and re-deploy to your machines. **Microsoft recommends to always test on a smaller sample before deploying to production.** In cases where a smaller sample is used, exclude a few machines from the main policy and create a new configuration profile that will be deployed to the sample. The excluded machines should be included in the new policy.

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

1) Log into your JAMF environment as an admin and navigate to **Settings**(1), **Computer management**(2), then **packages**(3)

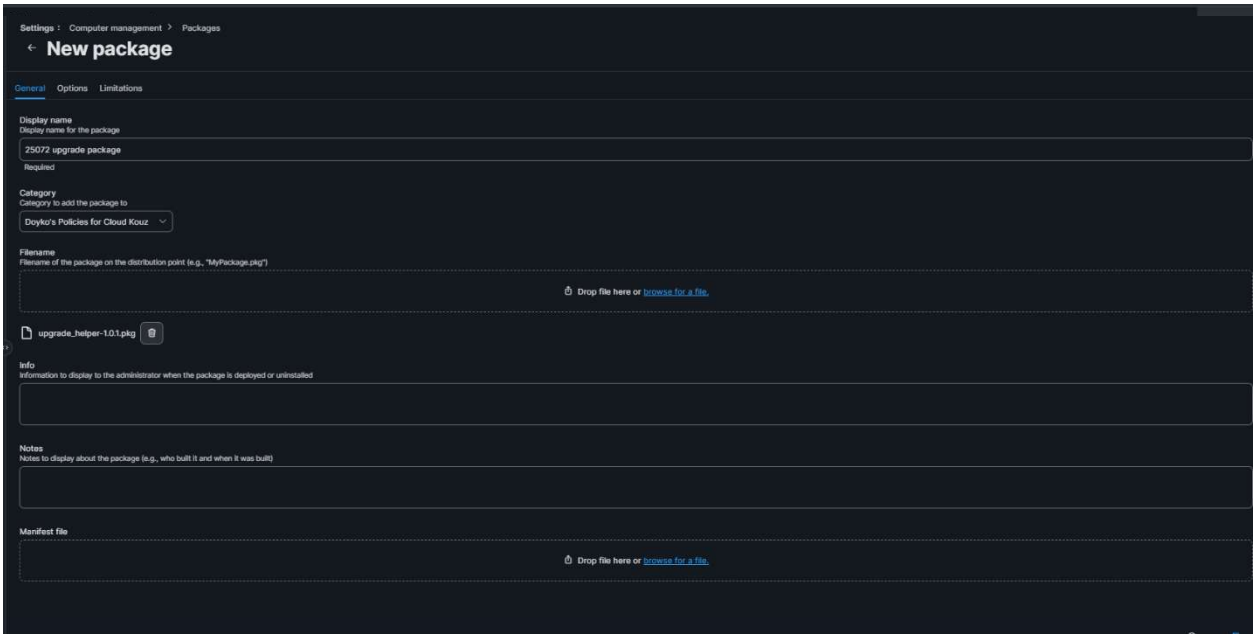


2) In **packages**, select **+New**(1) and specify the following in the fields and save. After this step is completed the package will be uploaded to JAMF.

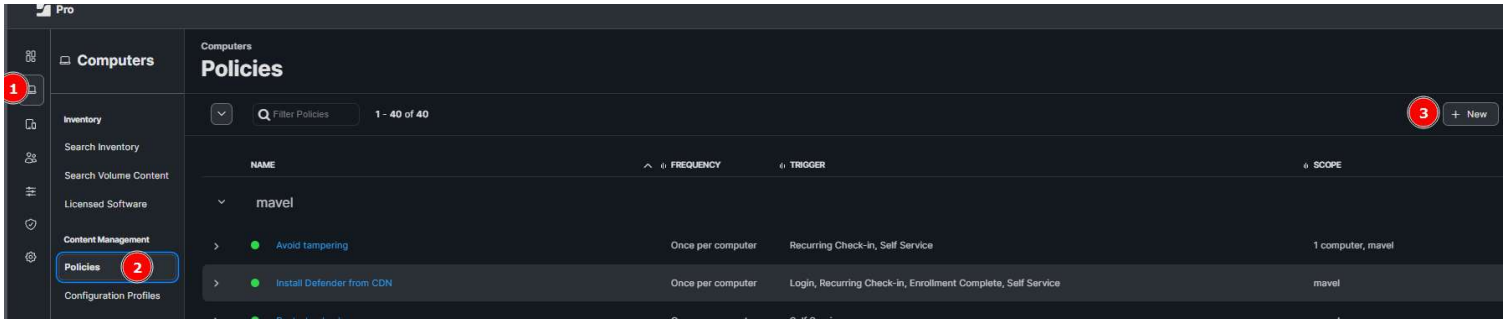
    a. Display Name: 25072 Upgrade Package
    b. Category: Choose any category that you can easily locate
    c. Filename: Download the file from this public Microsoft CDN link:

       https://officecdn-microsoft-com.akamaized.net/pr/C1297A47-86C4-4C1F-97FA-950631F94777/MacAutoupdate/upgrade_from_25062_helper.pkg

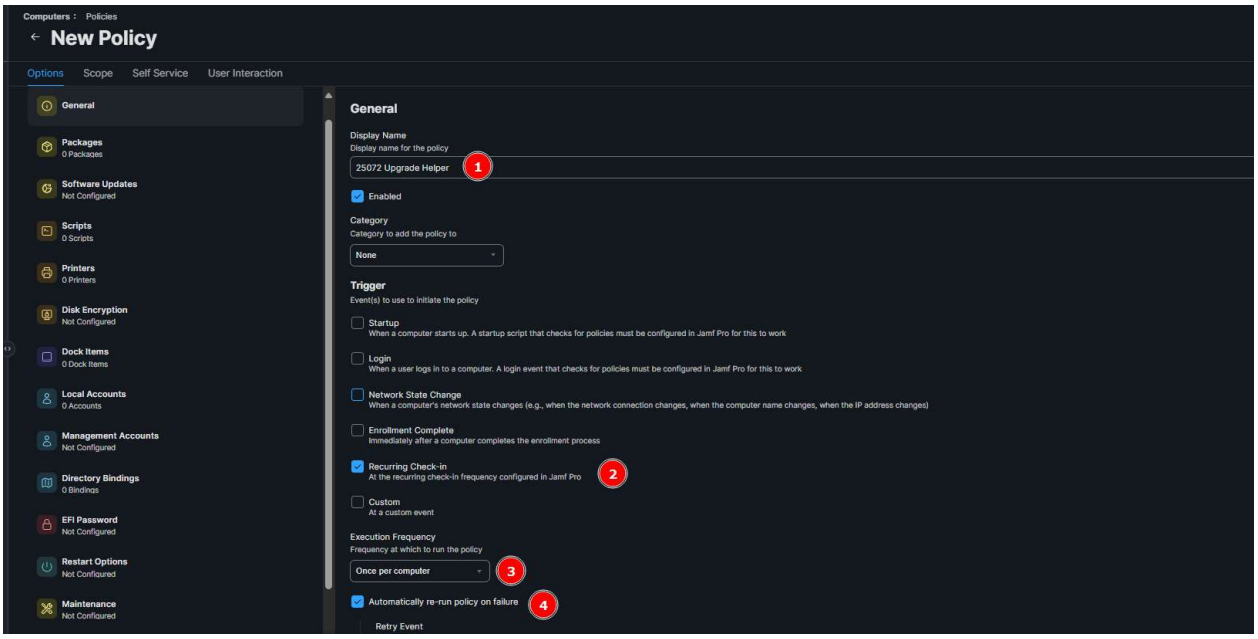
       Ensure you have unzipped the file and located **upgrade_helper-1.0.1.pkg** which will be uploaded to JAMF.
    d. Info: Not required
    e. Notes: Not required
    f. Manifest File: This isn't required. Leave as default

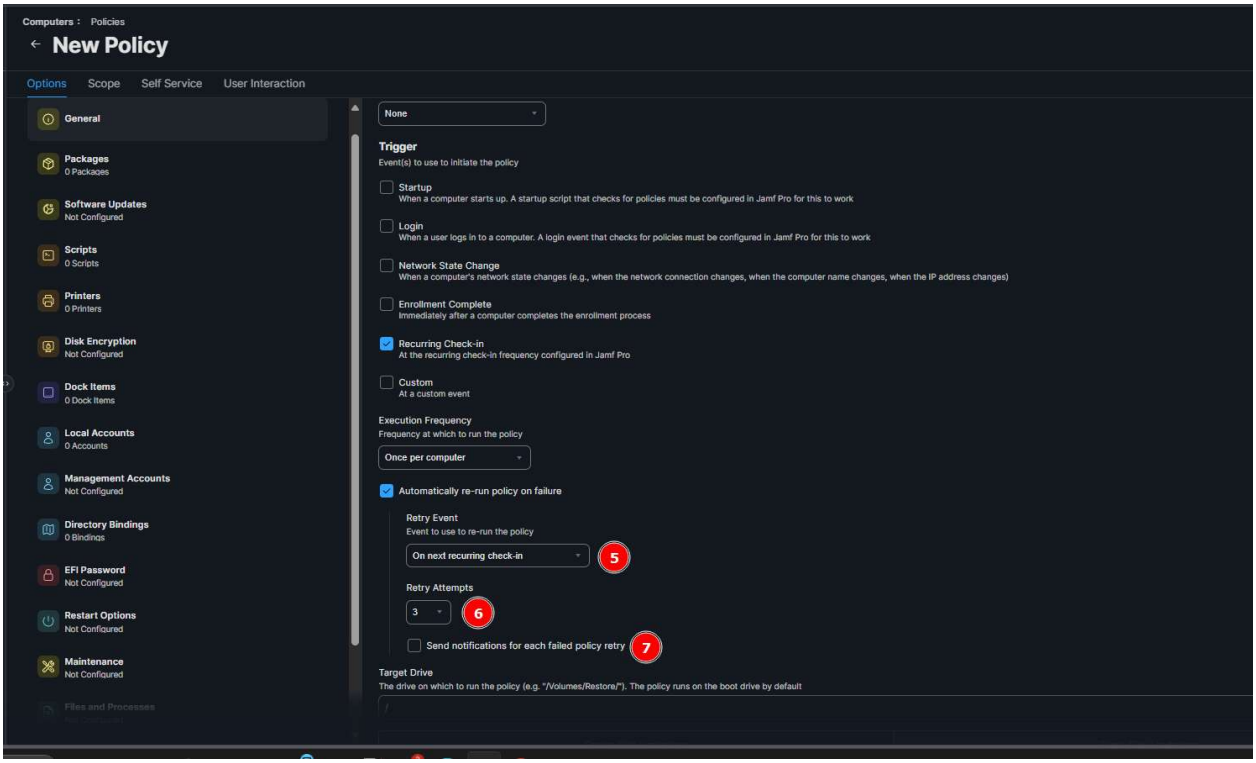


3) Now that we have the package in JAMF, we can deploy it to our endpoints. Navigate to Policies page by going **to computer management**(1), select **Policies**(2), and select +**New**(3)

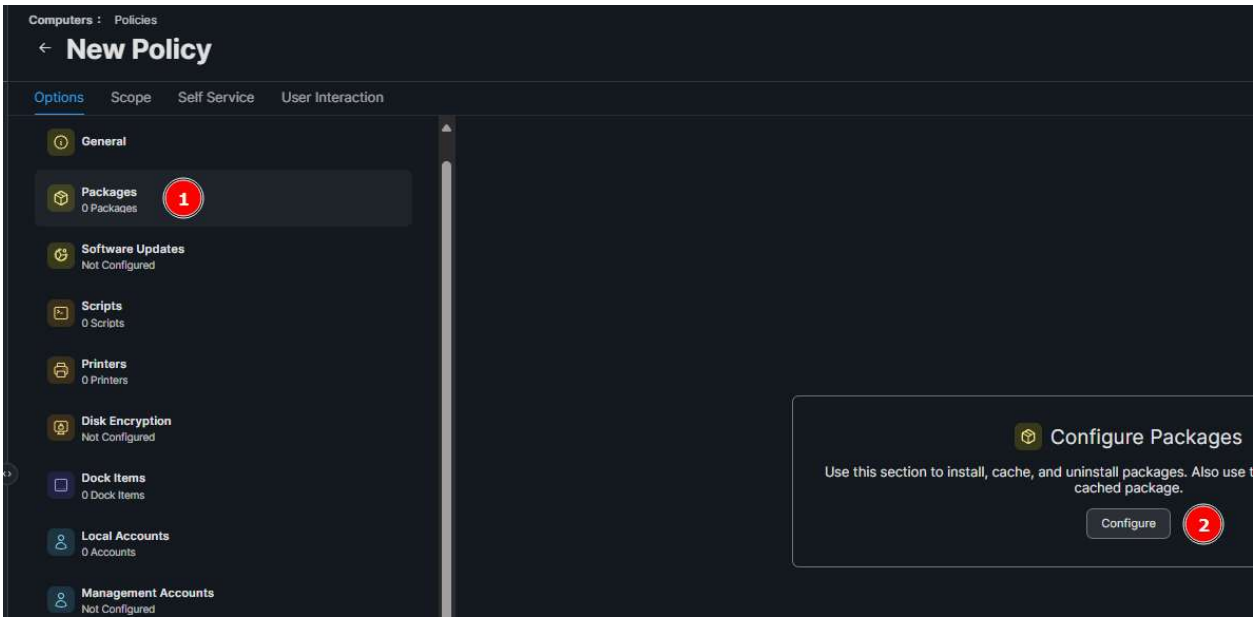


4) In General, for the Display name, type **25072 Upgrade Helper**(1) then select **Recurring Check-in**(2) under the **Trigger** section. You should also configuration an execution frequency of at least **once per computer(3)** and check the **Automatically re-run policy on failure**(4). Under this section, specify **Retry Event** to **On next recurring check-in**(5) as well as **3 retry attempts(**6) and **send notification of failed policy retry**(7). Review images below for assistance on configuring these settings

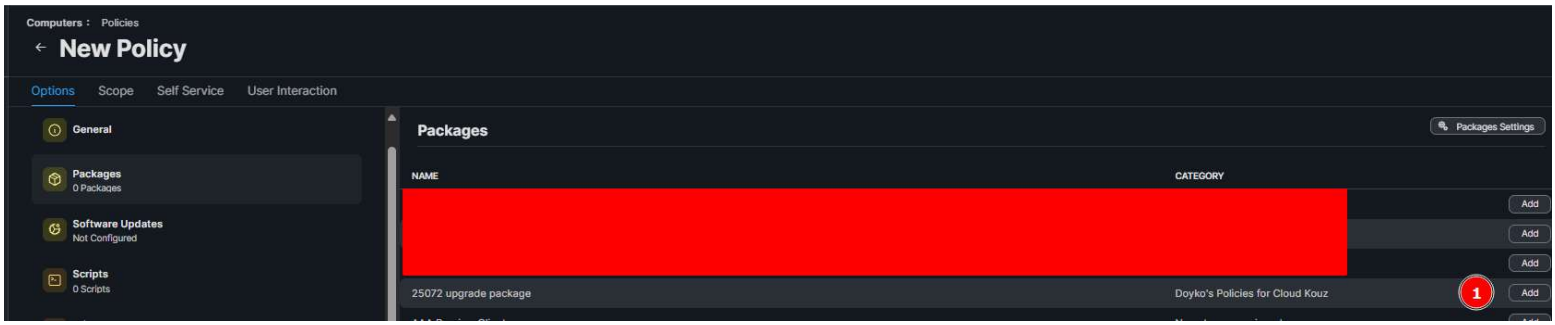




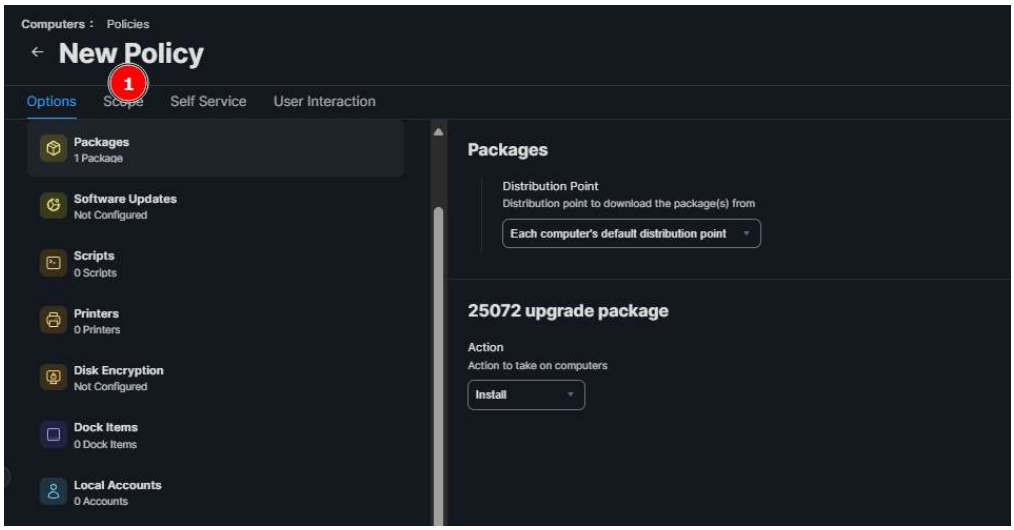
5) Select **packages**(1) on left hand side and click on **configure**(2) to add the previously uploaded package.



6) In the packages displayed find and add the **25072 Upgrade package** from Section 2 step 2.



7) Leave everything as is on the next page and navigate to the Scopes tab in order to specify the devices that will receive this package



8) JAMF Admins should specify either specific computers to get this package or they should specify a specific computer group. **Microsoft always recommends testing on a smaller sample size before deploying to production!** The devices that are **targeted in this policy should also be the same ones targeted from section 1 or the policy will fail to install.**

9) Once the scope is selected, you can save the policy.

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:**

```
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**