

Contents

- Privilege Manager for macOS User Guide 2
- Installation..... 2
 - Deploy Agents using an Unattended Install Method 3
 - After Initial Deployment..... 4
 - Register New Agents and Finding Logs for Troubleshooting: 4
 - Terminal Commands 4
- Overview: Creating macOS Policies..... 5
 - Actions supported by macOS Agents 5
 - Adding macOS Agents to a Computer Testing Group and Setting Up Learning Mode Policies for macOS 6
 - macOS Application Self-elevation 6
 - Configuring Application Self-elevation..... 7
 - How to Request an Application Run as Administrator 8
 - Troubleshooting: Verify the Finder Extension is Installed 9
 - Request Application Installation 10
 - Example Policy: Allow Copy/Install of Applications 12
 - Updating Existing Policies to Use the Copy Install Application Filter 15
 - Example Policy: Require Justification - FireFox 15
 - Example Policy: Deny Photos 17
- How to Recover an Unresponsive macOS Endpoint 19
- Pro Tips..... 20
 - Creating Filters Manually 20
 - Preference Pane in Macs : Targeting System Preferences..... 21

Privilege Manager for macOS User Guide

Welcome to Privilege Manager for macOS. MacOS machines work differently than Windows machines and navigating the Thycotic macOS agent has a slightly different process as well. Here is what you will need to know for installing, setting up, and configuring policies for your macOS endpoints.

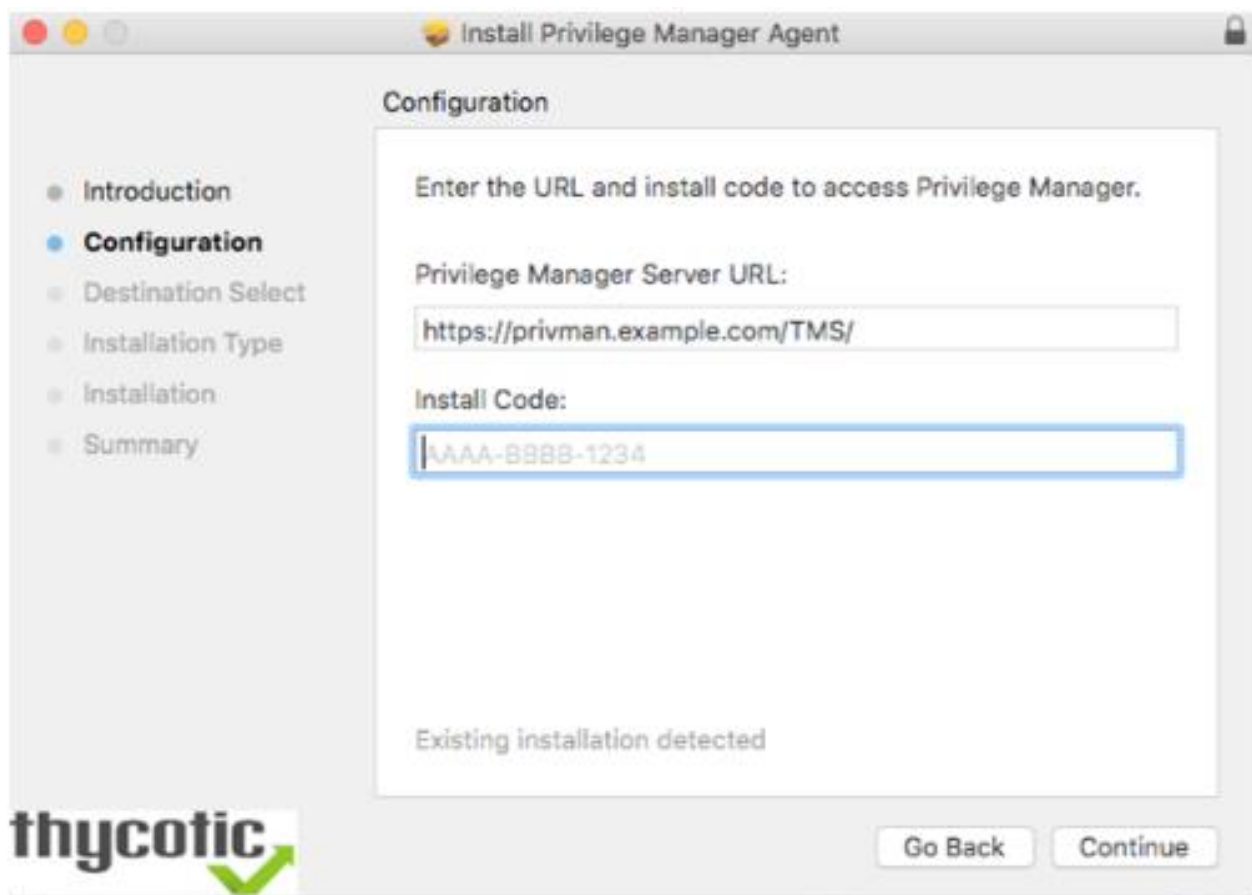
Installation

The bundled macOS Agent is a DMG + PKG file. You can use this macOS agent installer directly on individual endpoints for testing or production environments.

To install the Thycotic agents on a single testing machine, follow these steps:

1. Go to [Agent Downloads](#) and download the Privilege Manager macOS Agent.
2. Run the bundled macOS Agent DMG + PKG Installer on the computer you want to manage.
3. During the setup process, enter the base URL and the [Install Code](#) when prompted.

Note: The Install Code field can be left blank when using versions lower than 10.5



Deploy Agents using an Unattended Install Method

Begin by downloading the DMG + PKG package (see link for Privilege Manager macOS Agent listed above) on one of your Mac endpoints. Run the installer by double clicking the PKG file.

After installing this first agent, navigate to */Library/Application Support/Thycotic/Agent/agentconfig.json*. The agentconfig.json file stores information such as your organization's URL and a few other custom settings like 'Task Polling Interval,' etc.

Open the file and add the "installCode" parameter after the "tmsBaseUrl" to that file (see example below).

```
{
    "tmsBaseUrl": "https://servername/Tms/",
    "installCode": "VALUEHERE"
}
```

Note: The Install Code field can be left blank when using versions lower than 10.5

There are two methods for deploying your remaining macOS agents in an unattended fashion:

1. Network File Share

If you want administrators to deploy agents onto individual macOS endpoints, save the PKG installer from the DMG side-by-side with the agentconfig.json file in a network share folder.

Due to new macOS security enhancements, users cannot run a PKG installer from a network share anymore. The administrator must then run the installer command-line tool from Terminal.app after mounting and cd'ing to the directory containing the PKG installer and agentconfig.json file:

```
cd /Volumes/<network share>/<path to PKG installer>
sudo installer -pkg ThycoticManagementAgent-10.6.18.pkg -target /
```

The PKG first looks for an agentconfig.json file located in the same folder. When it finds this file, it will copy agentconfig.json into the */Library/Application Support/Thycotic/Agent* folder during the unattended install on the macOS endpoint where the installer is running.

2. Distribution Tool

Using a Deployment Tool like Jamf or SCCM, include both the PKG installer and the agentconfig.json files in the distribution package together, then deploy the package onto your endpoint macs by running a script using a tool or remotely by using ssh to install the PKG, for example:

```
sudo installer -pkg ThycoticManagementAgent-10.6.18.pkg -target /
```

As in the example using a Network Share, the PKG will first look for an agentconfig.json file located in the same folder. When it finds this file, it will copy agentconfig.json into the */Library/Application*

Support/Thycotic/Agent folder during the unattended install on the macOS endpoint where the installer is running.

For more instructions on how to deploy in bulk using Microsoft Software System Center Configuration Manager (SCCM), Microsoft instructions for macOS endpoints are described [here](#).

After Initial Deployment

If the macOS endpoint already has an existing `agentconfig.json` file, it will NOT be overwritten because creating a file only occurs if the computer didn't already have an `agentconfig.json` installed. This means you can use the same distribution package for upgrades and new installs.

Note that it will take 15-30 minutes for newly installed agents to register in Privilege Manager, and policies will update according to a scheduled task in Privilege Manager. To check the schedule on this task, go to Admin | Resources | [Select Mac Machine Name] | "Update Agent Commands (Mac OS)" Policy | Triggers tab. To register agents immediately, see instructions in the **Terminal Commands** section below.

Register New Agents and Finding Logs for Troubleshooting:

For troubleshooting the macOS agent, logs are found in the Console application. There are two places to check for logs in Console:

First, you can filter your machine's logs by clicking your machine's name under Devices and typing "Thycotic" into the top search bar.

Second, Thycotic-specific logs are recorded in a Console folder that is titled `thycotic`, found in the left side bar:

- Reports | /var/log | `thycotic`.

Terminal Commands

In the macOS Terminal application you can perform the following commands directly to your Thycotic macOS agent. Find this list by entering: `sudo /usr/local/thycotic/agent/agentUtil.sh` into Terminal:

```
runschedule -scheduleId {id}
updateclientitems
clientitemsummary
register
settmsserver -serverUri {https://servername.com/Tms/}
settmsserver -serverName {servername}
stop
start
restart
enableverboselogging
disableverboselogging
```

To perform a command, insert the name of the above command that you need to perform into this command string:

```
sudo /usr/local/thycotic/agent/agentUtil.sh [InsertCommandHere]
```

As one example, if you entered an incorrect server name path in the agent installer and Privilege Manager therefore cannot find and register your macOS agent, you can run the command:

```
sudo /usr/local/thycotic/agent/agentUtil.sh settmsserver -serverUri {https://servername.com/Tms/}
```

using the correct server name uri to redirect your agent toward the correct server location. Or, to register an agent immediately after updating the Privilege Manager server location, type:

```
sudo /usr/local/thycotic/agent/agentUtil.sh register
```

```
macadmins-MacBook-Pro:~ macadmin$ sudo /usr/local/thycotic/agent/agentUtil.sh register
Password:
Initiated registration.
macadmins-MacBook-Pro:~ macadmin$ █
```

Overview: Creating macOS Policies

Once your macOS agent is registered, creating policies for your macOS machines follows a very similar process to creating policies for Windows machines in Privilege Manager:

1. **Collect File Data**—This enables Privilege Manager to recognize specific files and file types in your environment. The file data that you want to target with policies are called Events. All imported files can be viewed in the Event Discovery | Files page.
2. **Create Filters**—This step sorts important file data (Events) according to different criteria.
3. **Create Policies**—This step defines what 1) Actions to perform on applications and the 2) Targets (Locations) for those actions.
4. **Assign Filters to Policies**—This step directs a Policy's actions to the appropriate Events happening on your network. This step also allows a Policy to be Enabled, or activated.
5. **Order your Policies based on priority level**—Once your policies are created, the order they execute across your network matters. See the Policy Priority section in this guide for more details.

Things to know: In macOS, roles are bifurcated into two groups: Admins, and Users rather than by Group Policy Objects (GPO) found in Windows environments.

Actions supported by macOS Agents

The following actions are supported by macOS agents:

- Allow Copy to /Applications/Directory
- Allow Package Installation
- Application Approval Request (with Offline Fallback) Message Action
- Application Approval Request (with ServiceNow Request Item Number) Message Action
- Application Approval Request Message Action (workflow request)
- Application Denied Message Action
- Application Justification Message Action

- Application Warning Message Action
- Deny Execute / Deny Execute Message
- File Quarantine
- Quarantine Message
- Run as Root (Elevate)

The following instructions will walk you through how to create several example policies for your Macs to get started.

Adding macOS Agents to a Computer Testing Group and Setting Up Learning Mode Policies for macOS

The Policy Configuration examples in the following section will use a Learning Mode Policy that enables us to perform actions (i.e. run applications) on a test computer that Privilege Manager will then pick up. This makes targeting specific applications during policy creation easy.

To create a Learning Mode Policy on your Mac, begin by adding your newly registered macOS Agent to your Test Computer Group for Macs:

1. In Privilege Manager go to Admin | Event Discovery | Configuration, then click the underlined Application Compatibility Testing Computers link next to the Log all MacOS activity option.

2. Under the Filter Definition tab, select the macOS computer/s you want to target for testing under the Include Specific Resources section. This "Testing Computers" group should only be used for testing specific machines and configuration purposes. It should not be assigned to large groups of computers in your production environment.

Note that you may have both macOS and Windows target computers listed in this group but policies are platform-specific, meaning they will distinguish between macOS and Windows computers.

3. To activate your learning mode policy for this target group, verify that the "Log all MacOS activity from Application Compatibility Testing Computers" is checked under the General tab of Admin | Event Discovery | Configuration. Under Admin | Policies | Mac OS tab, you should also see an Event Discovery Testing Computers (MacOS) policy enabled.

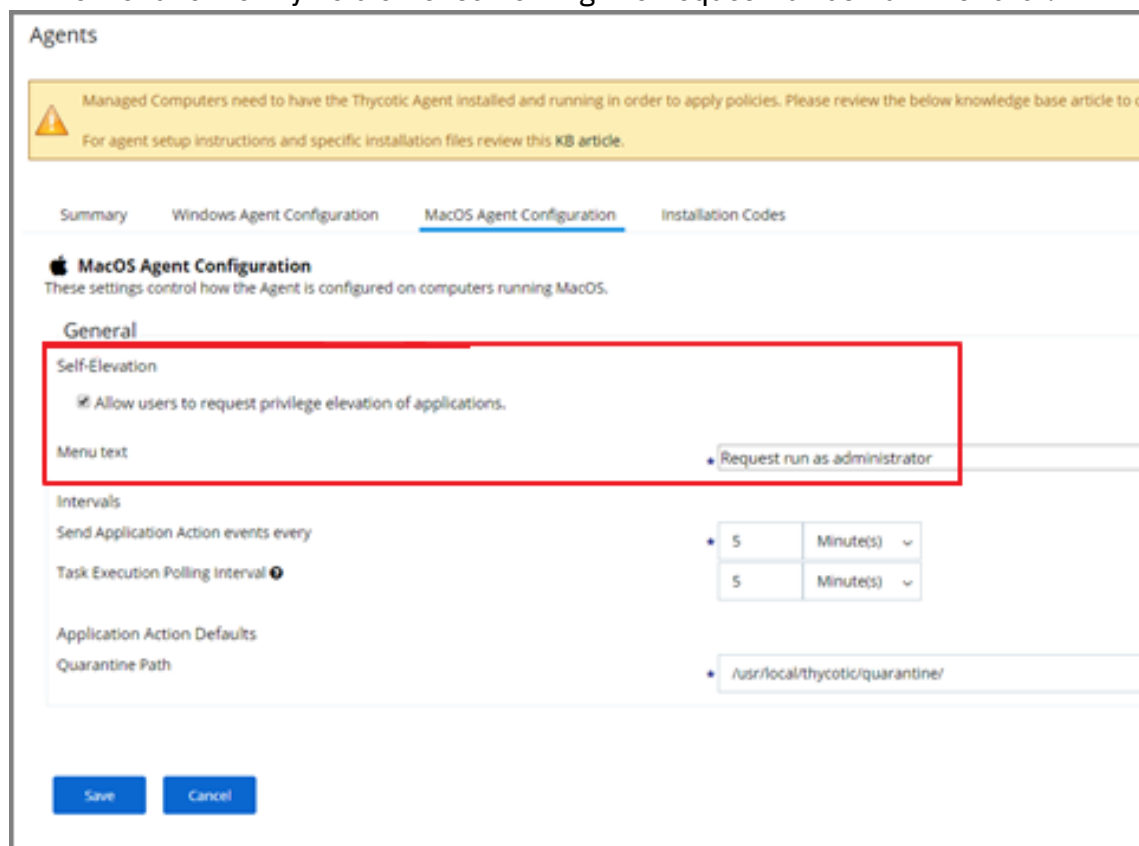
macOS Application Self-elevation

Finder Sync Extensions allow application control on macOS endpoints. Just as on Windows endpoints, users can request application self-elevation via right-click mouse action. The application control is policy based and the macOS system with the endpoint agent must have been online at least once to request its policies from the Privilege Manager server.

Configuring Application Self-elevation

Your Privilege Manager needs to be configured to allow self-elevation of applications on an endpoint. Follow these server configuration steps:

1. Navigate to Admin | Agents and select the MacOS Agent Configuration tab.
2. Click Edit.
3. Under the General section enable Allow users to request privilege elevation of applications.
4. In the Menu text entry field enter something like Request run as Administrator.



The screenshot shows the 'Agents' management console. A yellow banner at the top states: 'Managed Computers need to have the Thycotic Agent installed and running in order to apply policies. Please review the below knowledge base article to do so. For agent setup instructions and specific installation files review this KB article.' Below this is a tabbed interface with 'Summary', 'Windows Agent Configuration', 'MacOS Agent Configuration' (selected), and 'Installation Codes'. The 'MacOS Agent Configuration' section has a title 'MacOS Agent Configuration' and a subtitle 'These settings control how the Agent is configured on computers running MacOS.' Under the 'General' section, the 'Self-Elevation' option is checked, with the text 'Allow users to request privilege elevation of applications.' Below this, the 'Menu text' field is populated with 'Request run as administrator'. Further down, the 'Intervals' section shows 'Send Application Action events every' set to 5 Minute(s) and 'Task Execution Polling Interval' set to 5 Minute(s). The 'Application Action Defaults' section shows the 'Quarantine Path' set to '/usr/local/thycotic/quarantine/'. At the bottom are 'Save' and 'Cancel' buttons.

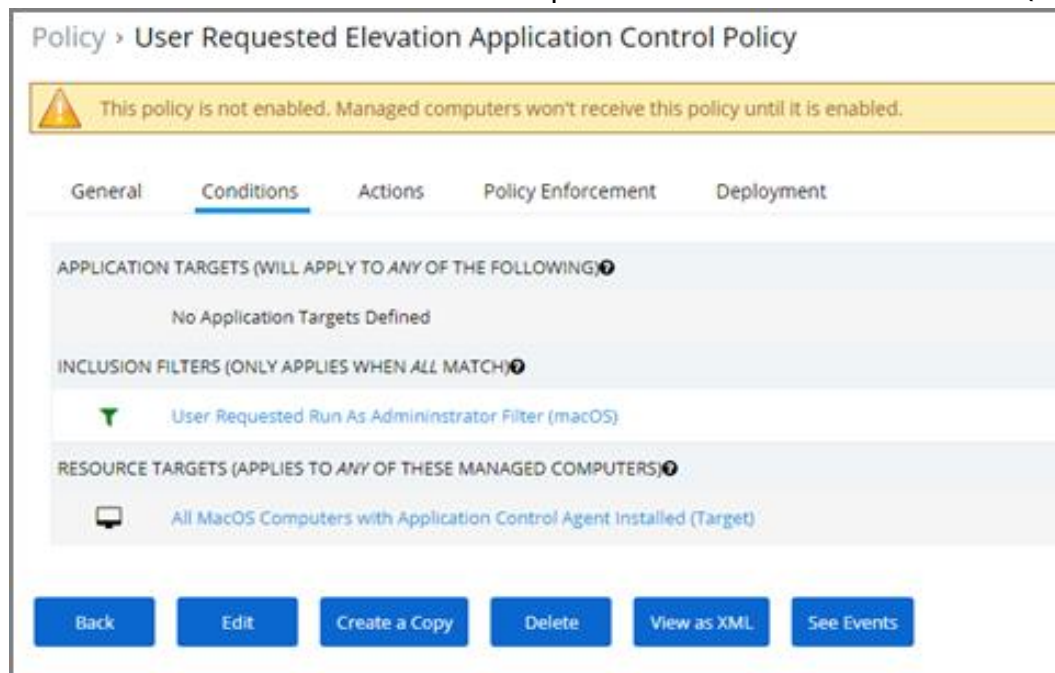
5. Click Save.

NOTE: When Self-Elevation options are modified in the MacOS Agent Configuration, client items on a macOS system must be updated and on older versions of macOS the user must logout and login for the changes to take effect.

After enabling the Allow users to request privilege elevation of applications in the MacOS Agent Configuration, you can create policies to target the User Requested Run As Administrator Filter (macOS) and specify which action you want taken. If you choose Approval Request, users will have to request and gain approval before having the application elevated.

1. Navigate to Admin | Policies.
2. Click Add New Policy.
3. Navigate to the Conditions tab and Inclusion Filters section.

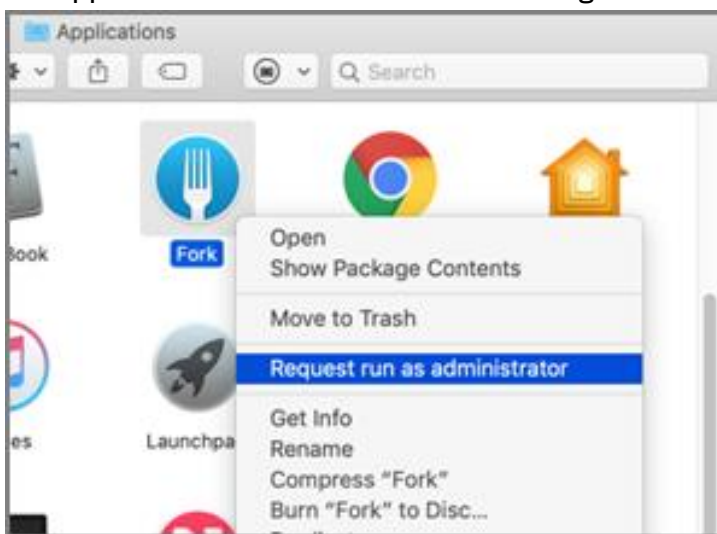
4. Click + Add Filter and select the User Requested Run As Administrator Filter (macOS) filter.



5. Click Save.

How to Request an Application Run as Administrator

To request to run an application as Administrator, the user at the macOS endpoint navigates to and selects the applications in Finder and uses either right-click or Control+Click to invoke Finder's context menu.:



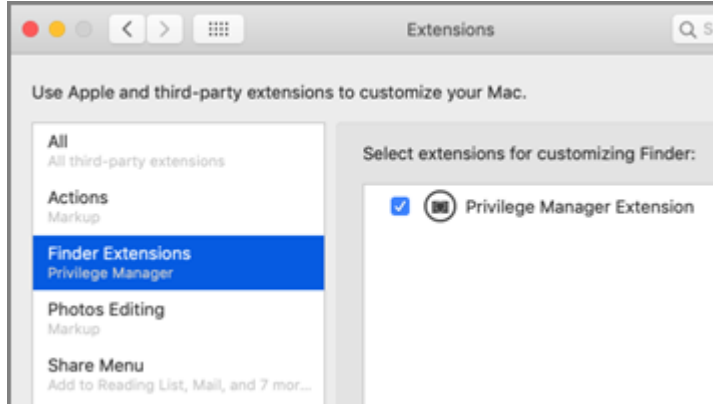
Here the user selects the Request run as administrator menu option.

Depending on the policy in place, this will either be granted immediately or trigger an approval request.

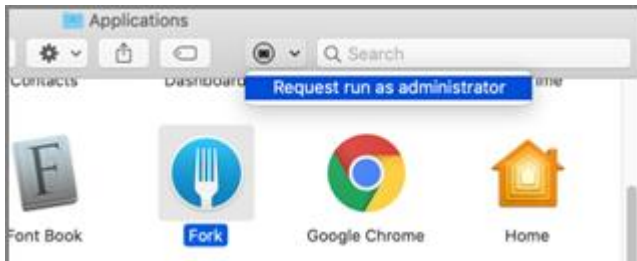
Troubleshooting: Verify the Finder Extension is Installed

The Finder Privilege Manager extension installs by default during an agent install or upgrade. The extension is enabled/disabled based on the MacOS Agent Configuration policy on the Privilege Manager Server. If the extension is not enabled, check with your system administrator.

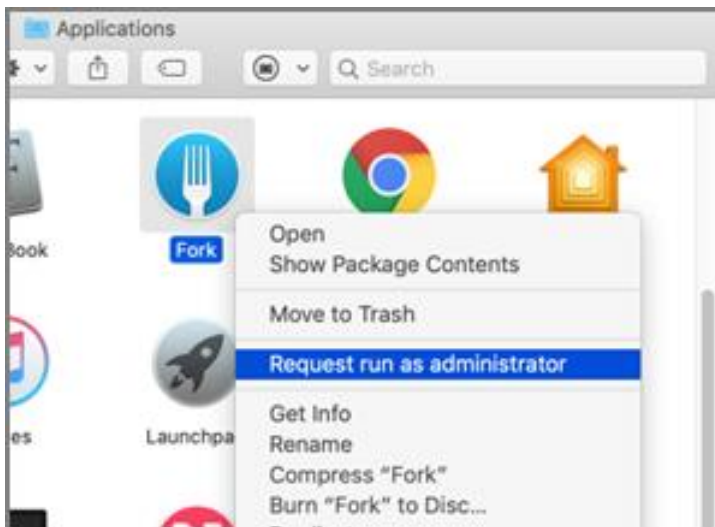
1. Open System Preferences | Extensions.
2. Select Finder Extensions.
3. Verify that Privilege Manager Extension is listed and enabled for customizing Finder.



Once the Privilege Manager Extension is enabled, the extension icon is visible in Finder:



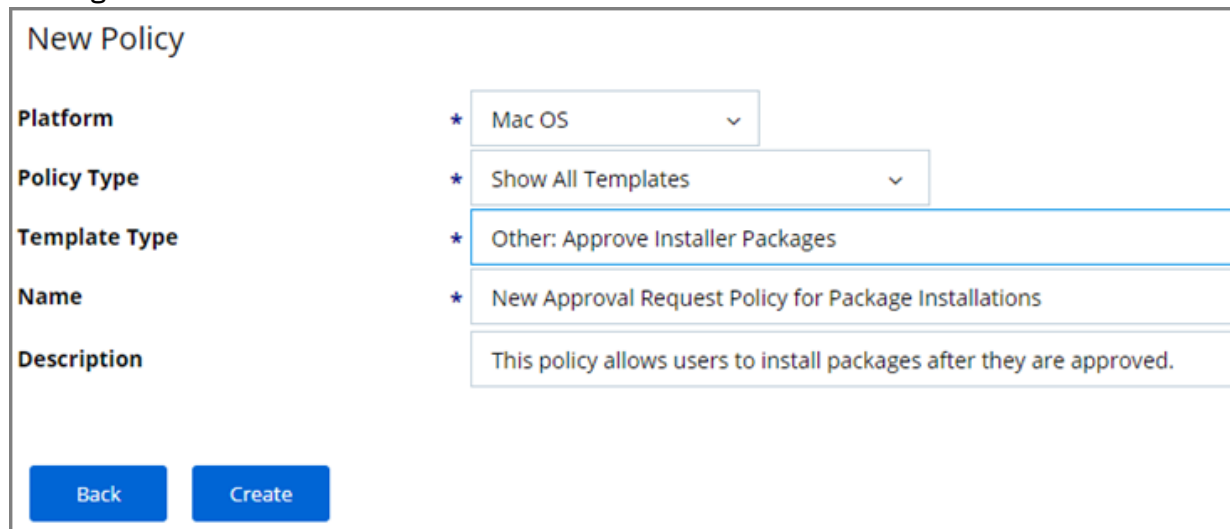
The extension is also present as a menu item when you right-click or control+click an application in Finder.



Request Application Installation

Privilege Manager can allow macOS users to install packages on demand. Do the following to create a policy to allow users to request installation of certain packages. For this to work, your endpoint must be online.

1. Navigate to Admin | Policies and select Add Policy.
2. Choose the Mac OS Platform and select Show All Templates and then Other: Approve Installer Packages.

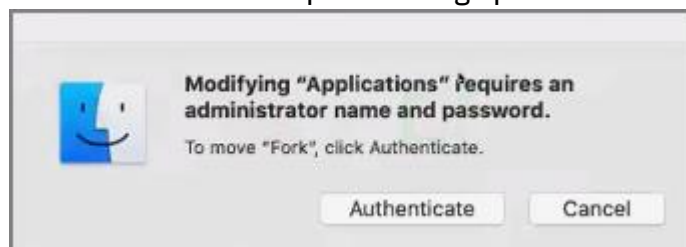


The screenshot shows the 'New Policy' form. It has a title 'New Policy' at the top. Below it are five fields: 'Platform' with a dropdown menu showing 'Mac OS', 'Policy Type' with a dropdown menu showing 'Show All Templates', 'Template Type' with a dropdown menu showing 'Other: Approve Installer Packages', 'Name' with a text input field containing 'New Approval Request Policy for Package Installations', and 'Description' with a text input field containing 'This policy allows users to install packages after they are approved.' At the bottom of the form are two buttons: 'Back' and 'Create'.

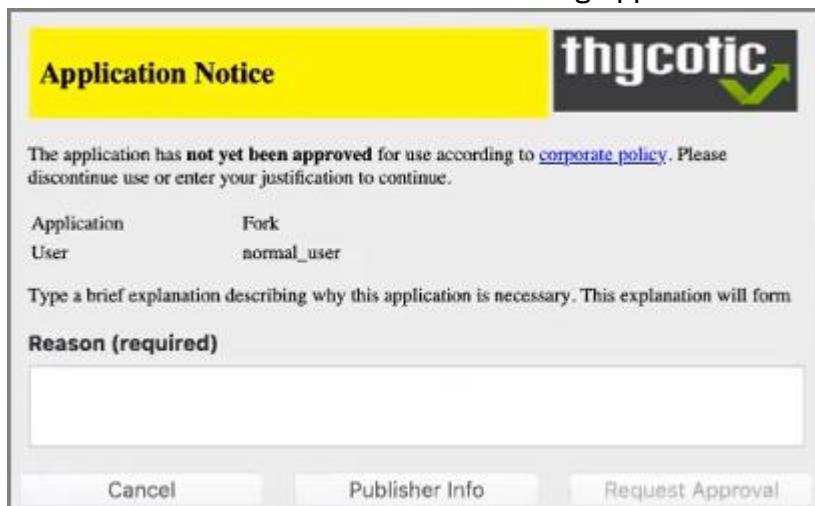
3. Customize the Name and Description and click Create.
4. Enable the policy after it has been created and update policies at the endpoint.

Once the policy is enabled and in place at the endpoint, a user will see the following steps to request an application installation:

1. Mount the DMG containing the application you'd like to install to Applications. If the DMG contains an application bundle that can be dragged to the Applications folder, do so. If the DMG contains an installer application, double-click and proceed with the steps outlined in installing an application.
2. The Authentication required dialog opens:

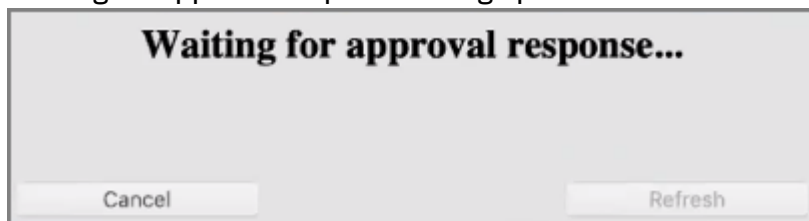


3. Click the Authenticate button. The following Application Notice opens:



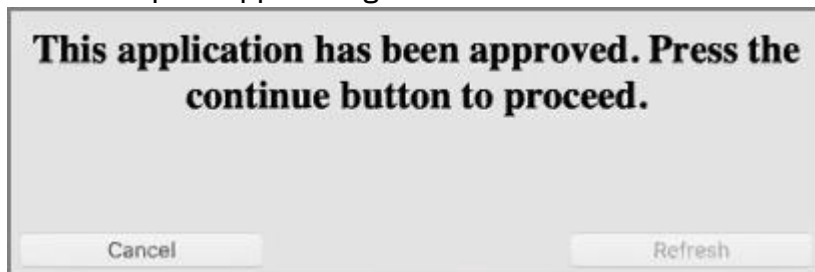
The dialog box titled "Application Notice" features the Thycotic logo in the top right corner. The main text states: "The application has **not yet been approved** for use according to [corporate policy](#). Please discontinue use or enter your justification to continue." Below this, it displays "Application: Fork" and "User: normal_user". A prompt asks the user to "Type a brief explanation describing why this application is necessary. This explanation will form Reason (required)". A large text input field is provided for this purpose. At the bottom, there are three buttons: "Cancel", "Publisher Info", and "Request Approval".

4. Enter the Reason why the application should be installed and click the Request Approval button. The Waiting for approval response dialog opens.



The dialog box titled "Waiting for approval response..." contains two buttons at the bottom: "Cancel" and "Refresh".

5. Once approved, the "This application has been approved..." text displays. Click the Continue button to proceed with the installation. If you click Cancel, the application will not be installed and you may need to request approval again.



The dialog box titled "This application has been approved. Press the continue button to proceed." contains two buttons at the bottom: "Cancel" and "Refresh".

Example Policy: Allow Copy/Install of Applications

A policy can be created to allow or deny standard users to install specific applications by copying/pulling the application into the Applications folder. Follow this example to create a policy that will enable this functionality for your Mac OS user.

1. Navigate to Admin | Policies and click the Add New Policy button.
2. From the Platform drop-down select Mac OS.
3. From the Policy Type drop-down select Show All Templates.
4. From the Template Type drop-down select Other: Allow Standard Users to Copy to Applications Directory (via Drag and Drop), this can also be done via Other: Empty Policy.

New Policy

Platform * Mac OS

Policy Type * Show All Templates

Template Type * Other: Allow Standard Users to Copy to Applications Directory (via Drag and Drop)

Name * New Allow Standard Users to Copy Chosen Apps to Applications Directory Policy


Description This policy allows users to copy approved apps to the Applications directory via drag and drop with justification.

[Back](#) [Create](#)

5. Enter a name and description for the new policy and click Create.
6. Once the policy is created, it can be modified to be restricted to certain applications instead of targeting every application:
 1. Click + Add Application Target to specify an application bundles filter for Mac OS applications.
 2. Click + Add Inclusion Filter to specify the Copy Install Application filter.


3. Click Save.

Policy > Mac Copy to Applications Folder


 This policy is not enabled. Managed computers won't receive this policy until it is enabled.

General Conditions Actions Policy Enforcement Deployment


APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING) ⓘ

 [FaceTime Application Bundle Filter \(MacOS\)](#)

INCLUSION FILTERS (ONLY APPLIES WHEN ALL MATCH) ⓘ

 [Copy Install Application](#)

RESOURCE TARGETS (APPLIES TO ANY OF THESE MANAGED COMPUTERS) ⓘ


 [All MacOS Computers with Application Control Agent Installed \(Target\)](#)

[Back](#) [Edit](#) [Create a Copy](#) [Delete](#) [See Events](#)

7. Navigate to the General tab.
8. Click Edit.

9. Select the Enabled checkbox to enable the policy.

Policy > Mac Copy to Applications Folder

 This policy is not enabled. Managed computers won't receive this policy until it is enabled.

General Conditions Actions Policy Enforcement Deployment


Common

Policy Name Mac Copy to Applications Folder


Description


Platform Mac OS

Type

Folder  MacOS Policies

Status

Enabled ☐ 

Policy Priority 50 

Back Edit Create a Copy Delete See Events

10. Click Save.

The new Copy Install Application Filter should not be used with the existing Privilege Manager Copy/Installer Helper Parent Process Filter, which should be removed from any policy before adding the new Copy Install Application Filter to the policy.

Updating Existing Policies to Use the Copy Install Application Filter

If you have policies that currently use the Privilege Manager Copy/Installer Helper Parent Process Filter use the following steps to update them to use the Copy Install Application Filter:

1. Navigate to Admin | Policies.
2. Click Edit and navigate to Conditions tab.
3. Under Inclusion Filters remove Privilege manager copy/installer helper parent process filter.
4. Under Add Inclusion Filter search for and select Copy Install Application and click Add.
5. Navigate to the Actions tab and remove Allow copy to/Applications/Directory.
6. Click Add Action and select Application Approval Request Message Action then click Add.
7. Navigate to Policy Enforcement and select any of the options:
 - Continue enforcing policies after enforcing this policy
 - Continue enforcing policies for child processes after enforcing this policy
8. Login as Admin user.
9. Open the macOS Agent via Terminal and run an update using command:

```
sudo /usr/local/thycotic/agent/agentUtil.sh updateclientitems
```

Agents update with new and updated policies and synchronize.

Example Policy: Require Justification - FireFox

1. With your Learning Mode Policy enabled, open Firefox on your test Mac. A few minutes after doing this you should find a new item in Admin | Event Discovery | Policies titled Firefox. Click Create Filter, then +Create.

Note: If you are not immediately directed to an Add New Filter screen, this means Privilege Manager doesn't have enough information to target this application. In these cases you may need to create Filters manually (Admin | Filters | Add Filter). See the Create Filters Manually section under Pro Tips below for more information.

2. Next, navigate to Admin | Policies and Add New Policy. Select Mac OS as a Platform, Show All Templates for Policy Type and then Other: Empty Policy as Template Type. Name your new policy "Firefox - Request Access (MacOS)" and add a Description. Click Create.
3. Under the Conditions tab, click Edit, then Add Application Target. Search for filter name for your Firefox policy (created in step 1) and Add. Verify the Resource Targets section at the bottom of this page lists the correct target computer group for Mac machines that you want to apply this policy to.
4. Under the Actions tab, click Add Action, search for "Application Justification Message Action" and "Application Approval Request Message Action," and Add these. Then navigate to the General tab and check the Enabled box. Save.

5. To make sure your policy is effective, pull up Terminal on your testing Mac endpoint and run the `sudo /usr/local/thycotic/agent/agentUtil.sh updateclientitems` command.

Once this Request Access-policy is updated on your endpoint, when you click Firefox you will see a prompt where the user can enter their reason for accessing Firefox:

Application Notice

thycotic

Please provide a reason as to why you require this application to be run with elevated rights.

Application Firefox
User macadmin

Type a brief explanation describing why this application is necessary. This explanation will be recorded and may be reviewed by the IT staff for consideration into [corporate policy](#).

Reason (required)

What does the fox say?

Cancel Publisher Info Continue

To Accept this request, navigate to Tools | Manage Approvals in Privilege Manager. Click the request and approve--you may do so for one time access or for a time interval:

Manage Approval Requests

Revisions that are awaiting approval.

Default Approve Deny

	Policy	User	User Reason	Requested
	Firefox - Request Access	macadmin@MacBook-Pro-thycotic	What does the fox say?	October 22, 2017, 10:45 AM

User reason:
File path:
Computer:

What does the fox say?
(Applications/Netflix.app/Contents/Resources/...)
macadmin: MacBook

Approve Deny

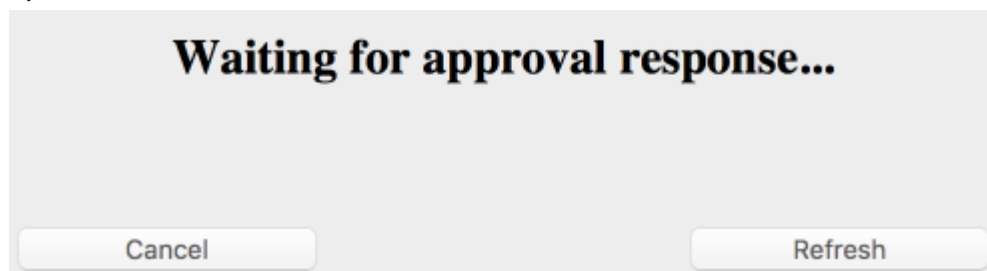
Confirm Approval

Approve: ☐ One time ☒ For: hour(s) ▼

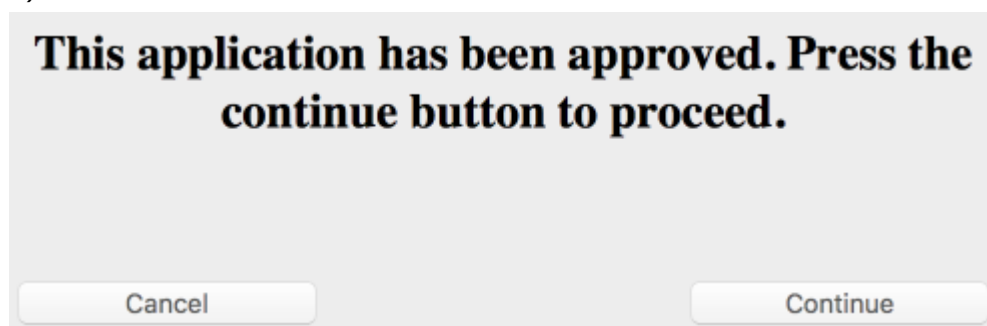
Approve Cancel

On the Mac machine, your user will see these messages:

1)



2)



Example Policy: Deny Photos

With your Learning Mode policy properly set up, anything you do on your Mac test machine will be discovered by Privilege Manager. For this example we will create a policy that blocks the Photos application as well as the PhotoBooth application.

1. Begin by opening the Photos and PhotoBooth applications on your Mac test machine. Then, in Event Discovery | Policies, check to make sure new items have been registered by your Event Discovery Testing Computers (MacOS) policy. These may be listed as "New Loaded Resources." Click into these items and then click the Discover Now button. It still may take time to properly load details about these new events.
2. Next, navigate to Admin | Policies and Add New Policy. Select Mac OS as a Platform, Blacklist / Deny Application Execution for Policy Type and then Blacklist: Deny Specific Applications. Name your new policy "Block Photos (MacOS)" and add a Description. Click Create.
3. Return to Admin | Event Discovery | Policy Activity. You should see an event titled Photos and another titled PhotoBooth. Click Create Filter underneath each of these events and then +Create.
4. Navigate back to Admin | Policies | MacOS tab, select the Block Photos (MacOS) policy that you created in step 2. Under the Conditions tab, click Edit, then Add Application Target. Search for the two filter names you created in step 3. Add both filters to this policy. Verify the Resource Targets section at the bottom of this page lists the correct target computer group for Mac machines that you want to apply this policy to. Then navigate to the General tab and check the Enabled box. Save.

To make sure your policy is effective, pull up Terminal on your testing Mac endpoint and run the command:

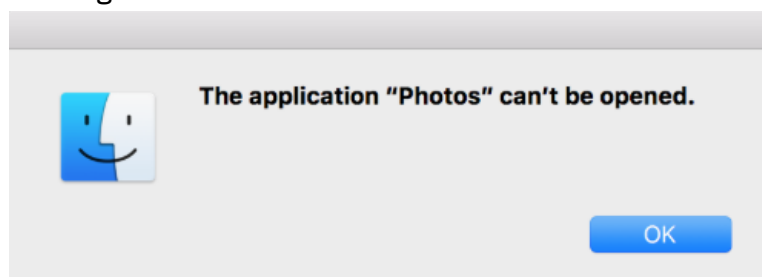
```
sudo /usr/local/thycotic/agent/agentUtil.sh updateclientitems
[macadmins-MacBook-Pro:~ macadmin$ sudo /usr/local/thycotic/agent/agentUtil.sh up]
dateclientitems
Updating policy client items...
Updating unknown client items...
Updating command client items...
Updating action client items...
Updating filter client items...

22 client items are up to date

13 policies are up to date

Updated policy "Block Photos (MacOS)" (657ded1a-79af-4bae-b444-fb52bd90bf29)
macadmins-MacBook-Pro:~ macadmin$
```

Once this Deny-policy is updated on your endpoint, when you click Photobooth or Photos, you will see this message:



How to Recover an Unresponsive macOS Endpoint

In case a macOS endpoint ever becomes unresponsive due to conflicting policy configurations, the following steps allow user to recover the endpoint without having to restore or rebuild the system.

1. Turn off the macOS system.
2. Hold down the $\text{⌘}+\text{s}$ keys and power the system back on. Keep holding those keys down until it shows that it is booting in single-user mode.
3. Follow the prompts to mount the root device as read-write. It will instruct you to enter the following:

```
/sbin/fsck -fy  
/sbin/mount -uw /
```

4. Rename the kernel extension so that you can get back to a functioning macOS:

```
cd /Library/Extensions  
mv ThycoticACS.kext ThycoticACS.kext.org  
exit
```

5. The system will restart.
6. Disable and/or delete policies that are causing the issue.
7. Update client items before renaming the kernel extension and having it start automatically. You can force client item updates by performing the following in Terminal.app:

```
sudo /usr/local/thycotic/agent/updateClientItems.sh
```

8. Restore the kernel extension in Terminal.app:

```
cd /Library/Extensions  
sudo mv ThycoticACS.kext.org ThycoticACS.kext  
exit
```

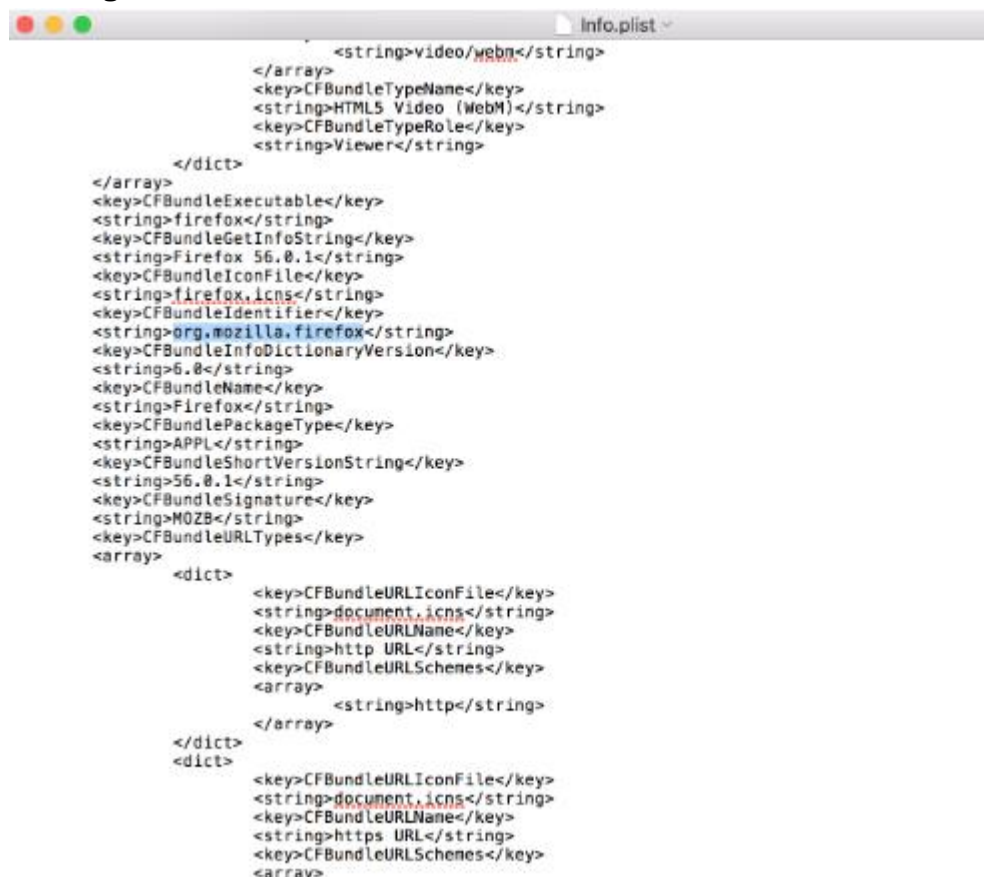
Pro Tips

Creating Filters Manually

From the Files Event Discovery View page (Admin | Event Discovery | Files), when you click “Create Filter” under a file, if you are NOT directed to an Add New Filter screen, this means Privilege Manager doesn’t have enough information to target this application. In these cases you may need to create Filters manually (Admin | Filters | Add Filter).

To manually find granular information required for targeting applications in Privilege Manager on your Mac, right-click the application on your endpoint machine and select Show Package Contents. Then Navigate to Contents > Info.plist, this gives you a coded list of items that you can match into the details page of your Filter.

For example, the highlighted section below can be entered into the "Bundled Identifier" line item when creating a Firefox filter.



```
<string>video/webm</string>
</array>
<key>CFBundleTypeName</key>
<string>HTML5 Video (WebM)</string>
<key>CFBundleTypeRole</key>
<string>Viewer</string>
</dict>
</array>
<key>CFBundleExecutable</key>
<string>firefox</string>
<key>CFBundleGetInfoString</key>
<string>Firefox 56.0.1</string>
<key>CFBundleIconFile</key>
<string>firefox.icns</string>
<key>CFBundleIdentifier</key>
<string>org.mozilla.firefox</string>
<key>CFBundleInfoDictionaryVersion</key>
<string>6.0</string>
<key>CFBundleName</key>
<string>Firefox</string>
<key>CFBundlePackageType</key>
<string>APPL</string>
<key>CFBundleShortVersionString</key>
<string>56.0.1</string>
<key>CFBundleSignature</key>
<string>MOZB</string>
<key>CFBundleURLTypes</key>
<array>
  <dict>
    <key>CFBundleURLIconFile</key>
    <string>document.icns</string>
    <key>CFBundleURLName</key>
    <string>http URL</string>
    <key>CFBundleURLSchemes</key>
    <array>
      <string>http</string>
    </array>
  </dict>
  <dict>
    <key>CFBundleURLIconFile</key>
    <string>document.icns</string>
    <key>CFBundleURLName</key>
    <string>https URL</string>
    <key>CFBundleURLSchemes</key>
    <array>
```

Preference Pane in Macs : Targeting System Preferences

A Preference Pane (abbreviated as prefpane) is a dynamically loaded plugin in Mac OS X. Introduced in Mac OS X v10.0, the purpose of a Preference Pane is to allow the user to set preferences for a specific application or the system by means of a graphical user interface.

How do you target Preference Panes on Macs? On versions of Privilege Manager 10.3 and lower, you need to specify Preference Pane actions via filepath or file name. A chart is listed below for reference to some of the most common Preference Pane targets:

Preference Pane	File Name	File Path
App Store	com.apple.preferences.appstore.remoteservice	/System/Library/PreferencePanes/AppStore.prefPane/Contents/XPCServices/com.apple.preferences.appstore.remoteservice.xpc/Contents/MacOS/
Date & Time	com.apple.preference.datetime.remoteservice	/System/Library/PreferencePanes/DateAndTime.prefPane/Contents/XPCServices/com.apple.preference.datetime.remoteservice.xpc/Contents/MacOS/
Energy Saver	com.apple.preference.energysaver.remoteservice	/System/Library/PreferencePanes/EnergySaver.prefPane/Contents/XPCServices/com.apple.preference.energysaver.remoteservice.xpc/Contents/MacOS/
Network	com.apple.preference.network.remoteservice	/System/Library/PreferencePanes/Network.prefPane/Contents/XPCServices/com.apple.preference.network.remoteservice.xpc/Contents/MacOS/
Parental Controls	com.apple.preferences.parentalcontrols.remoteservice	/System/Library/PreferencePanes/ParentalControls.prefPane/Contents/XPCServices/com.apple.preferences.parentalcontrols.remoteservice.xpc/Contents/MacOS/
Printers and Scanners	com.apple.preference.printfax.remoteservice	/System/Library/PreferencePanes/PrintAndScan.prefPane/Contents/XPCServices/com.apple.preference.printfax.remoteservice.xpc/Contents/MacOS/
Security & Privacy	com.apple.preference.security.remoteservice	/System/Library/PreferencePanes/Security.prefPane/Contents/XPCServices/com.apple.preference.security.remoteservice.xpc/Contents/MacOS/
Sharing	com.apple.preferences.sharing.remoteservice	/System/Library/PreferencePanes/SharingPref.prefPane/Contents/XPCServices/com.apple.preferences.sharing.remoteservice.xpc/Contents/MacOS/
Time Machine	com.apple.prefs.backup.remoteservice	/System/Library/PreferencePanes/TimeMachine.prefPane/Contents/XPCServices/com.apple.prefs.backup.remoteservice.xpc/Contents/MacOS/
User & Groups	com.apple.preferences.users.remoteservice	/System/Library/PreferencePanes/Accounts.prefPane/Contents/XPCServices/com.apple.preferences.users.remoteservice.xpc/Contents/MacOS/