ENDPOINT PROTECTOR

JAMF Deployment User Manual Version 5.2.0.7

User Manual

COSOSYS

Table of Contents

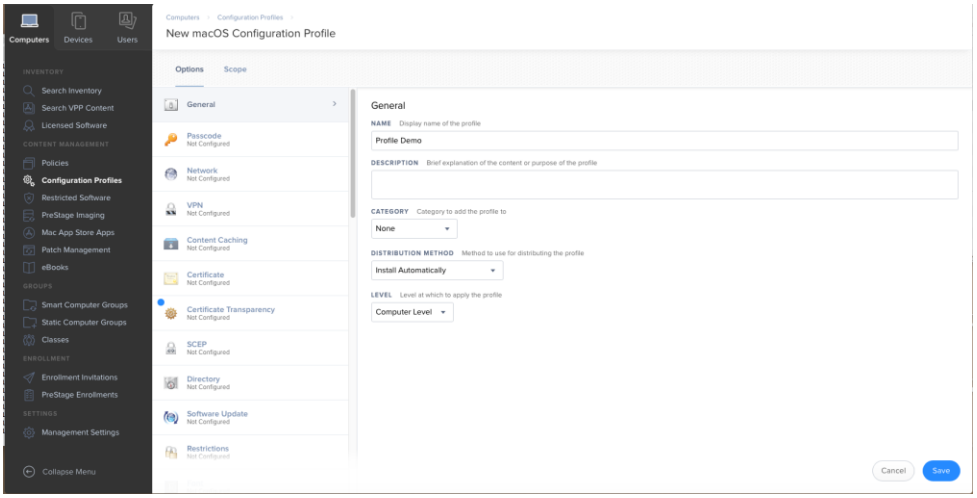
1. Introduction

Since the release of macOS 10.13 (High Sierra), changes have been made in regards to Kernel Extensions (KEXT) that are not signed by Apple. Third-party KEXT are no longer automatically installed and require user approval before loading.

This affects the deployment of the Endpoint Protector Client on all Macs using 10.13 or later. One option to mitigate the scenario is to follow the steps described in this FAQ: Why do I get the System Extension Blocked notification on macOS 10.13 (High Sierra)?

Alternatively, companies can use third party deployment tools such as JAMF and take advantage of the functionalities Apple offers - via the use of Team ID and Bundle ID. General information on this can be found in this FAQ: Where can I find the CoSoSys' Team ID and Bundle ID?. For those using JAMF in particular, the steps are as followed:

1. Login to JAMF Pro account
2. Go to **Computers > Configuration Profile** tab, create a new profile and add a name to it

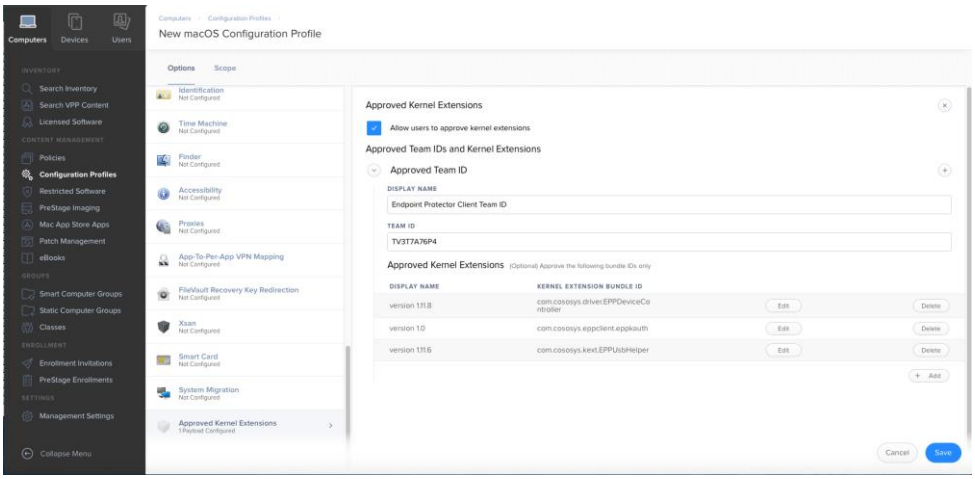


3. Under the **Approved Kernel Extension** tab, press the **Configure** button

4. Fill in the requested information, as follows:

   Endpoint Protector Client Team ID: TV3T7A76P4

   Endpoint Protector Client Bundle IDs:
   com.cososys.driver.EPPDeviceController | version 1.11.8
   com.cososys.eppclient.eppkauth | version 1.0
   com.cososys.kext.EPPUsbHelper | version 1.11.6



5. Under the **Private Preferences Policy Control** tab, press the **Configure** button

6. Fill in the requested information, as follows:

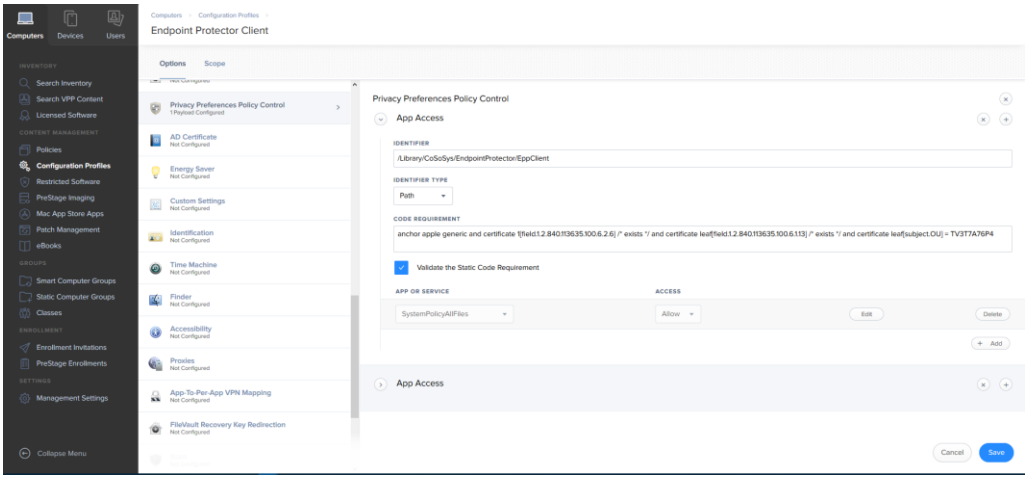
   Endpoint Protector Identifier:
   /Library/CoSoSys/EndpointProtector/EPPClient

   Endpoint Protector Identifier Type: Path

   Endpoint Protector Code Requirement: anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = TV3T7A76P4

   Validate the Static Code Requirement: check it

   Proceed by adding allow access to SystemPolicyAllFiles



6.1 Add new App Access

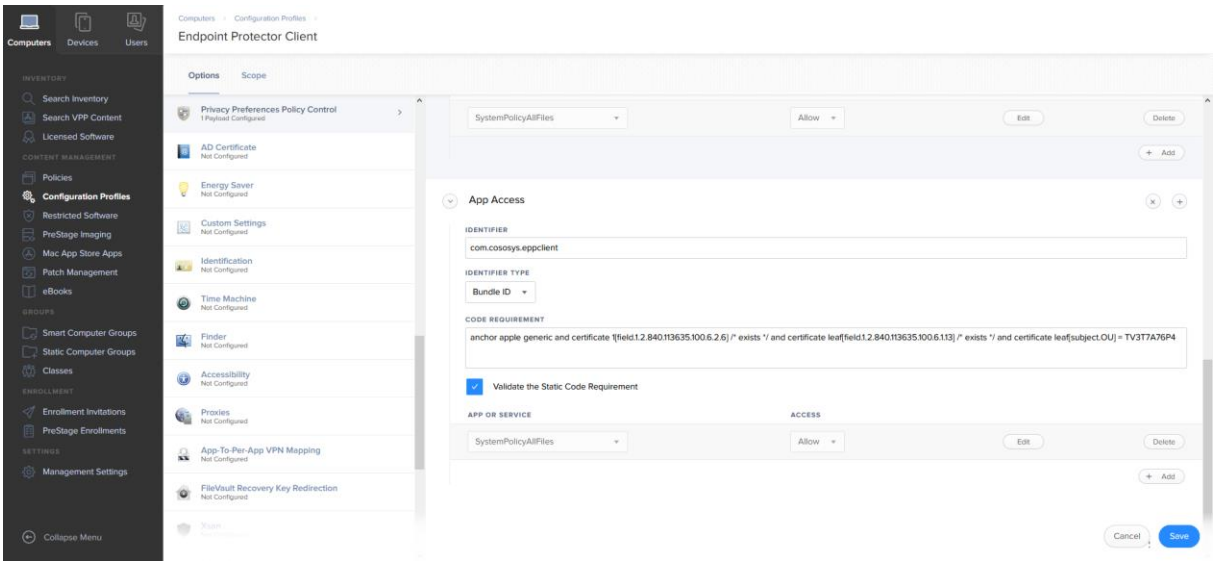
Endpoint Protector Client Identifier: com.cososys.eppclient

Endpoint Protector Client Type: Bundle ID

Endpoint Protector Client Code Requirement: anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = TV3T7A76P4

Validate the Static Code Requirement: check it

Proceed by adding allow access to SystemPolicyAllFiles



6.2 For EasyLock Enforced Encryption, also fill in the following:

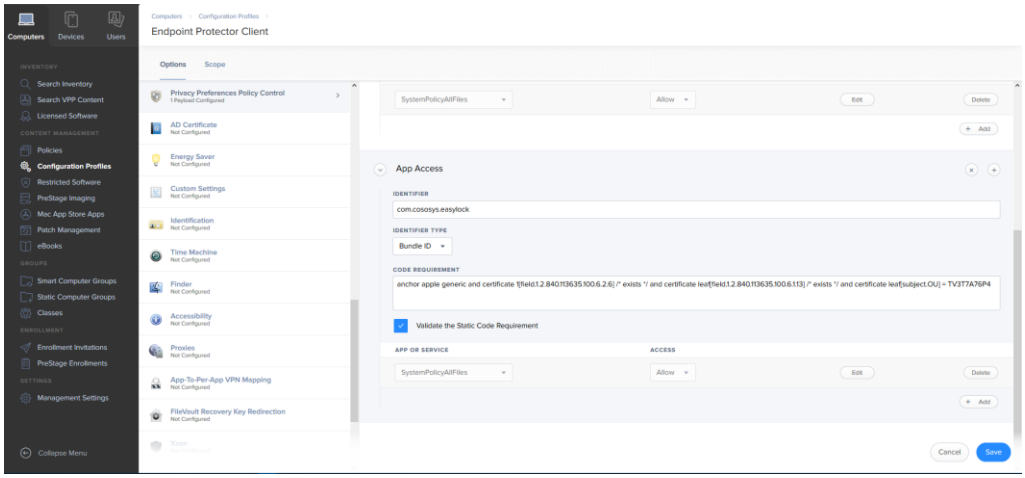
EasyLock Identifier: com.cososys.easylock

EasyLock Identifier Type: Bundle ID

EasyLock Code Requirement: anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = TV3T7A76P4

Validate the Static Code Requirement: check it

Proceed by adding allow access to SystemPolicyAllFiles



7. Assign a scope and wait for the Team ID and Private Preferences Policy Control to be deployed.

After the Team ID and Private Preferences Policy Control have been successfully deployed, you can proceed to the Endpoint Protector Client Deployment described in the following chapter.

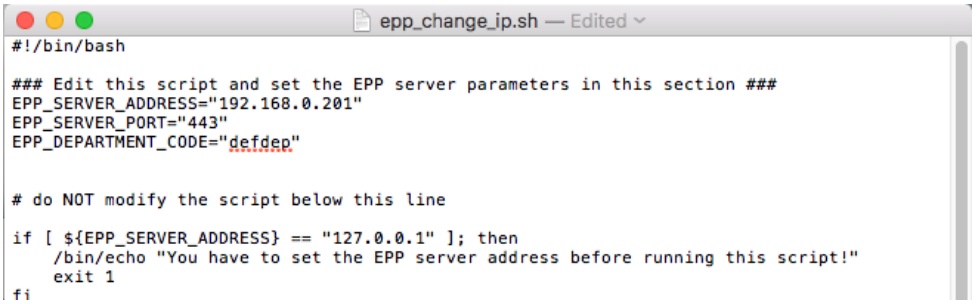
Information

If the Endpoint Protector Client has been previously deployed on the Mac, the above steps are not needed as the KEXT was already approved once.

2. Deployment using Policies and Scripts

Follow the steps described below to deploy the Endpoint Protector Client using JAMF policies:

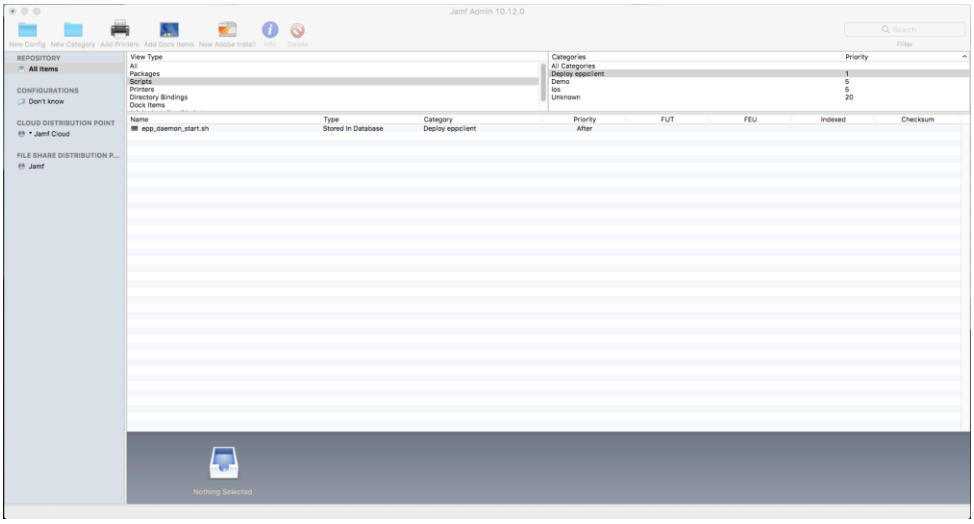
1. With your prefer text editor, open the **epp_change_ip.sh** script, received from Endpoint Protector
2. Add the required Server IP (EPP_SERVER_ADDRESS)



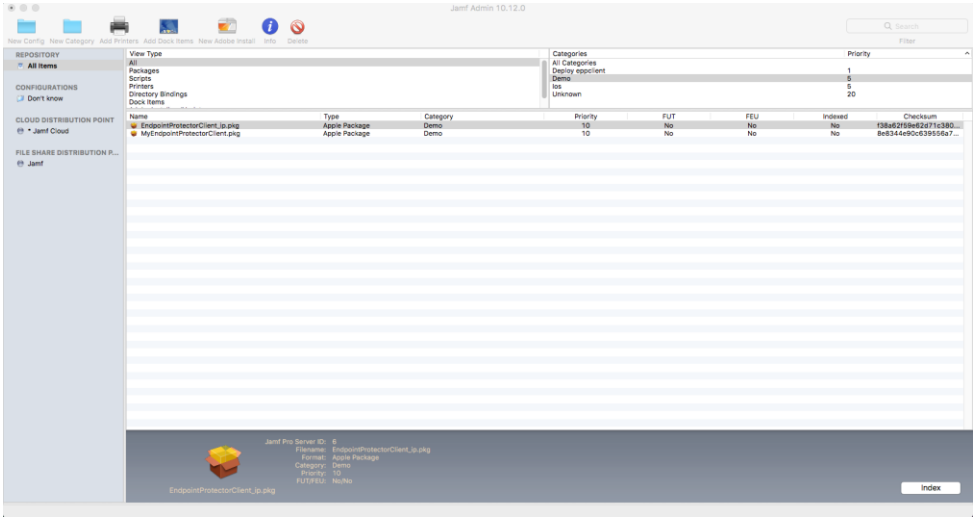
> **Information**
>
> If additional branding is required, the EPP_SERVER_PORT and EPP_DEPARTMET CODE can also be changed.

> **Note**
>
> Some text editors might change the formatting (e.g.: replacing commas “”, etc.). Make sure these are not altered. One way would be to use the Terminal Editor as the text editor.

3. Copy the modified **epp_change_ip.sh** into JAMF Admin

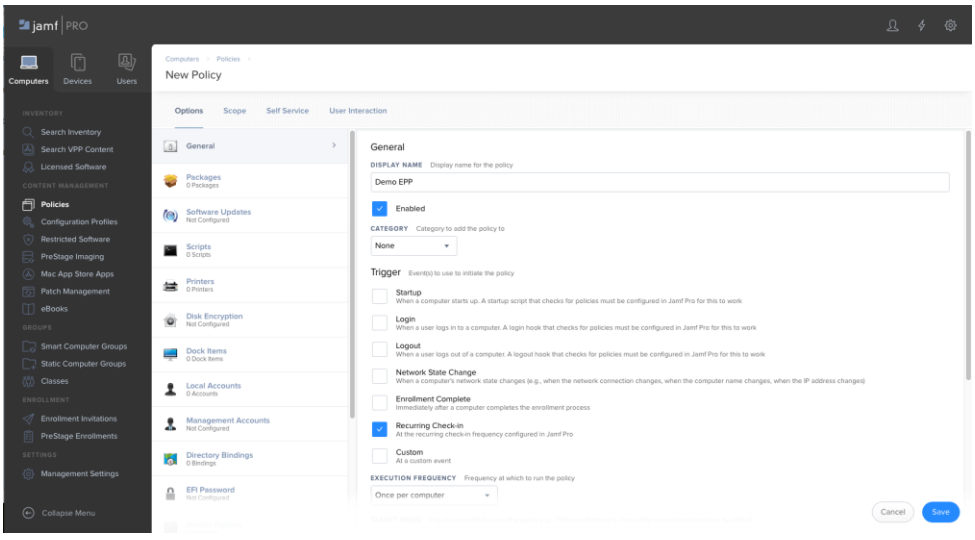


4. Copy the **EndpointProtector.pkg** into JAMF Admin

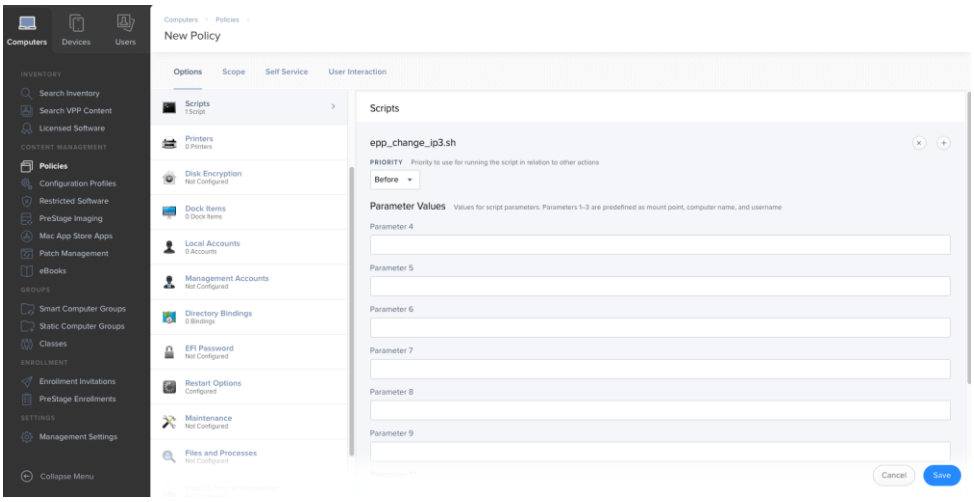


5. Login to JAMF Pro and go to **Computer > Policies**

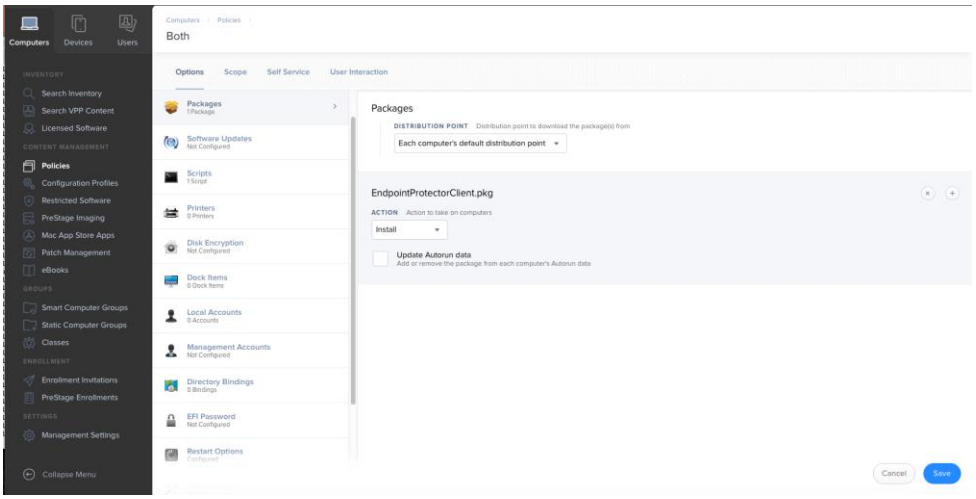
6. Create a new policy, add a name and make sure **Recurring check-in** is checked



7. In the **Scripts > Configure Scripts** section, add the **epp_change_ip.sh** script. Make sure the **Priority** is set to **Before** as the script need to be installed before the next step.



8. On the same policy, in the **Packages > Configure Packages** section, add the **EPPClient.pkg**



9. Add a scope to the policy and save it

10. Check that the Endpoint Protector Client has been deployed correctly and the Server-Client communication and policies work as expected. This means the endpoint appears in the **List of Computes** within the Endpoint Protector UI and that the Endpoint Protector Client is displayed in the menu bar.

3. Disclaimer

Endpoint Protector Appliance does not communicate outside of your network except with liveupdate.endpointprotector.com and cloud.endpointprotector.com.

Endpoint Protector does not contain malware software and does not send at any time any of your private information (if Automatic Live Update Reporting is DISABLED).

Each Endpoint Protector Server has the default SSH Protocol (22) open for Support Interventions and there is one (1) System Account enabled (epproot) protected with a password. The SSH Service can be disabled at customers' request.

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.