

## **JAMF** Deployment Guide



Version 4.0

Date 05.05.2023

### Table of Contents

Document Changelog	3
1. Introduction	4
2. Creating the Configuration Profile	5
2.1. General settings	5
2.2. Certificate settings	6
2.3. Privacy Preferences Policy Control settings	s 9
2.4. Allow EppNotifier settings	10
2.5. EasyLock Enforced Encryption settings	11
2.6. System Extension settings	12
2.6.1. Allow System Extension	12
2.6.2. Removable System Extensions	13
2.6.3. Managed Login Items	13
2.7. VPN settings	14
2.8. Notifications settings	16
2.9. Scope	17
<ol><li>Uploading the Script and Package</li></ol>	18
4. Creating the Policy	20
5. Disclaimer	23

## **Document Changelog**

Version	Date	Notes
1.0	2019	The document was created.
2.0	16.02.2022	The document was updated.
3.0	11.11.2022	Updated the VPN settings section, added the Document Changelog section and applied the current template.
4.0	05.05.2023	

## 1. Introduction

Since the release of macOS 11.0 (Big Sur), significant changes have been made regarding system extensions that now allow deploying endpoint security solutions without kernel-level access.

This affects the deployment of the Endpoint Protector Client on all Macs that are using 11.0 operating systems or later. Companies can use third-party deployment tools such as JAMF as well as other alternatives.

This user manual aims to explain how to use JAMF in order to deploy Endpoint Protector on multiple endpoints.

## 2. Creating the Configuration Profile

In order to use JAMF, first, you need to create a new configuration profile.

To do so, follow these steps:

- 1. Open the JAMF Pro account and log in using your credentials;
- 2. In your **JAMF** account, from the main navigation bar click **Computer**, and then from the left sidebar menu, select **Configuration Profiles**;
- 3. To create a new configuration profile, in the upper right, above the table with available configuration profiles, click **+New**.

🌌 jamf 🛛 PRO						ይ \$ ‡
Computers Devices Users	Computers ← Configuration	n Profiles				
INVENTORY	C Q Filter Pr	- 33 of <b>33</b>		+	New [] Uploa	d (Ⅲ 🖽
Search Inventory	NAME	LOGS	COMPLETED	PENDING	FAILED	SCOPE
CONTENT MANAGEMENT	<ul> <li>No category as</li> </ul>	signed				
Policies	Profile 1	View	0	0	0	No scope defined
Restricted Software	Profile 2	View	0	0	0	No scope defined

On the **New macOS Configuration Profile** section, you can manage profile settings and select the devices and users to which you want to deploy the profile.

Note: Click Save only once you have managed all settings and the profile scope.

#### 2.1. General settings

On the default **General** section, enter the following information:

- Name enter a name to use for this configuration profile
- **Description** (optional) add a description that details the purpose of the configuration profile

You can continue with the default settings for the **category**, **level**, and **distribution method** fields.

🞜 jamf   PRO		
Computers Devices Users	Computers : Configuration Profile ← New macOS Config	uration Profile
	Options Scope	
Search Inventory Search Volume Content Licensed Software	® <sub>o</sub> General	General Name Display name of the profile
CONTENT MANAGEMENT	Passcode Not configured	[Required] Description Brief explanation of the content or purpose of the profile
Configuration Profiles Restricted Software	Retwork Not configured	
PreStage Imaging     Mac App Store Apps	VPN Not configured	Category Category to add the profile to None
eBooks	DNS Settings Not configured	Level Level at which to apply the profile
Smart Computer Groups	BNS Proxy Not configured	Distribution Method Method to use for distributing the profile
<u>ំពំំំំ</u> Classes	- Content Caching	

#### 2.2. Certificate settings

You will add the Client CA Certificate in .cer format on the Certificate settings section.

**Note**: This step is not required if you are not using Deep Package Inspection. To continue the process, go to the **Privacy Preferences Policy Control** section.

1. Log in to **Endpoint Protector Server**, go to the **System Configuration** section, and then select **System Settings**;

2. On the **Default System Settings** section, enable **Deep Packet Inspection Certificate** and then download **Client CA Certificate** – the downloaded .zip file contains the .cer and .crt client certifications.

ENDPOINT PROTECTOR		s Q A Velcome
Denylists and Allowlists	« E Default System Settings	
inforced Encryption	Log Settings	
Offline Temporary Password	Maximum number of rows for CSV export (Million):	1.0
Reports and Analysis	Content Aware Protection - Report all sensitive information	on
Alerts	Report all sensitive information :	Off
Directory Services	Virtual Desktop Clones	
E Appliance	Virtual Desktop Clones Support:	
System Maintenance	Deep Packet Inspection Certificate	
System Configuration	Deep Packet Inspection Certificate download :	On
Client Software Client Software Upgrade	Download Client CA Certificate	
Client Uninstall	Server Certificate Stack	
Administrators Groups	Use FQDN in subject :	Off
System Departments System Security	Regenerate Server Certificate Stack :	Regenerate
<u>System Settings</u> System Licensing	Single Sign On	
System Parameters	Enable Single Sign On Login:	
Support	Active Directory Authentication	

- 3. Go to JAMF, the Certificate section, and click Configure;
- 4. Enter a **Certificate name** and then select and upload the downloaded **Client CA Certificate** in **.cer** format.

┛ jamf 🛛 PRO		
Computers Devices Users	Computers : Configuration Profiles ← New macOS Configuration Profile	
INVENTORY	Options Scope	
Search Inventory     Search Volume Content	Certificate 1 payload configured Certificate	
CONTENT MANAGEMENT	Certificate Transparency Not configured Client Certificate Name Display name of the certificate credential Client Certificate	
Policies     Configuration Profiles     Restricted Software	E SCEP Not configured Upload Certificate	
PreStage Imaging Mac App Store Apps	Directory Filename cacert.cer	
Patch Management	Software Update Not configured Expiration Date	
Smart Computer Groups	i and a second	

#### 2.3. Privacy Preferences Policy Control settings

On the **Privacy Preferences Policy Control** section, click **Configure** and then enter the following information:

- Identifier com.cososys.eppclient
- Identifier Type go with the default Bundle ID type
- 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

**Note**: Use the **Terminal Editor** to verify there are no formatting alterations before executing this command line.

- Select the Validate the Static Code Requirement checkbox
- Click Add and Save to allow access to SystemPolicyAllFiles and Accessibility services.

┛ jamf   PRO		요 🕴 🕸
Computers Devices Users	Computers : Configuration Profiles ← New macOS Configura	ation Profile
	Options Scope	
Search Inventory  Search Volume Content  Licensed Software	Privacy Preferences Policy Control 1 payload configured	Privacy Preferences Policy Control     × <ul> <li>App Access</li> <li>+</li> </ul>
CONTENT MANAGEMENT	AD Certificate Not configured	Identifier
Restricted Software	Q: Energy Saver Not configured	Identifier Type
Mac App Store Apps     Patch Management     Sector	Application & Custom Settings ~ Not configured	Code Requirement anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
GROUPS	[A∓] Identification Not configured	leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[ <u>subject.OU</u> ] = <u>TV3T7A76P4</u>
Classes	D Time Machine Not configured	APP OR SERVICE ACCESS
ENROLLMENT	Finder Not configured	SystemPolicyAllFlies  Allow Edit Delete
PreStage Enrollments	Accessibility	Accessibility

#### 2.4. Allow EppNotifier settings

On the **Privacy Preferences Policy Control** section, click the **+** icon to add a new policy and then enter the following information:

- Identifier com.cososys.eppclient.notifier
- Identifier Type go with the default Bundle ID type
- 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

**Note**: Use the **Terminal Editor** to verify there are no formatting alterations before executing this command line.

• Select the Validate the Static Code Requirement checkbox

<ul> <li>Click Add and then Save to allow access to Accessibility set</li> </ul>	ervices.
--	----------

🗖 jamf   PRO		<u>£</u> \$ \$
Computers Devices Users	Computers : Configuration Profiles ← New macOS Configuration	ration Profile
	Options Scope	
Search Inventory     Search Volume Content     Licensed Software	Privacy Preferences Policy Control 1 payload configured	Privacy Preferences Policy Control
CONTENT MANAGEMENT	AD Certificate Not configured	Identifier
	C Energy Saver	com.cososys.eppclient.notifier Identifier Type Ruadia ID, a
Mac App Store Apps     Patch Management     eBooks	Application & Custom Settings ~ Not configured	Code Requirement anchor apple generic and certificate [[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and
GROUPS	a≡ Identification Not configured	certificate leaf <u>[subject.QU]</u> = <u>TV3T7A76P4</u>
C☐ Static Computer Groups	Time Machine Not configured	APP OR SERVICE ACCESS
ENROLLMENT	Finder Not configured	Accessibility Allow Edit Delete

#### 2.5. EasyLock Enforced Encryption settings

On the **Privacy Preferences Policy Control** section, click the **+** icon to add a new policy and then enter the following information:

- Identifier com.cososys.easylock
- Identifier Type go with the default Bundle ID type
- 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

**Note**: Use the **Terminal Editor** to verify there are no formatting alterations before executing this command line.

- Select the Validate the Static Code Requirement checkbox
- Click Add and then Save to allow access to SystemPolicyAllFiles and Accessibility services

🏜 jamf 🛛 PRO								ম	4 ŵ
Computers Devices	L) Co Users ←	mputers : Configuration Profiles	s uration l	Profile					
		Options Scope							
Search Inventory Search Volume C	Content 👳	Privacy Preferences Policy Control 1 payload configured	$\odot$	App Access					× +
CONTENT MANAGEMEN		AD Certificate Not configured	_	Identifier com.cososys.easylock					
Configuration Pr     Restricted Softwa     PreStage Imaging	rofiles are Q:	Energy Saver Not configured		Bundle ID 🔻					
Mac App Store Ap Patch Manageme	pps ent	Application & Custom Settings Not configured		Code Requirement anchor apple generic an leaf[field.1.2.840.113635.1	nd certificate 1(1 100.6.1.13) /* exi	field.1.2.840.113635.10 sts */ and certificate	00.6.2.6] /* exists */ a leaf[ <u>subject.OU]</u> = <u>TV</u>	nd certificate '3T7A76P4	
GROUPS	Groups	Identification Not configured		Validate the Static C	ode Requirem	ent			
Classes	Groups	Time Machine Not configured		SystemPolicyAllFiles	×	Allow	•	Edit	Delete
ENROLLMENT	tions	Finder Not configured		Accessibility		Allow		Edit	Delete

#### 2.6. System Extension settings

#### 2.6.1. Allow System Extension

On the System Extension section, click Configure and then enter the following information:

- Display Name (optional) enter a name to use for this configuration
- System Extension Type select Allow System Extension type
- Team Identifier TV3T7A76P4
- Allowed System Extensions click Add, enter com.cososys.eppclient, and then Save the changes

🗖 jamf 🛛 PRO			<u>r</u> .	\$ \$
Computers Devices Users	Computers : Configuration Profiles ← New macOS Configuration P	rofile		
INVENTORY	Options Scope			
<ul> <li>Search Inventory</li> <li>Search Volume Content</li> </ul>	Not configured	m Extensions		×
CONTENT MANAGEMENT	Xsan Not configured	allow users to approve system extensions		
Policies	Smart Card     Not configured	Allowed Team IDs and System Extensions		+
Restricted Software	System Migration	[Optional]		
Mac App Store Apps     Patch Management	Approved Kernel	System Extension Types Allowed System Extensions		
eBooks	Extensions Not configured	Team Identifier TV3T7A76P4		
Smart Computer Groups	Associated Domains Not configured	ALLOWED SYSTEM EXTENSIONS		
Static Computer Groups	- Extensions	com.cososys.eppclient Edit	Delete	

**Note**: For operating systems lower than macOS 11 (Big Sur), manage settings from the **Approved Kernel Extensions** section instead of System Extensions. Define the **Team ID** (enter **TV3T7A76P4**) and proceed to the next step.

#### 2.6.2. Removable System Extensions

On the **System Extension** section, click the **+** icon to add a new policy that will allow removing system extensions without a pop-up, and then enter the following information:

- Display Name (optional) enter a name to use for this configuration
- System Extension Type select Removable System Extensions type
- Team Identifier TV3T7A76P4
- Allowed System Extensions click Add, enter com.cososys.eppclient, and then Save the changes

Note: This setting will be applied starting with MacOS 12 version (Monterey).

┛ jamf 🛛 PRO			<u>}</u> 4 @
Computers Devices Users	Computers : Configuration Profiles ← New macOS Configuration Profile		
INVENTORY	Options Scope		
<ul> <li>Search Inventory</li> <li>Search Volume Content</li> </ul>	San Allowed Team IDs and S	System Extensions	× +
Licensed Software	Smart Card     Not configured		
Policies           Policies	System Migration Not configured Removable System Extension	ns 🔻	
Restricted Software     PreStage Imaging     Mac App Store Apps	Approved Kernel Extensions Not configured		
Patch Management     eBooks	Associated Domains     Not configured	Edit	Delete

#### 2.6.3. Managed Login Items

Administrators can quickly disable Endpoint Protector Items in JAMF Configuration Profiles with Ventura's (macOS 13) new capability. This can be accomplished by taking the following steps:

- 1. Log in to your JAMF account.
- 2. Click "Computer" from the main navigation bar.
- 3. Select "Configuration Profiles" from the sidebar menu on the left.
- 4. Click "New" in the upper right-hand corner.
- 5. On the left, under the "Options" box, select "Managed Logged In Items."

Endpoint Protector Items can be simply disabled in your JAMF Configuration Profiles from here. Simply uncheck the box next to the Endpoint Protector Item(s) you want to disable, and then click "Save" to save your changes.

**Note**: Disabling Endpoint Protector Items may have an impact on the security of your system. Only disable these items if you are positive it is essential and you have taken every precaution necessary to keep your system secure.

#### 2.7. VPN settings

**Note**: This step is not required if you are not using **VPN** services. To continue the process, go to the **<u>Scope</u>** section.

On the VPN section, click Configure and then enter the following information:

- Connection Name enter a connection name that will be displayed on the device
- VPN Type select Per-App VPN type
- Per-App VPN Connection Type select Custom SSL connection type
- Identifier com.cososys.eppclient.daemon
- Server localhost
- Provider Bundle Identifier com.cososys.eppclient.daemon
- Provider Type select App-proxy type
- Select the Include All Networks checkbox
- Provider Designated 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

**Note**: Use the **Terminal Editor** to verify there are no formatting alterations before executing this command line.

• Select the Prohibit users from disabling on-demand VPN settings checkbox

#### CoSoSys Confidential. Copyright © 2004 - 2023 CoSoSys SRL and its licensors. All rights reserved.

🗖 jamf 🛛 PRO		<u>\</u> \$ @
Computers Devices Users	Computers : Configuration Profiles ← New macOS Configuration	ion Profile
	Options Scope	
Search Inventory Search Volume Content Licensed Software	VPN 1 payload configured	Connection Name Display name of the connection (displayed on the device) VPN Connection
CONTENT MANAGEMENT	DNS Settings Not configured	VPN Type The type of VPN connection to configure Per-App VPN
Configuration Profiles     Restricted Software	BNS Proxy Not configured	Per-App VPN Connection Type The type of connection enabled by this policy. L2TP and PPTP are not supported.
PreStage Imaging Mac App Store Apps	Content Caching Not configured	Listom SSL
Patch Management     eBooks	Certificate 1 payload configured	com.cososys.eppclient.daemon Server Hostname or IP address for server
GROUPS	O Certificate Transparency Not configured	Iocalhost           Account User account for authenticating the connection
Classes	SCEP Not configured	Provider Bundle Identifier Bundle Identifier for the selected VPN provider
Enrollment Invitations	Directory	com.cososys.eppclient.daemon



#### 2.8. Notifications settings

Note: This step is optional. To continue the process, go to the <u>Scope</u> section.

On the Notifications section, click Configure and then enter the following information:

- App Name EppNotifier
- Bundle ID com.cososys.eppclient.notifier
- Toggle the switch to include the settings type and then disable/enable to manage each notification option

🌌 jamf 🛛 PRO				ይ		
Computers Devices Users	Computers : Configuration Profiles ← New macOS Config	uration Profile				
INVENTORY  Search Inventory  Search Volume Content  Licensed Software	Notifications     1 payload configured	App Name EppNotifier	Bundle ID com.cososys.eppclient.notifier			-
CONTENT MANAGEMENT	Printing Not configured	Settings	Required		Include	
Configuration Profiles	ネ Parental Controls Not configured	Critical Alerts Critical Alerts can ignore Do Not Disturb and ringer settings for this app	[	Disable Enable		
PreStage Imaging Mac App Store Apps	Security and Privacy Not configured	Notifications Allow notifications to be displayed for this app	[	Disable Enable		
Patch Management     eBooks     GROUPS	Privacy Preferences Policy Control 1 payload configured	Banner alert type Banner alerts appear in the upper-right corner. Temporary banners clea Temporary v	ar automatically and persistent banners require the end user to take action before clea	ring.		
Smart Computer Groups  Static Computer Groups  Classes	AD Certificate Not configured	Notifications on Lock screen Notifications in Notification Center		Hide Display		
ENROLLMENT	Q: Energy Saver Not configured	Badge app icon		Hide Display		
PreStage Enrollments	Application & Custom Settings ~ Not configured	Play sound for notifications	(	Disable Enable	) cel 5	(E) Save

#### 2.9. Scope

Once you manage all settings, go to the Scope tab and select the devices and users to deploy the new profile.

Click **Save** to apply all settings to the new configuration profile.

**Note**: To confirm that the new configuration profile is saved successfully, reboot your computer at this point.

🛎 jamf   PRO			ይ 🖇 🕸
Computers Devices Users	Computers : Configuration Profiles ← New macOS Configuration Profil	e	
	Options Scope		
Search Volume Content	Targets	Limitations	Exclusions
CONTENT MANAGEMENT	Target Computers Computers to assign the profile to	Target Users Users to distribute the profile to	
Configuration Profiles  Restricted Software	Specific Computers 👻	Specific Users 👻	
PreStage Imaging     Mac App Store Apps	Selected Deployment Targets		+ Add
Patch Management	TARGET	TYPE	
GROUPS	No Targets		

# 3.Uploading the Script and Package

To deploy the Endpoint Protector Client, you need to upload the **EndpointProtector.pkg** package and **epp\_change\_ip.sh** script.

#### Important: You need to request the script at support@endpointprotector.com.

To upload the script and package, follow these steps:

- 1. In your **JAMF** account, from the main navigation bar, click **Computer**, and then from the left sidebar menu, select **Management Settings**;
- From the Computer Management section, select Scripts and then, in the upper right, click + New;
- On the General section, add a name for the profile, and then select the Script tab and add the epp\_change\_ip.sh script;
- 4. Add your Server IP to the EPP\_SERVER\_ADDRESS field;

**Note**: You can edit the **EPP\_DEPARTMET CODE** and **EPP\_SERVER\_PORT** fields to deploy the Endpoint Protector Client on specific departments or custom ports.

🗖 jamf 🛛 PRO				Ŋ	\$	ŝ
Computers Devices Users	Settings : Computer Management → Scripts ← New Script					
VERSION 10.35.0-11640197529 MANAGED Computers: <b>5</b> Mobile Devices: <b>0</b> UNMANAGED Computers: <b>0</b> Mobile Devices: <b>0</b>	General Script Options Limitations Script Contents Default Mode  Default Theme  #!/bin/bash ### Edit this script and set the EPP server parameters in th EPP_SERVER_ADDRESS="192.168.0.201" 5 EPP_SERVER_PORT="443" 6 EPP_DEPARTMENT_CODE="defdep"	-T his sec	T.	·	Comma	nds

- From the Computer Management section, select Package and then, in the upper right, click + New;
- 6. On the **General** tab, add a name and then upload the package **EndpointProtector.pkg**.

🛂 jamf 🛛 PRO		ይ	4	ŝ
Computers Devices Users	Settings : Computer Management → Packages ← New Package			
VERSION 10.35.0-t1640197529	General Options Limitations			
MANAGED Computers: 5 Mobile Devices: 0	Display Name Display name for the package EndpointProtector.pkg Category Category to add the package to			
Computers: 0 Mobile Devices: 0	None  Package File			
	EndpointProtector.pkg Upload Package File			

## 4. Creating the Policy

Once the script and package are successfully uploaded, you need to create a new JAMF policy.

To create the new policy, follow these steps:

1. In your **JAMF** account, from the main navigation bar, click **Computer**, from the left sidebar menu, select **Policies**, and then click **+ New**;

🖆 jamf 🛛 PRO			ſ	2 4 🕸
Computers Devices Users	Computers ← Policies			
	C Filter Pc 1-46 of 46		+ New	
Search Inventory	NAME	FREQUENCY	TRIGGER	SCOPE
CONTENT MANAGEMENT				
Policies	<ul> <li>Policy 1</li> </ul>	Once per computer	Check-in	No scope defined
Restricted Software	> Policy 2	Once per computer	Check-in	No scope defined

- 2. On the default **General** section, enter the following information:
  - Display Name enter the name to use for this policy
  - Select the Recurring Check-in checkbox

#### CoSoSys Confidential. Copyright © 2004 - 2023 CoSoSys SRL and its licensors. All rights reserved.

🗖 jamf 🛛 PRO	£ ·	<b>វ</b> ĝ
Computers Devices Users	Computers : Policies ← New Policy	
INVENTORY	Options Scope Self Service User Interaction	
Search Inventory	General > General	
CONTENT MANAGEMENT	Display Name         Display name for the policy           Packages         Policy name	
Policies	Software Updates Not Configured Enabled	
Restricted Software	Category Category to add the policy to Scripts O Scripts None	
Mac App Store Apps     Patch Management	Printers O Printers O Printers Startup	
eBooks	When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work     Disk Encryption     Not Configured     When a user logs in to a computer. A login event that checks for policies must be configured in Jamf Pro for this to work	
Smart Computer Groups	Dock Items 0 Dock Items 0 Dock Items 0 Dock Items	?S,
Classes	Local Accounts     D Accounts     Enrollment Complete     Immediately after a computer completes the enrollment process	
Enrollment Invitations	Management Accounts Not Configured Act the recurring Check-in At the recurring check-in frequency configured in Jamf Pro	

- 3. On the Scripts section, click Configure and then enter the following information:
  - Add the **epp\_change\_ip.sh** script
  - Priority set priority to Before, as the script needs to be installed before the next step

lamf   PRO	L \$ {	ŝ
Computers Devices Users Computers Policies ← New Policy		
INVENTORY Options Scope Self Service	User Interaction	
Search Inventory       Search Volume Content	Scripts	
CONTENT MANAGEMENT	epp_change_ip.sh	
Policies     Disk Encryption     Not Configuration Profiles	Priority Priority to use for running the script in relation to other actions Before	
Restricted Software       PreStage Imaging   Dock Items	Parameter Values Values for script parameters. Parameters 1–3 are predefined as mount point, computer name, and username	
Mac App Store Apps     Local Accounts     O Accounts		
eBooks     Management     Accounts	Parameter 5	

4. On the **Packages** section, click **Configure** and then add the package **EndpointProtector.pkg**;

CoSoSys Confidential. Copyright © 2004 - 2023 CoSoSys SRL and its licensors. All rights reserved.

🗖 jamf   PRO		ম	\$	ŝ
Computers Devices Users Computers : Policies ← New Policy				
INVENTORY Options Scope Self Serv	vice User Interaction			
Q       Search Inventory         ▲       Search Volume Content         ↓       Licensed Software         ♦       Packages         ↓       Packages	Packages Distribution Point Distribution point to download the package(s) from Each computer's default distribution point			
Policies Software Updates Not Configuration Profiles	EndpointProtector.pkg		×	(+)
Restricted Software       PreStage Imaging   Scripts Script	Action Action to take on computers			
Mac App Store Apps     Printers     O Printers	Install			
eBooks Disk Encryption	Add or remove the package from each computer's Autorun data			

- 5. Go to the Scope tab and add the devices and users to apply the new policy;
- 🗾 jamf 🛛 PRO <u>ئې</u> Computers : Policies 100  $\left[ \right]$ ← New Policy Devices Computers Self Service Options Scope User Interaction Q Search Inventory Search Volume Content Limitations Exclusions Targets Licensed Software **Target Computers** Target Users Computers to deploy the policy to Users to deploy the policy to Policies Specific Computers v Specific Users v Configuration Profiles Restricted Software PreStage Imaging Selected Deployment Targets + Add Mac App Store Apps Patch Management TARGET TYPE eBooks No Targets (E) Save  $\otimes$ Smart Computer Groups Cance Static Computer Groups (🎊 Classes
- 6. Click **Save** to apply all settings to the new policy.

To confirm that the Endpoint Protector Client has been successfully deployed and the Server-Client communication and policies work as expected, you can view the endpoint in the **List of Computers** from the Endpoint Protector UI, and the Endpoint Protector Client is displayed in the menu bar.

## 5. Disclaimer

The information in this document is provided on an "AS IS" basis. To the maximum extent permitted by law, CoSoSys disclaims all liability, as well as any and all representations and warranties, whether express or implied, including but not limited to fitness for a particular purpose, title, non-infringement, merchantability, interoperability, and performance, in relation to this document. Nothing herein shall be deemed to constitute any warranty, representation, or commitment in addition to those expressly provided in the terms and conditions that apply to the customer's use of Endpoint Protector.

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.

Copyright © 2004 – 2023 CoSoSys SRL and its licensors. Endpoint Protector is a trademark of CoSoSys SRL. All rights reserved. Macintosh, Mac OS X, macOS are trademarks of Apple Corporation. All other names and trademarks are the property of their respective owners.

Confidential. © CoSoSys 2023. Not to be shared without the express written permission of CoSoSys

EndpointProtector.com