

JAMF Deployment User Manual Version 5.2.0.9

User Manual



Table of Contents

1.Introduction	.1
2. Deployment using Policies and Scripts	5
3.Disclaimer	8

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

Computers Devices Users	Computers Configuration Profiles New macOS Configuration Profile	
Devices Desice UNINITIAL Search Invertory Search Invertory Search Invertory Search Invertory Search Invertory Uninitial Search Invertory Search Invertory Search Invertory Restricted Software Pression Inspirat Mac App Store Apps Mac App Store Apps Patch Management Pression Inspirat Store Computer Groups Store Computer Groups Store Computer Groups Store Computer Investrations Encollege Evolveres Store Computer Investrations Encollege Evolveres	Option: Scope Option: Scope Image: Contract Contract Image: Contract Contract Image: Contract Contract Image: Contract </th <th>Canceral MAXE Draphs name of the profile Patho Dana DESCRIPTION That explanation of the content or purpose of the profile DESCRIPTION That explanation of the content or purpose of the profile CATEGORY Contegory to add the profile to Nome * DESCRIPTION METHOD Methods to use for distribution the profile Testical Addomatically * URVEL Level at adds to brange the profile Computer Level *</th>	Canceral MAXE Draphs name of the profile Patho Dana DESCRIPTION That explanation of the content or purpose of the profile DESCRIPTION That explanation of the content or purpose of the profile CATEGORY Contegory to add the profile to Nome * DESCRIPTION METHOD Methods to use for distribution the profile Testical Addomatically * URVEL Level at adds to brange the profile Computer Level *
Collapse Menu	For Compares	Cancel

- 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

🞾 jamf PRO		<u>D</u> \$ @
Computers Devices Users	Computers : Configuration Profiles ← Team ID	
	Options Scope	
	Not configured	Approved Kernel Extensions ×
CONTENT MANAGEMENT	FileVault Recovery Key Redirection Not configured	Allow users to approve kernel extensions Approved Team IDs and Kernel Extensions
Configuration Profiles	Xsan Not configured	Approved Team ID t
PreStage Imaging Mac App Store Apps	Smart Card Not configured	CoSoSys Team ID
Patch Management Books	System Migration Not configured	TV3TTA76P4 Approved Kernel Extensions (pascws) Approve the following bundle Dis only
Smart Computer Groups	Approved Kernel Extensions 1 payload configured	DISPLAY NAME KERNEL EXTENSION BUNDLE No Kernel Extension Bundles
	Associated Domains Not configured	+ Add
	S Extensions Not configured	
	Single Sign-On Extensions Not configured	
	System Extensions Not configured	Cancel Store

- 5. Under the **Private Preferences Policy Control** tab, press the **Configure** button
- 6. Fill in the requested information, as follows:

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 and Accessibility.



6.1 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 and Accessibility.



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:

- 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

800			Jamf Admin 10.1					
	i 🔝 💼 🕧	8						
New Config New Category Add Pr	Inters Add Dock Items New Adobe Install Info			Orthogoday			Partecipe	Filter
CONFIGURATIONS	View type All Packages Scripts Printers			All Categories Deploy eppcient Demo los			1 5 5	~
Don't know	Directory Bindings Dock Items			Unknown			20	
CLOUD DISTRIBUTION POINT	Name epp_daemon_start.sh	Type Stored In Database	Category Deploy eppclient	Priority After	FUT	FEU	Indexed	Checksum
FILE SHARE DISTRIBUTION P Jamf								
	Nothing Selected							

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

800			Jamf Admin	10.12.0				
	i 🔝 💼 🕖	0						
New Config New Category Add Pri REPOSITORY	View Type			Categories			Prior	Filter n
CONFIGURATIONS	All Packages Scripts Printers Directory Bindings Dock Items			Al Categories Deploy eppclient Demo Ios Unknown			1 5 5 20	
CLOUD DISTRIBUTION POINT © - Jam (Coud FILE SHARE DISTRIBUTION P © Jamf	 EndpointProtecturClient () p pig MyEndpointProtecturClient () pig 	Appie Package Appie Package	Demo	10 10	No No	No No	No No	138621596422714280 Be8344e90c639556a7
	Janf Pr EndpointProtectorClient, jp pkg	o Server ID: 6 Filename: EndpointProtectorCl Format: Aggle Package Category: Den Prothy: 10 FUT(FEU: NajNo	iert, jo pkg					Index

- 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



 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.

Computers Devices Users	Computers > Policies > New Policy	
INVENTORY	Options Scope Self Service User In	nteraction
C Search Inventory	Scripts >	Scripts
CONTENT MANAGEMENT	Printers O Printers	epp_change_jp3.sh 🛞 🔶
Policies Configuration Profiles	Disk Encryption Not Configured	PIGORT Process to running the script in relation to other actions Before +
Restricted Software PreStage Imaging Mac Ann Store Anns	Dock Items 0 Dock Items	Parameter Values Values for script parameters. Parameters 1-3 are predefined as mount point, computer name, and usemanne Parameter 4
Patch Management eBooks	Local Accounts Q Accounts	Parameter 5
GROUPS	Management Accounts Nat Configured	Parameter 6
Static Computer Groups	O EFI Password	[]
ENROLLMENT	Restart Options	
PreStage Enrollments	Maintenance	Parameter 8
💮 Management Settings	Files and Processes	Parameter 9
Collapse Menu	A macOS intune integration	Cancel Save

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

Computers Devices Users	Computers / Policies / Both	
INVENTORY Search Inventory Search IVPP Content Search VPP Content Search VPP Content Search VPP Content Contest Macadement To The Search VPP Content Contest Macadement	Options Scope Self Service Us Inclusion Inclusion Inclusion Inclusion Inclusion Software Updates Inclusion Inclusion Inclusion Inclusion Inclusion	er Interaction Packages DISTRIBUTION FOINT Databute points devised the packages) from Each computery default distribution point +
	Pinters Photo Proto Photo Photo	EndpointProtectorCitem pike AcTition - Actine in this on computers Install - Voider Actions data Actions and actions action action action actions Actions actions action action action actions Actions actions action action actions Actions actions action actions Actions actions action actions Actions actions actions actions Actions actions actions Actions actions actions Actions actions actions Actions actions Actions Actions actions Actions
Smart Computer Groups Static Computer Groups Static Computer Groups Classes EHROLLMENT	Local Accounts GAcounts Management Accounts Marcompue	
Enrolment instablers PréStage Enrolments settings Management Settings	ClineCtory Bindings	
		Cancel

- 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.

© 2004 – 2020 CoSoSys Ltd.; Endpoint Protector, My Endpoint Protector, Endpoint Protector Basic and EasyLock are trademarks of CoSoSys Ltd. All rights reserved. Windows is a registered trademark of Microsoft Corporation. Macintosh, Mac OS X, macOS are trademarks of Apple Corporation. All other names and trademarks are property of their respective owners.