

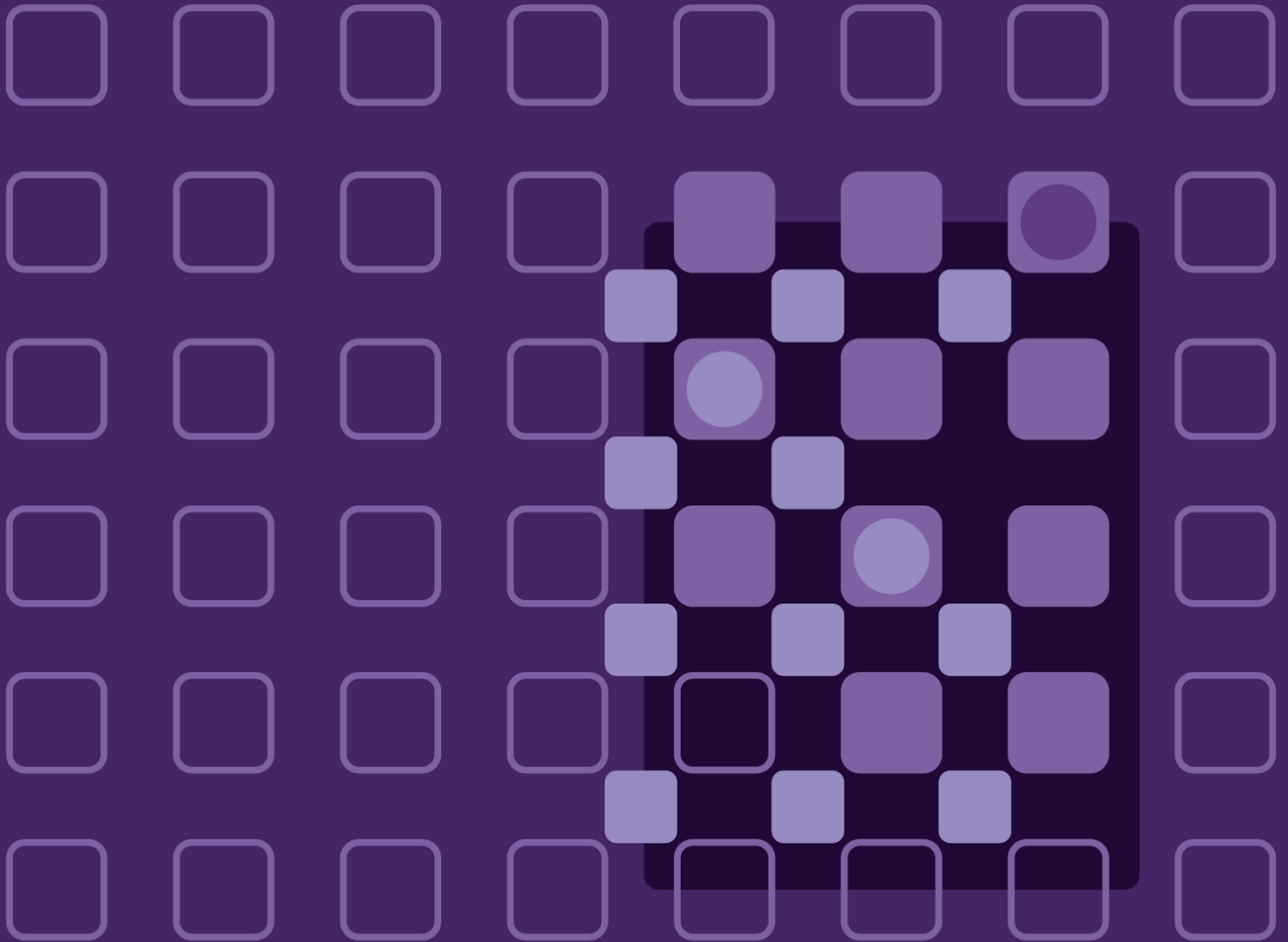


**ENDPOINT
PROTECTOR**

| by CoSoSys

Intune

Deployment Guide



1. Document Changelog

Version	Date	Notes
1.0	02.05.2022	The document was created.
2.0	01.07.2022	The macOS deployment section was added.
3.0	11.11.2022	Updated the macOS deployment section.

2.

Document Changelog	2
1. Introduction	5
2. Windows deployment	6
3. macOS deployment	11
4. Disclaimer	17

3.

1. Introduction

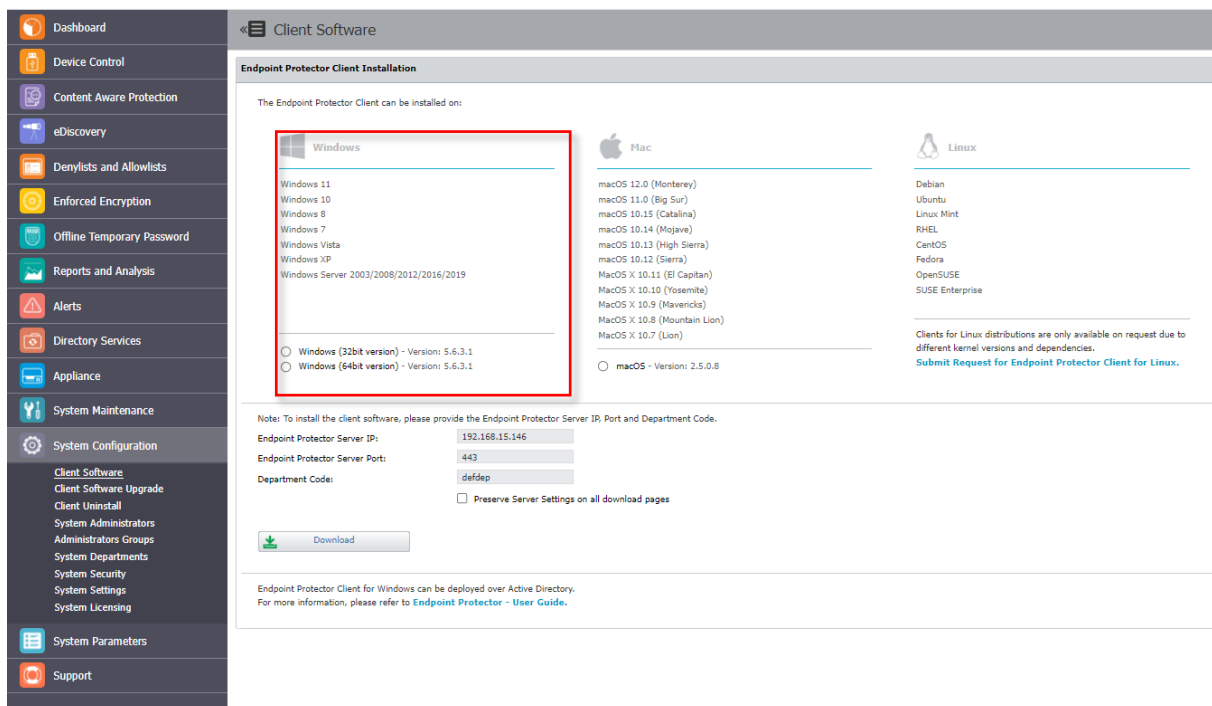
This document describes the steps needed to deploy Endpoint Protector to multiple endpoints using the MSI application in Microsoft Intune.

Microsoft Intune is a cloud-based service focusing on mobile device management (MDM) and mobile application management (MAM).

2. Windows deployment

To deploy the Endpoint Protector MSI package for Windows using Intune, follow these steps:

1. Open and log in to Endpoint Protector;
2. Go to the **System Configuration, Client Software** and download the **Windows Endpoint Protector MSI package**;

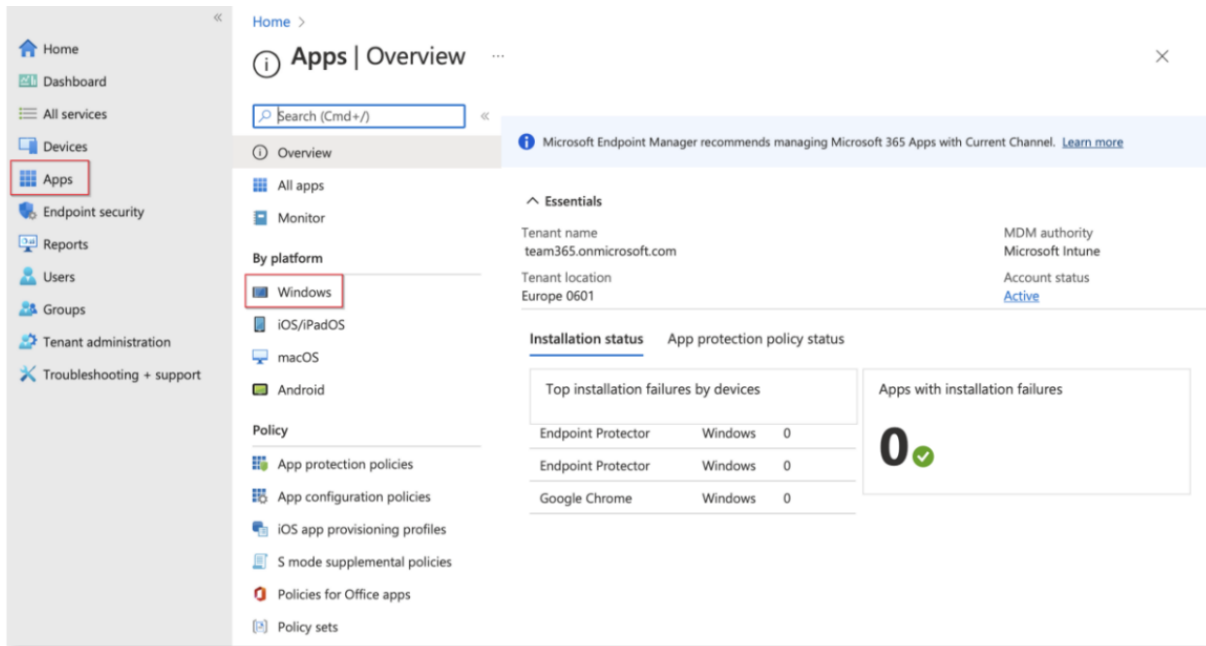


Important: When deploying the .msi package, delete the information contained in the brackets as well as the underscore that precedes it - EPPClientSetup.5.6.3.1_x86_64.msi

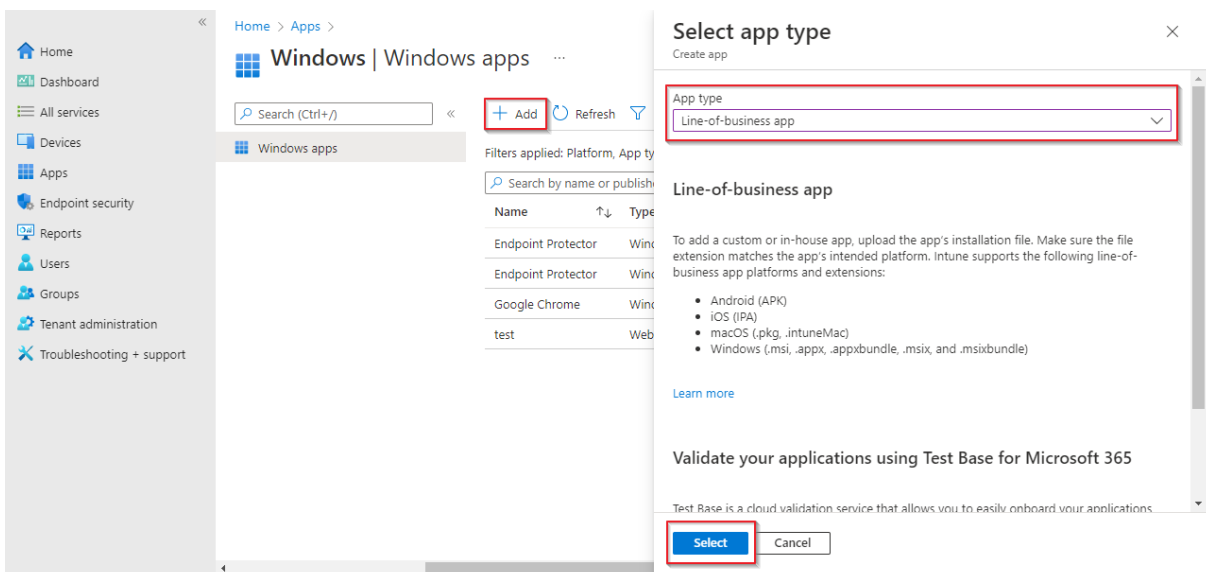
EPPClientSetup.5.6.3.1_x86_64[a=192.168.15.69].msi

3. Go to the **Microsoft Endpoint Manager admin center** and sign in;

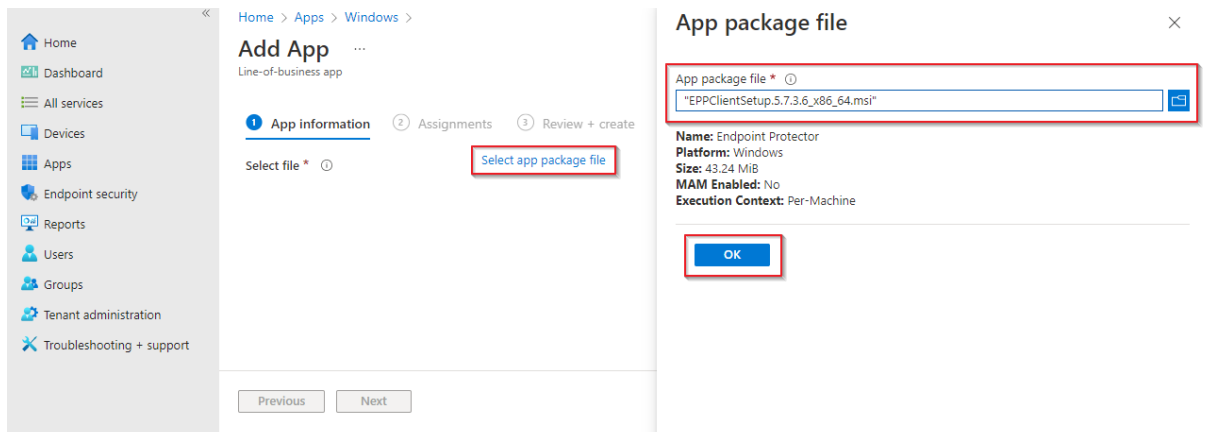
- Go to **Apps** from the left-hand side menu, and on the **Apps Overview** page, select the **Windows** platform;



- On the **Windows App** page, click **Add**, select the **Line of business app** type, and then click **Select**;

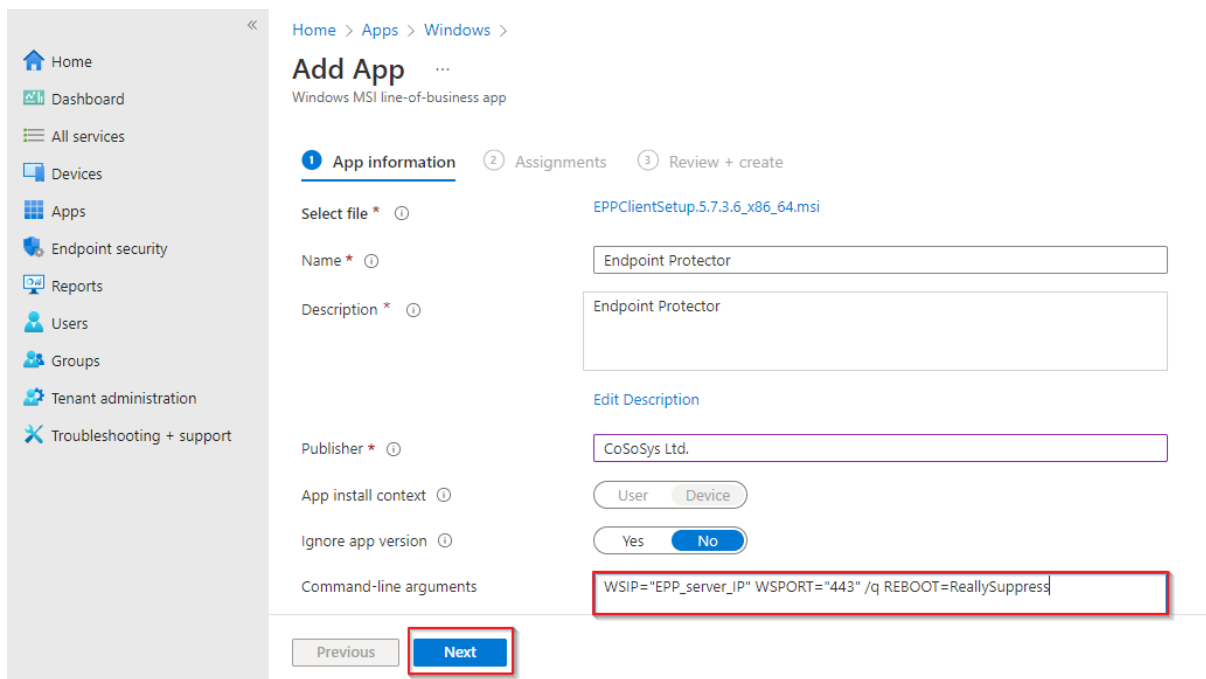


- Click **Select app package file** and from the right-hand side, select the **Endpoint Protector MSI** file and click **OK**;



- On the **App information** page, fill in the mandatory fields and then click **Next**:

- Name** – add Endpoint Protector and optional, the package version (Endpoint Protector 5.7.3.6)
- Description** – click **Edit Description** and add installation details
- Publisher** – add **CoSoSys Ltd.**
- Command-line argument** – add the following command line in the text box
WSIP="EPP_server_IP" WSPORT="443" /q REBOOT=ReallySuppress



- On the **Assignments** page, in the **Requirement** section, select the group for which you want to deploy the Endpoint Protector client and then click **Next**;

Home > Apps > Windows >

Add App

Windows MSI line-of-business app

App information Assignments Review + create

Required

Group mode	Group	Filter mode	Filter	Install Context
Included	All devices	None	None	Device context

+ Add group + Add all users + Add all devices

Available for enrolled devices

Group mode	Group	Filter mode	Filter	Install Context
Included	All users	None	None	Device context

+ Add group + Add all users

Uninstall

Previous **Next**

- On the **Review + create** page, click **Create** - this will start the **Endpoint Protector MSI package** upload.

Home > Apps > Windows >

Add App

Windows MSI line-of-business app

App information Assignments **Review + create**

Summary

App information

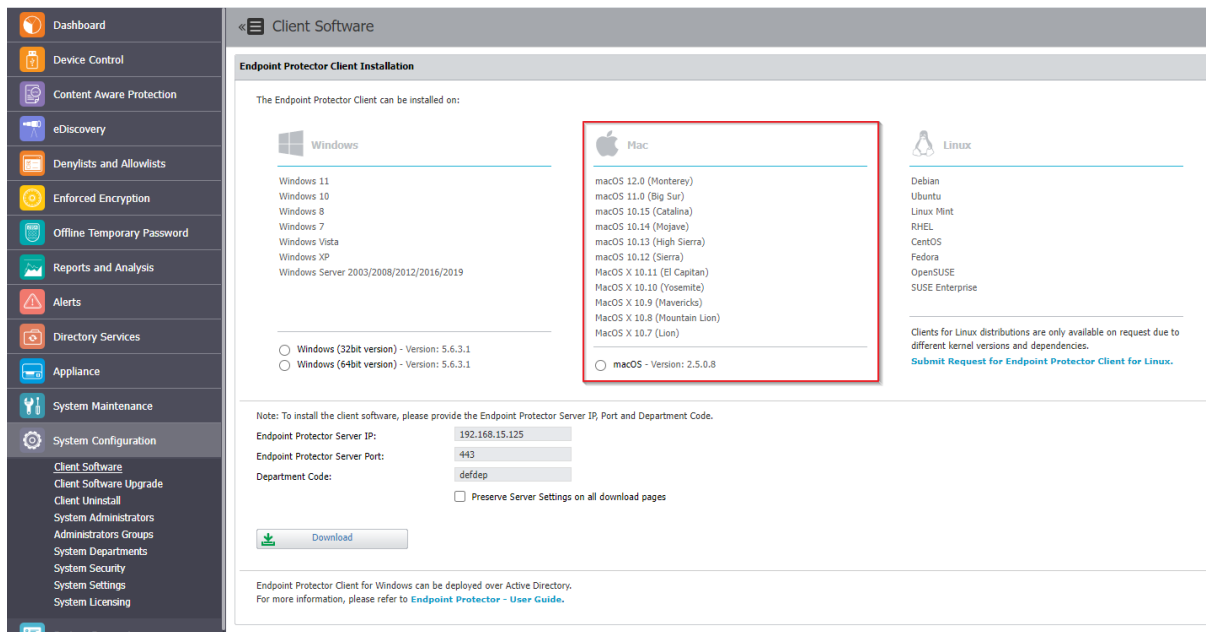
App package file	EPPClientSetup.5.7.3.6_x86_64.msi
Name	Endpoint Protector
Description	Endpoint Protector
Publisher	CoSoSys Ltd.
App install context	Device
Ignore app version	No
Command-line arguments	WSIP="EPP_server_IP" WSPORT="443" /q REBOOT=ReallySuppress
Category	--

Previous **Create**

3. macOS deployment

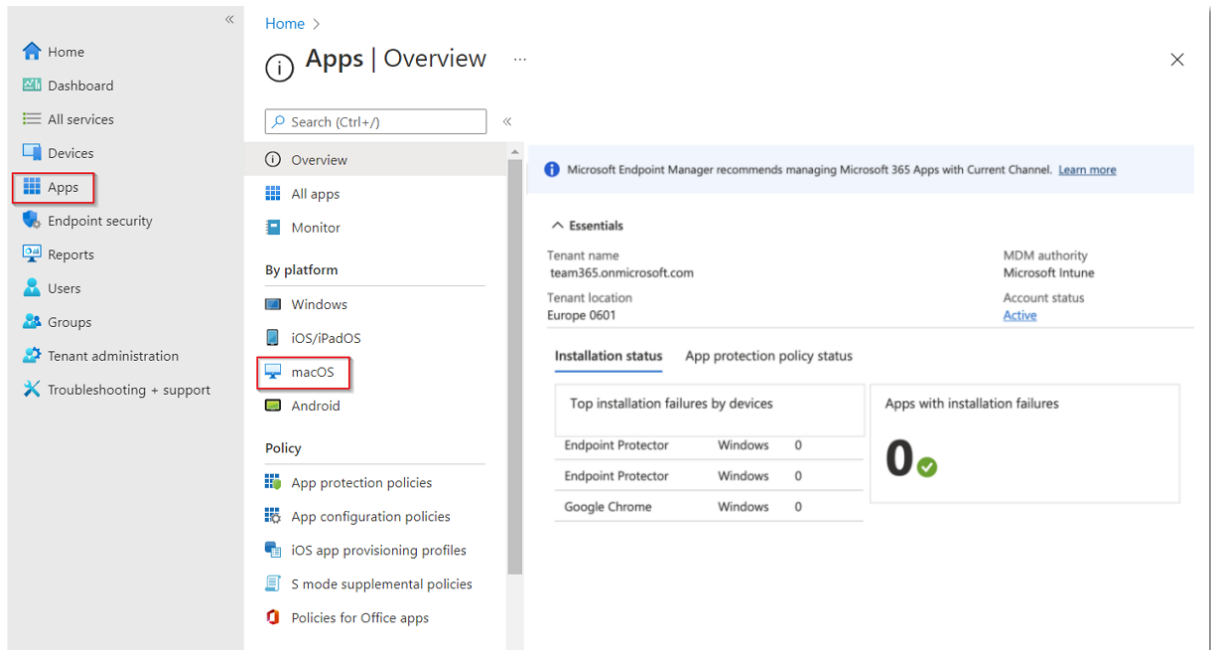
To deploy the Endpoint Protector package for macOS using Intune, follow these steps:

4. Open and log in to Endpoint Protector;
5. Go to the **System Configuration, Client Software** and download the **macOS Endpoint Protector package**;

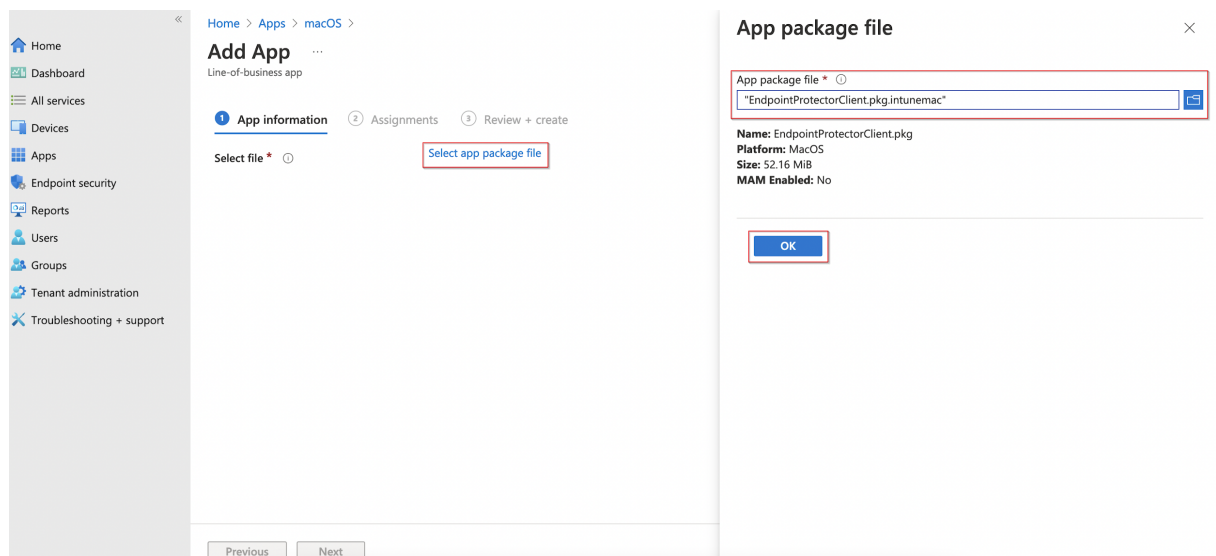


6. Convert the Endpoint Protector client to an `.intunemac` file – for more information and procedure, visit the [Microsoft Docs portal](#);
7. Go to the **Microsoft Endpoint Manager admin center** and sign in
8. Go to **Apps** from the left-hand side menu, and on the **Apps Overview** page, select the **macOS platform**;

- On the macOS apps page, click **Add**, select the **Line of business app** type, and then click **Select**;



- Click **Select app package file** and from the right-hand side, select the **Endpoint Protector intunemac file, Upload** and click **OK**;



- On the **App information** page, fill in the mandatory fields and then click **Next**:

- **Name** – add **Endpoint Protector Client**
- **Description** – add **Endpoint Protector Client**
- **Publisher** – add **CoSoSys Ltd.**

Home > Apps > macOS >

Add App ...
macOS line-of-business app

App information Assignments Review + create

Select file * EndpointProtectorClient.pkg

Name * Endpoint Protector Client

Description * Endpoint Protector Client

Publisher * CoSoSys Ltd.

The minimum operating system for uploading a .pkg file is macOS 10.14. Upload a .intunecat file to select an older minimum operating system.

Minimum operating system * macOS Mojave 10.14

Ignore app version Yes No

Install as managed Yes No

Included apps *

Review the included apps list to edit apps or remove anything that isn't an app. The app listed first is used as the primary app in app reporting. The app version can be the CFBundleShortVersionString or CFBundleVersion. [Learn more about included apps.](#)

App bundle ID (CFBundleIdentifier) App version (CFBundleShortVersionString)

com.cososys.eppclient 2.5.0.8

Enter bundle ID Enter app version

Category 0 selected

Show this as a featured app in the Company Portal Yes No

Previous Next

12. On the **Assignments** page, in the **Required** section, select the group for which you want to deploy the Endpoint Protector client and then click **Next**;

Home > Apps > macOS >

Add App ...
macOS line-of-business app

App information Assignments Review + create

Required

Group mode	Group	Filter mode	Filter
Included	All devices	None	None

+ Add group + Add all users + Add all devices

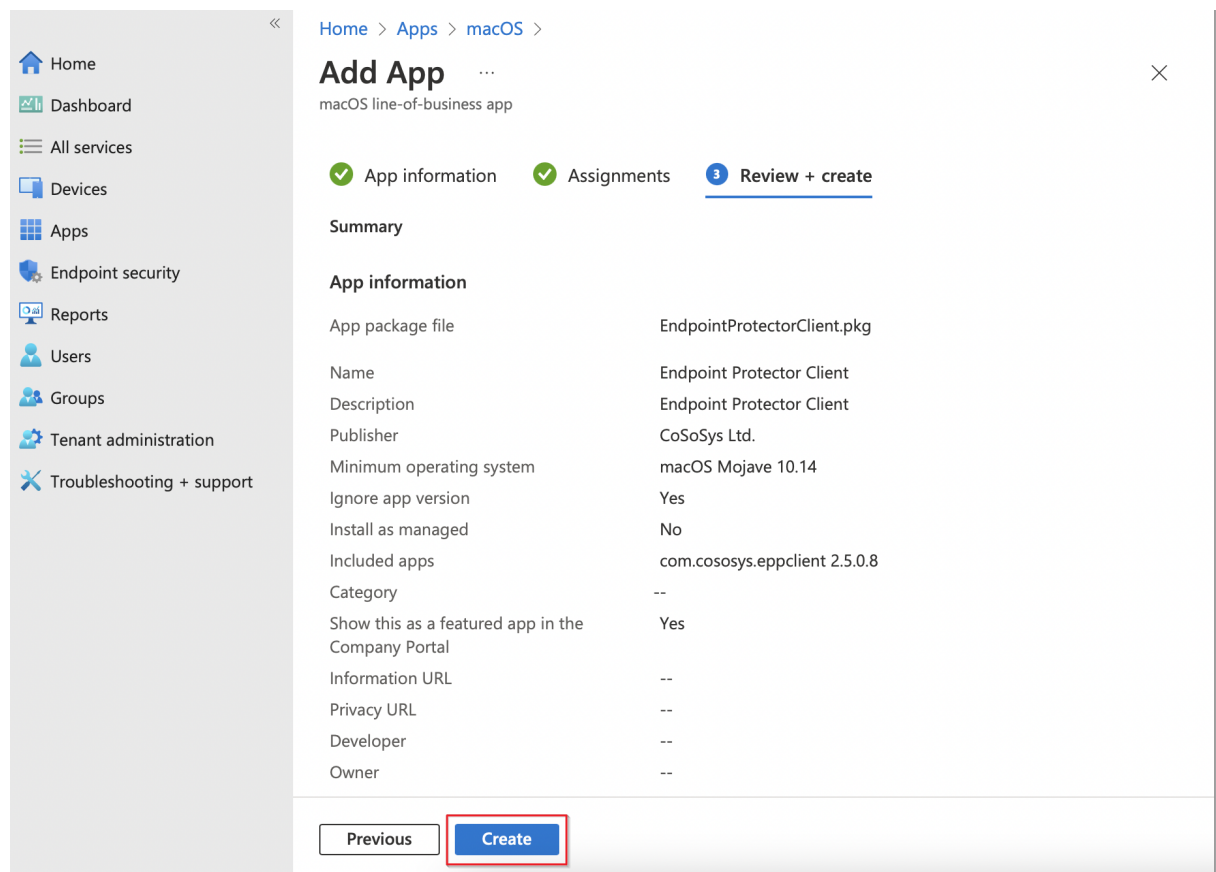
Available for enrolled devices

Group mode	Group	Filter mode	Filter
Included	All users	None	None

+ Add group + Add all users

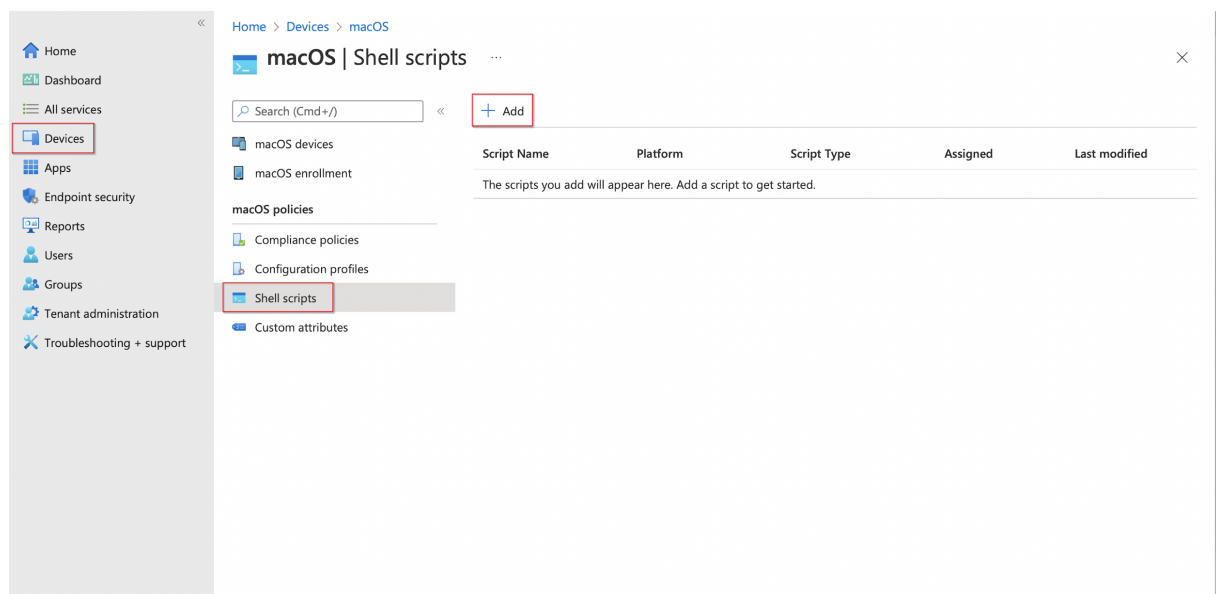
Previous Next

13. On the **Review + create** page, click **Create** - this will start the **Endpoint Protector** package upload.



14. Go to **Devices** from the left-hand menu, select **macOS, Shell scripts** and then click **Add**;

Note: Please contact the Customer Support department to provide the script.



15. On the **Add script** page, fill in the mandatory information and then click **Next**

- **Name** (mandatory) – add a name for the script (Post install script)

- **Description** – add a description for the script

The screenshot shows the 'Add script' dialog box with the 'Basics' tab selected. The breadcrumb navigation at the top reads 'Home > Devices > macOS >'. The left sidebar contains a list of navigation items: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area has a title 'Add script' with a dropdown menu showing 'macOS'. Below the title are four tabs: '1 Basics' (active), '2 Script settings', '3 Assignments', and '4 Review + add'. The 'Name' field is labeled 'Name *' and contains the text 'Post install script'. The 'Description' field is a large empty text area. At the bottom of the dialog are two buttons: 'Previous' and 'Next', with the 'Next' button highlighted by a red rectangle.

16. On the **Script settings** tab, add the following information and then click **Next**:

- Upload and select the **New Jamf PostInstall** script from your computer
- Set the **Run script as sign-in user** setting to **No**

The screenshot shows the 'Add script' dialog box with the 'Script settings' tab selected. The breadcrumb navigation at the top reads 'Home > Devices > macOS >'. The left sidebar is the same as in the previous screenshot. The main content area has the same title 'Add script' and dropdown menu 'macOS'. The tabs are '1 Basics', '2 Script settings' (active), '3 Assignments', and '4 Review + add'. The 'Upload script *' field contains the text 'epp_change_ip_epp.sh' and has a file selection icon to its right. The 'Run script as signed-in user' field has two radio buttons, 'Yes' and 'No', with 'No' selected and highlighted by a red rectangle. The 'Hide script notifications on devices' field is a dropdown menu with 'Not configured' selected. The 'Script frequency' field is a dropdown menu with 'Every 15 minutes' selected. The 'Max number of times to retry if script fails' field is a dropdown menu with 'Not configured' selected. At the bottom of the dialog are two buttons: 'Previous' and 'Next', with the 'Next' button highlighted by a red rectangle.

17. On the **Assignments** tab, include the groups you prefer (Add groups, all users, or all devices) and then click **Next**;

The screenshot shows the 'Add script' page for macOS, specifically the 'Assignments' tab. The left sidebar contains navigation links: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area has a breadcrumb trail 'Home > Devices > macOS >' and a title 'Add script' with a dropdown menu. Below the title are four tabs: 'Basics' (checked), 'Script settings' (checked), 'Assignments' (active), and 'Review + add' (disabled). The 'Included groups' section has three buttons: 'Add groups', 'Add all users', and 'Add all devices'. Below this is a table with one row: 'All devices' with a 'Remove' link. The 'Excluded groups' section has a blue information box stating: 'When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.' Below the box is a '+ Add groups' button and a table with one row: 'No groups selected'. At the bottom are 'Previous' and 'Next' buttons, with 'Next' highlighted.

Home > Devices > macOS >

Add script

macOS

Basics Script settings Assignments Review + add

Included groups

Add groups Add all users Add all devices

Groups
All devices Remove

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.

+ Add groups

Groups
No groups selected

Previous Next

18. On the **Review + add** tab, you can view the script information and click **Add**.

The screenshot shows the 'Add script' page for macOS, specifically the 'Review + add' tab. The left sidebar is the same as the previous screenshot. The main content area has the same breadcrumb trail and title. The tabs are: 'Basics' (checked), 'Script settings' (checked), 'Assignments' (checked), and 'Review + add' (active). The 'Summary' section is at the top. Below it are three sections: 'Basics', 'Script settings', and 'Assignments'. The 'Basics' section has 'Name' (Post install script) and 'Description' (--). The 'Script settings' section has 'Shell script' (epp_change_ip_epp.sh), 'Run script as signed-in user' (No), 'Hide script notifications on devices' (Not configured), 'Script frequency' (Every 15 minutes), and 'Max number of times to retry if script fails' (Not configured). The 'Assignments' section has 'Included groups' (All devices) and 'Excluded groups' (--). At the bottom are 'Previous' and 'Add' buttons, with 'Add' highlighted.

Home > Devices > macOS >

Add script

macOS

Basics Script settings Assignments Review + add

Summary

Basics

Name	Post install script
Description	--

Script settings

Shell script	epp_change_ip_epp.sh
Run script as signed-in user	No
Hide script notifications on devices	Not configured
Script frequency	Every 15 minutes
Max number of times to retry if script fails	Not configured

Assignments

Included groups	All devices
Excluded groups	--

Previous Add

4. 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 (eproot) 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.

Confidential. © CoSoSys 2022.
Not to be shared without the express
written permission of CoSoSys

EndpointProtector.com