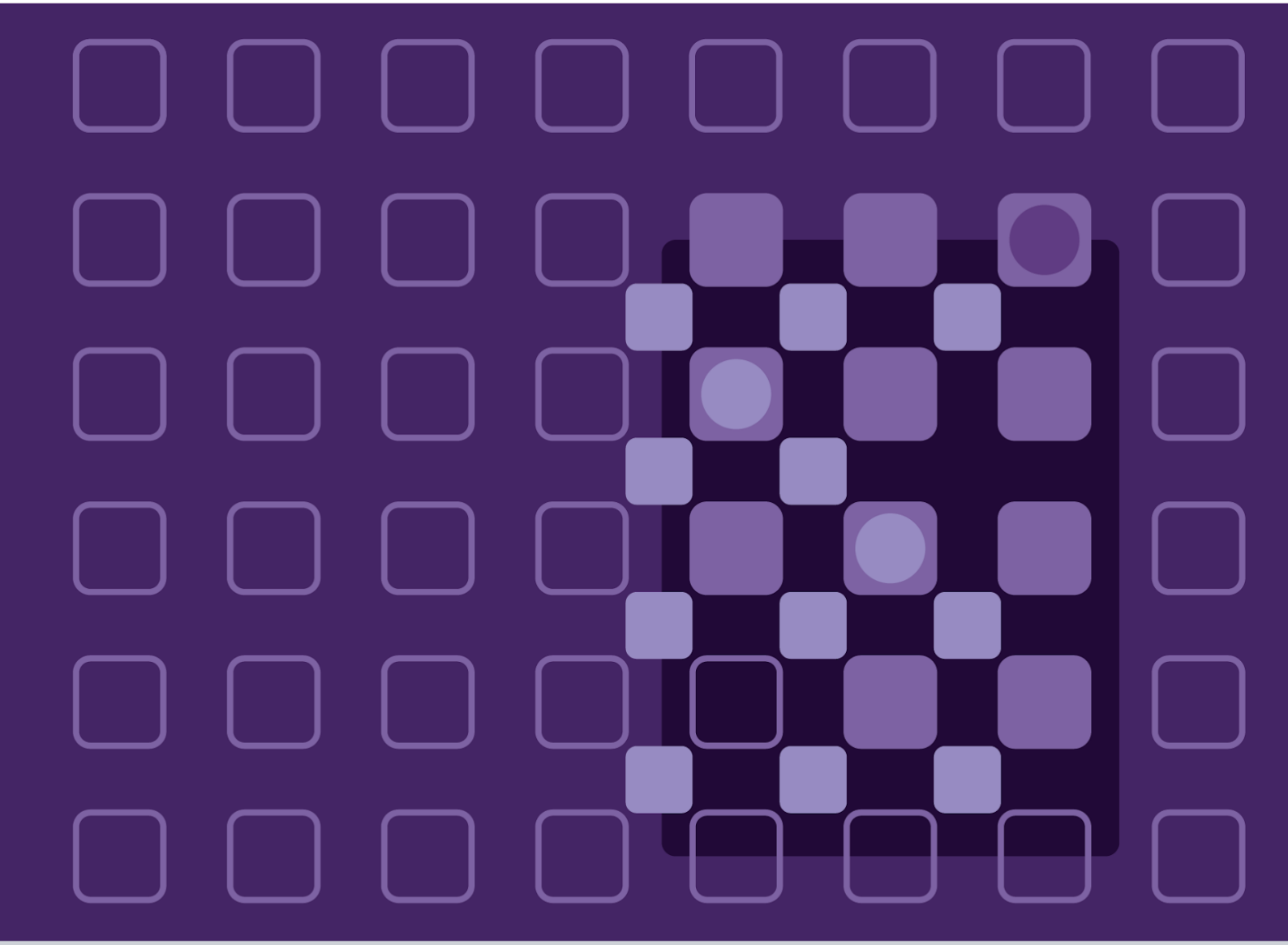
ENDPOINT PROTECTOR | by CoSoSys

Intune

Deployment Guide



Version 3.0

Date 11.11.2022

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.

3.

1. Introduction

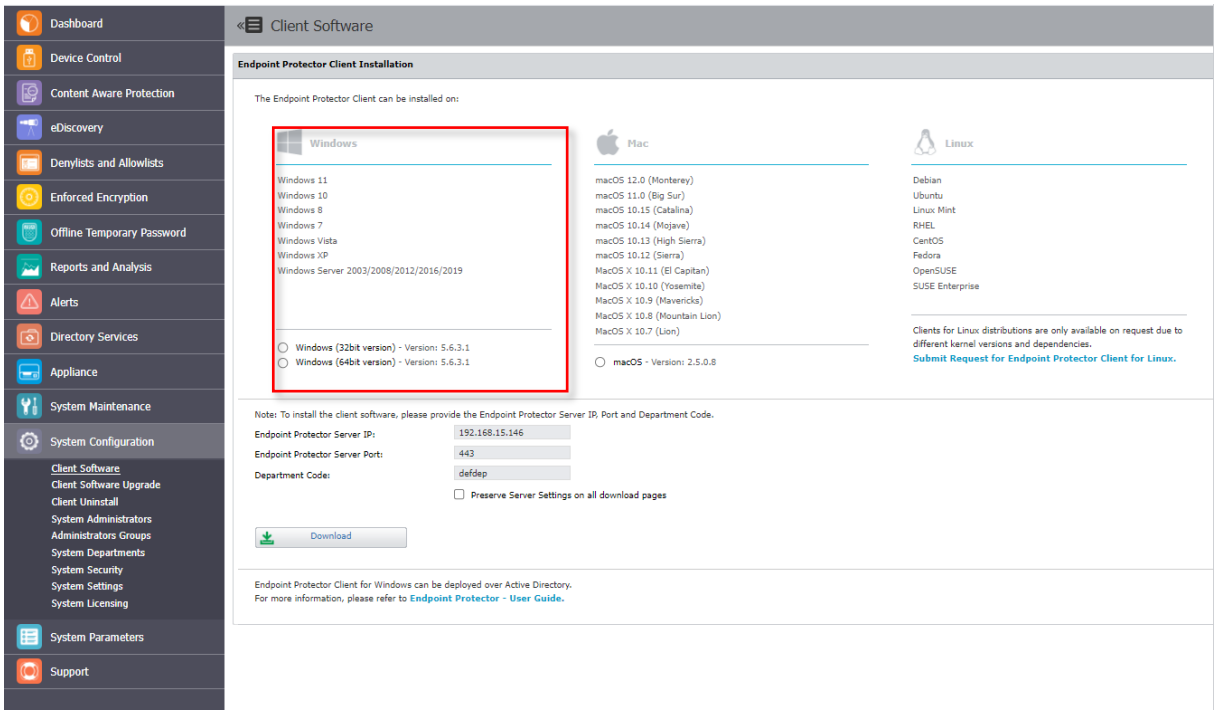
This document describes the steps needed to deploy Endpoint Protector to multiple endpoints using the MSI application in Microsoft Intune.

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

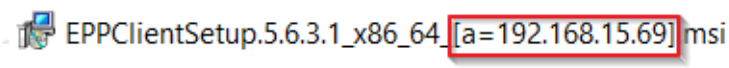
2. Windows deployment

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**;

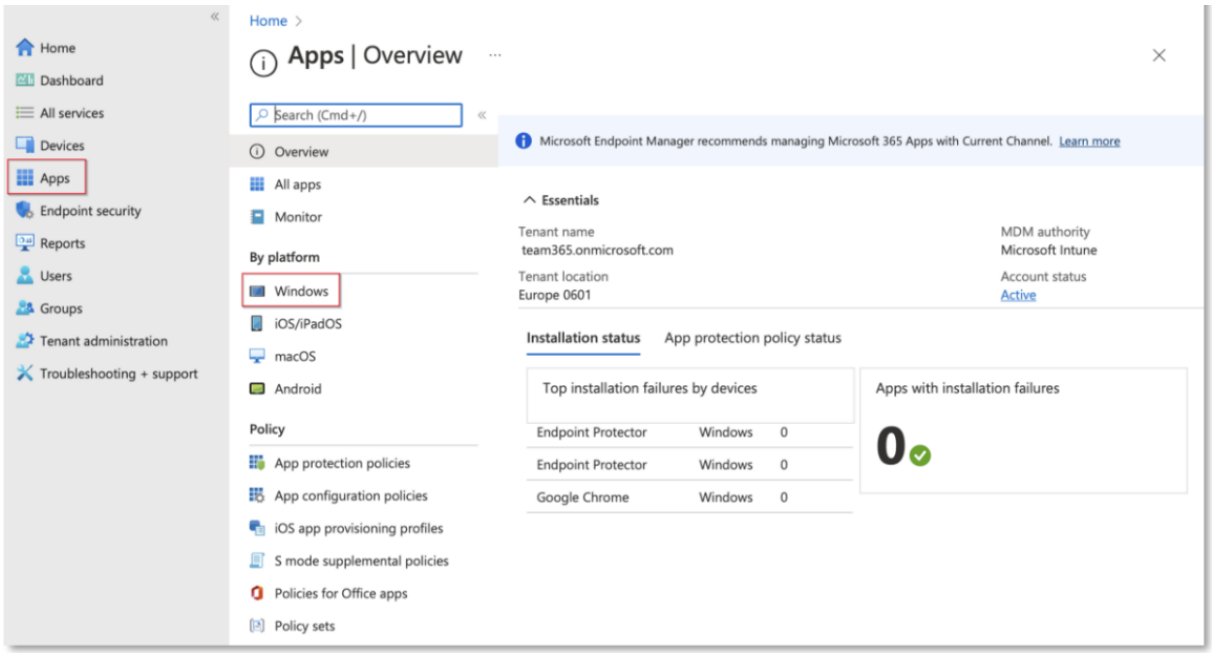


Important: When deploying the .msi package, delete the information contained in the brackets as well as the underscore that precedes it - EPPClientSetup.5.6.3.1_x86_64.msi

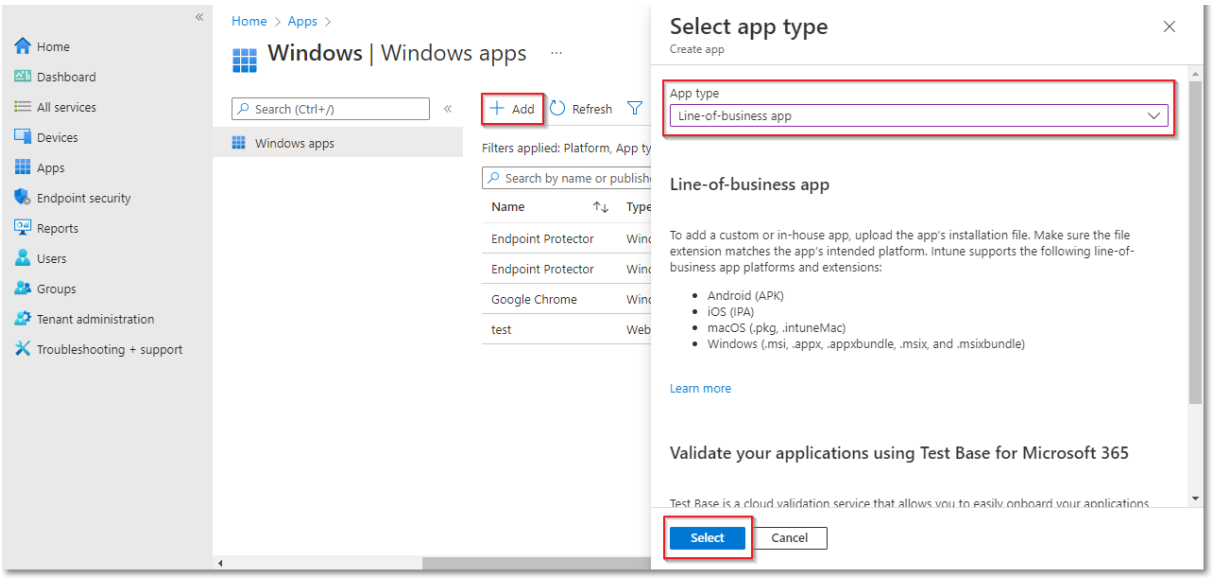


3. Go to the **Microsoft Endpoint Manager admin center** and sign in;

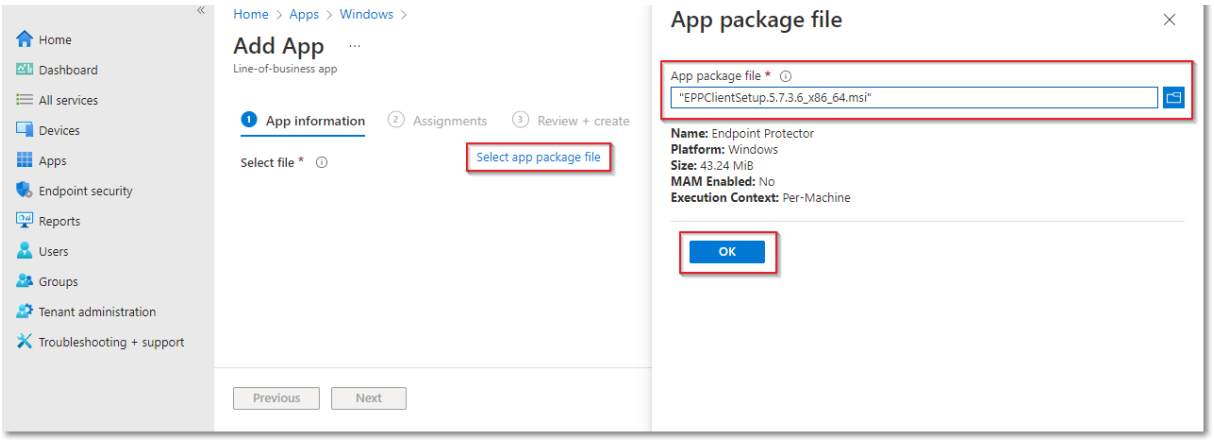
4. Go to **Apps** from the left-hand side menu, and on the **Apps Overview** page, select the **Windows** platform;



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

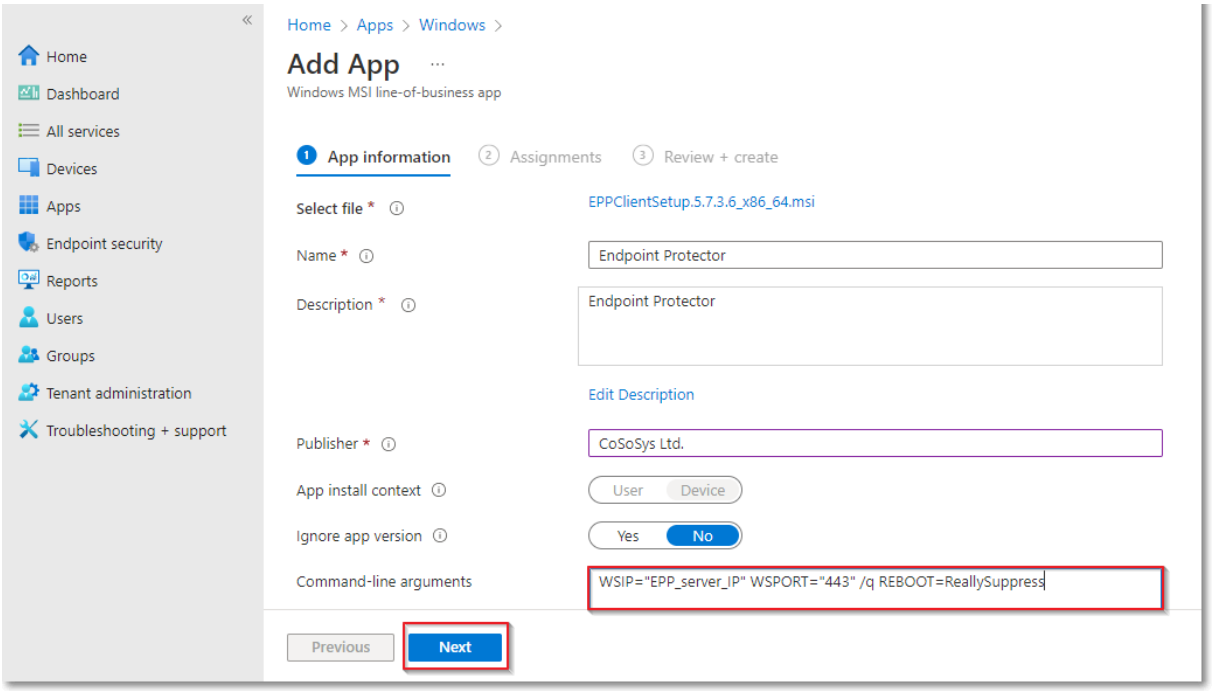


6. Click **Select app package file** and from the right-hand side, select the **Endpoint Protector MSI** file and click **OK**;

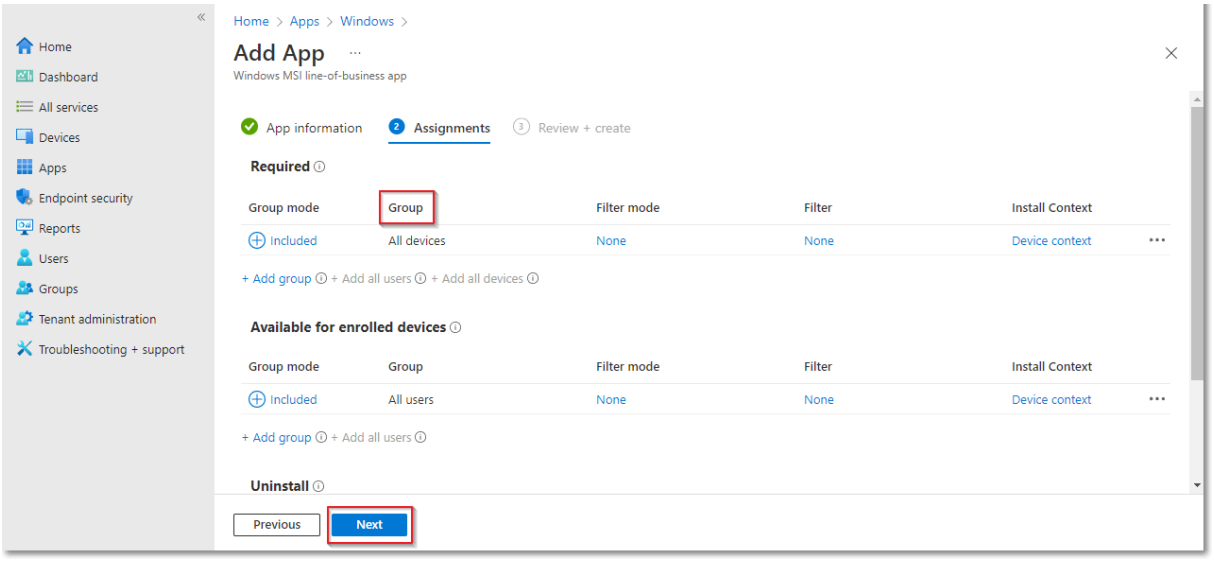


7. On the **App information** page, fill in the mandatory fields and then click **Next**:
   - **Name** – add Endpoint Protector and optional, the package version (Endpoint Protector 5.7.3.6)
   - **Description** – click **Edit Description** and add installation details
   - **Publisher** – add **CoSoSys Ltd**.
   - **Command-line argument** – add the following command line in the text box

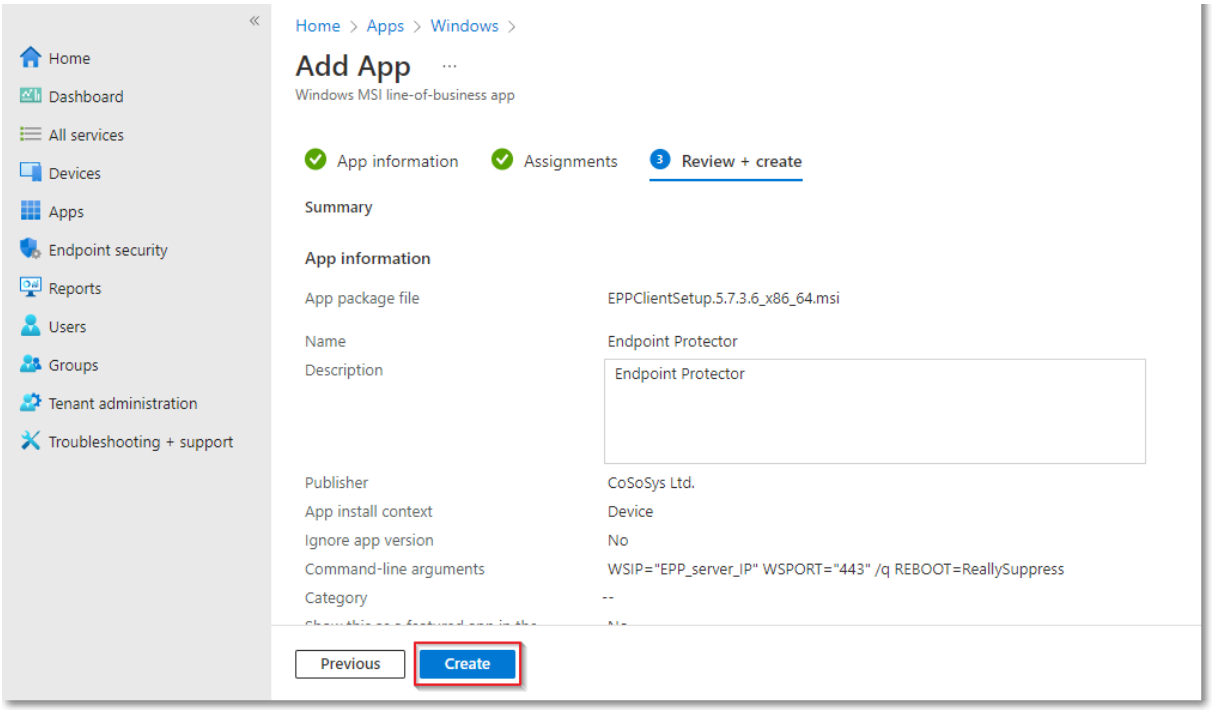
     WSIP="EPP_server_IP" WSPORT="443" /q REBOOT=ReallySuppress



8. 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**;



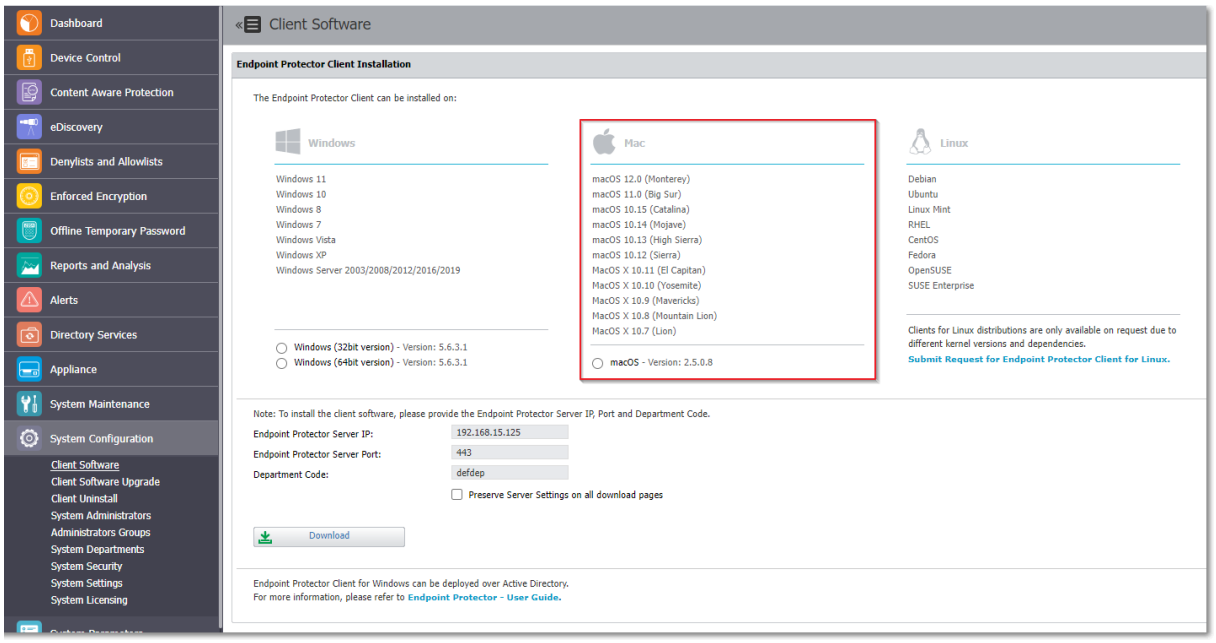
9. On the **Review + create** page, click **Create** - this will start the **Endpoint Protector MSI package** upload.



3. macOS deployment

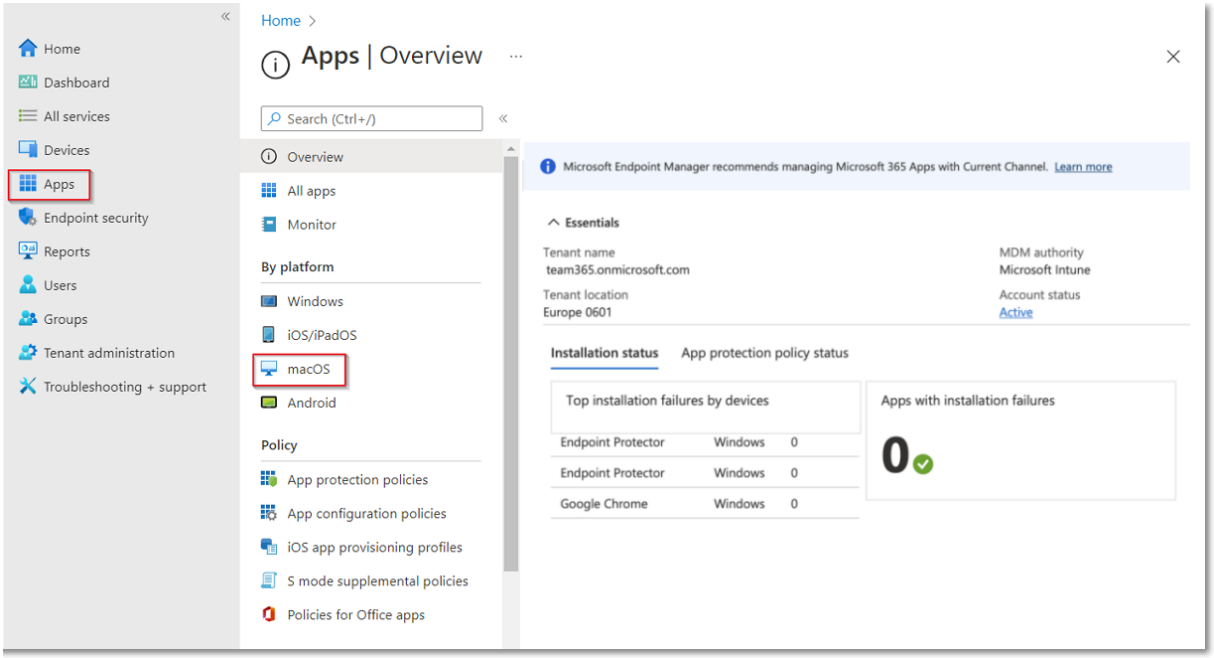
To deploy the Endpoint Protector package for macOS using Intune, follow these steps:

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

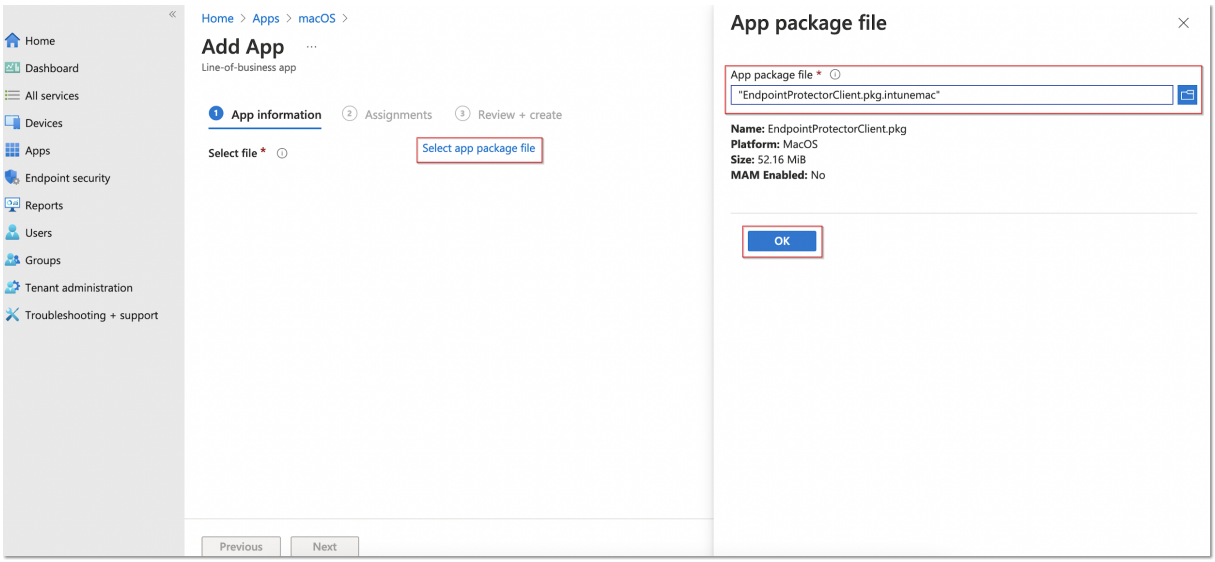


6. Convert the Endpoint Protector client to an *.intunemac* file – for more information and procedure, visit the Microsoft Docs portal;
7. Go to the **Microsoft Endpoint Manager admin center** and sign in
8. Go to **Apps** from the left-hand side menu, and on the **Apps Overview** page, select the **macOS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

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

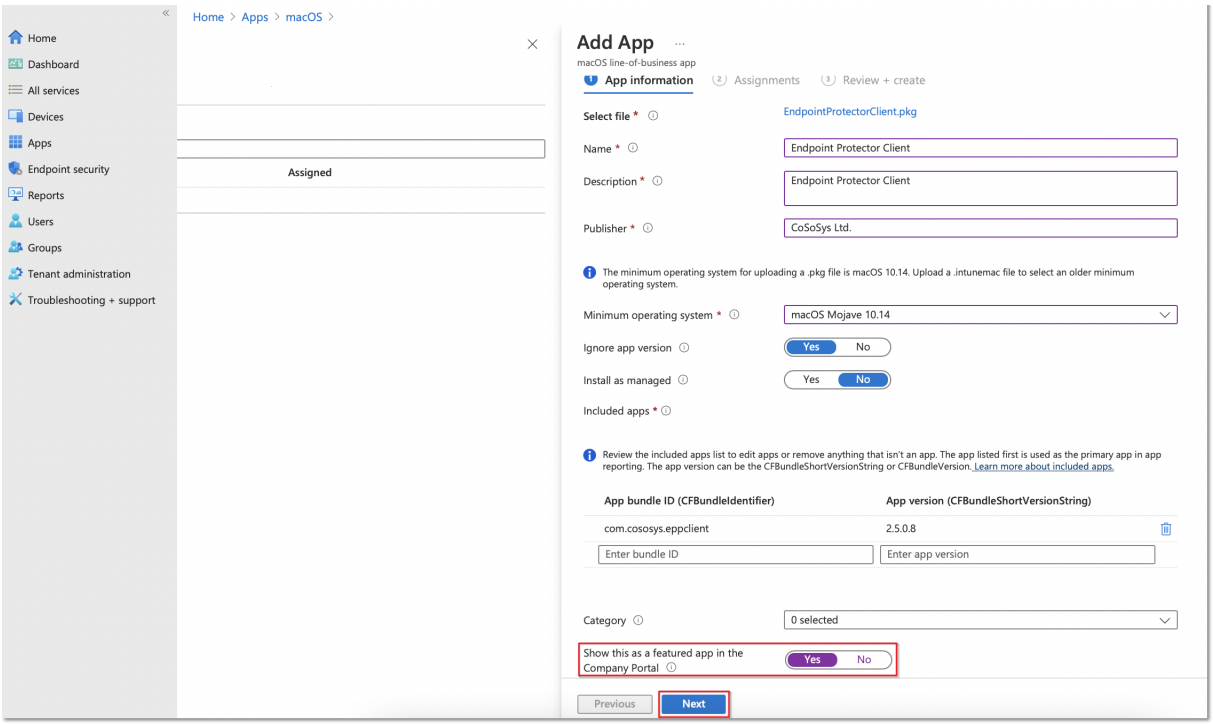


10. Click **Select app package file** and from the right-hand side, select the **Endpoint Protector intunemac file**, **Upload** and click **OK**;

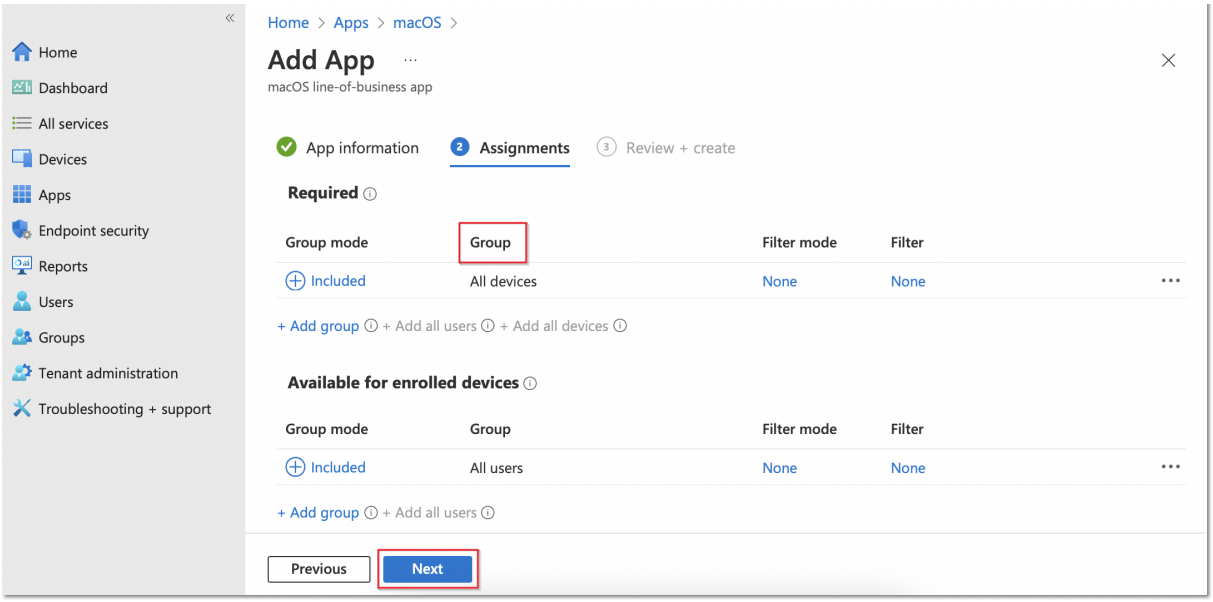


11. On the **App information** page, fill in the mandatory fields and then click **Next**:

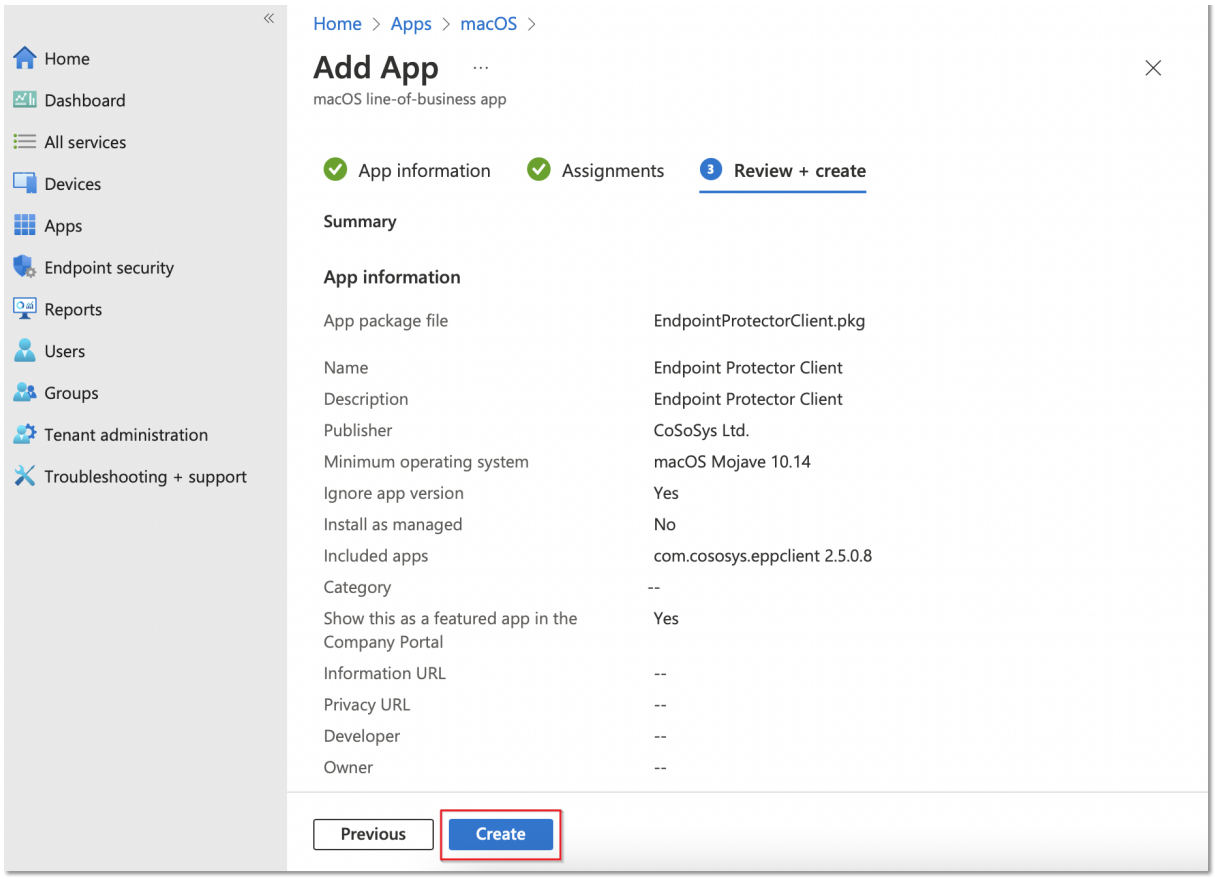
- **Name** – add **Endpoint Protector Client**
- **Description** – add **Endpoint Protector Client**
- **Publisher** – add **CoSoSys Ltd**.



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**;

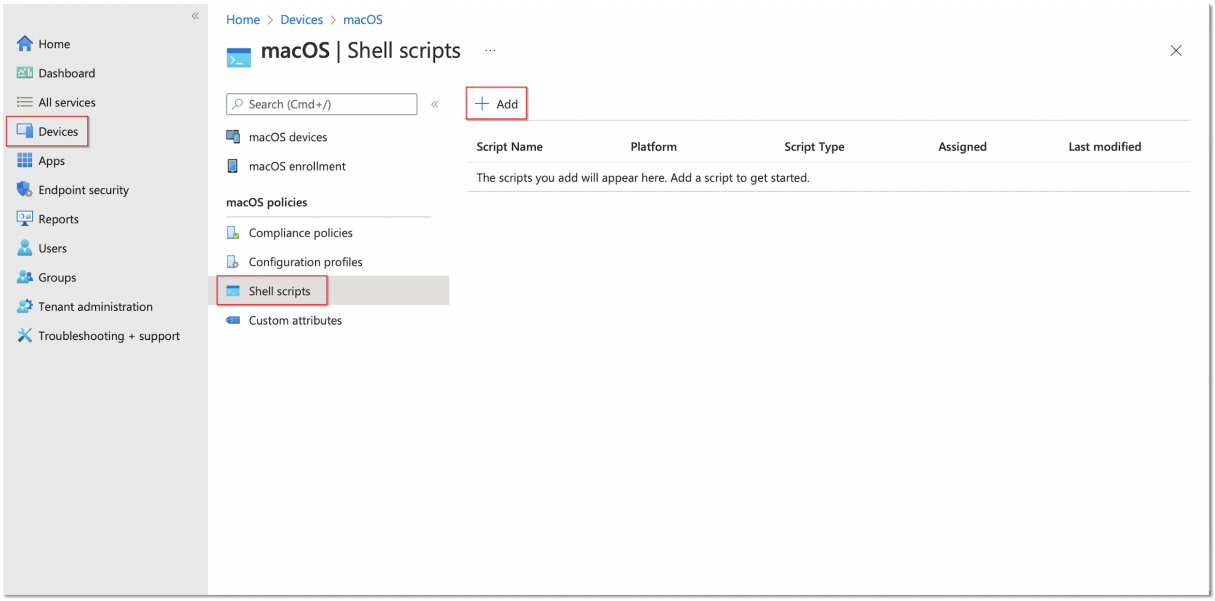


13. On the **Review + create** page, click **Create** - this will start the **Endpoint Protector** package upload.



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

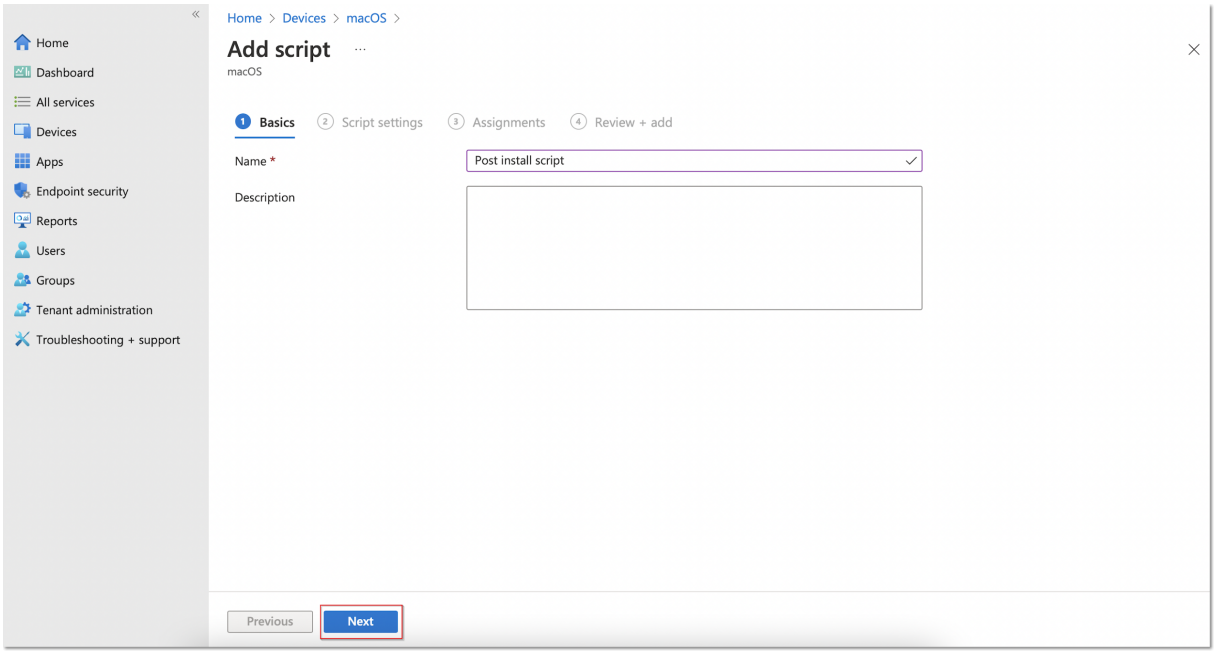
Note: Please contact the Customer Support department to provide the script.



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

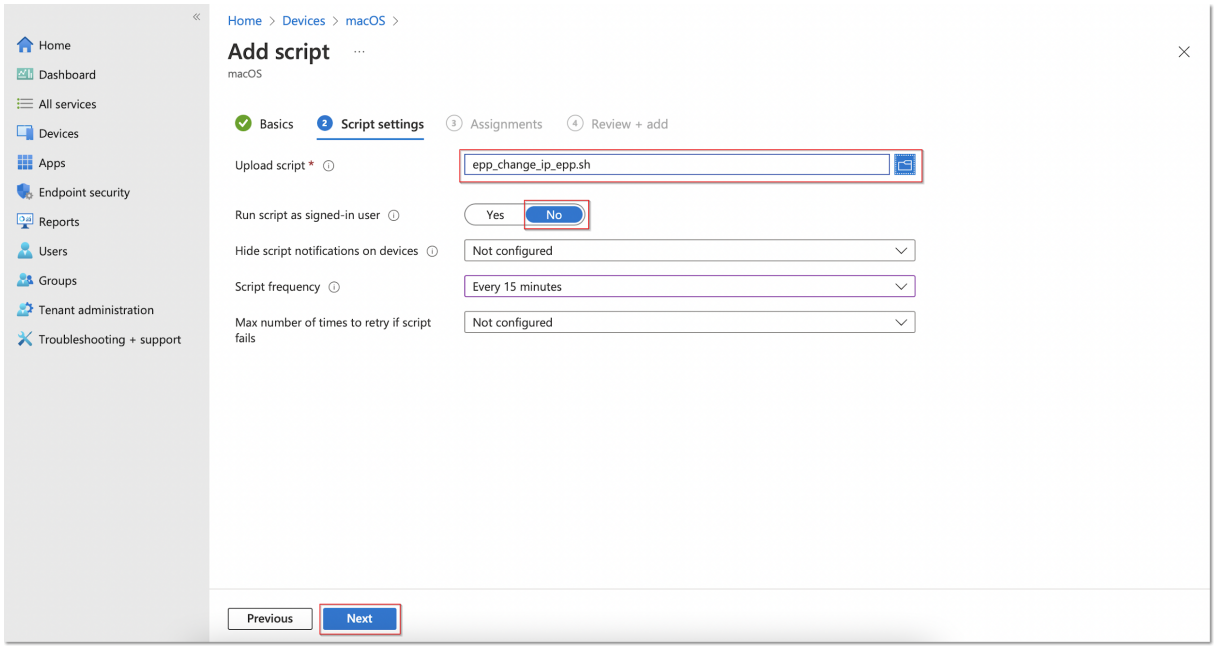
- **Name** (mandatory) – add a name for the script (Post install script)

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

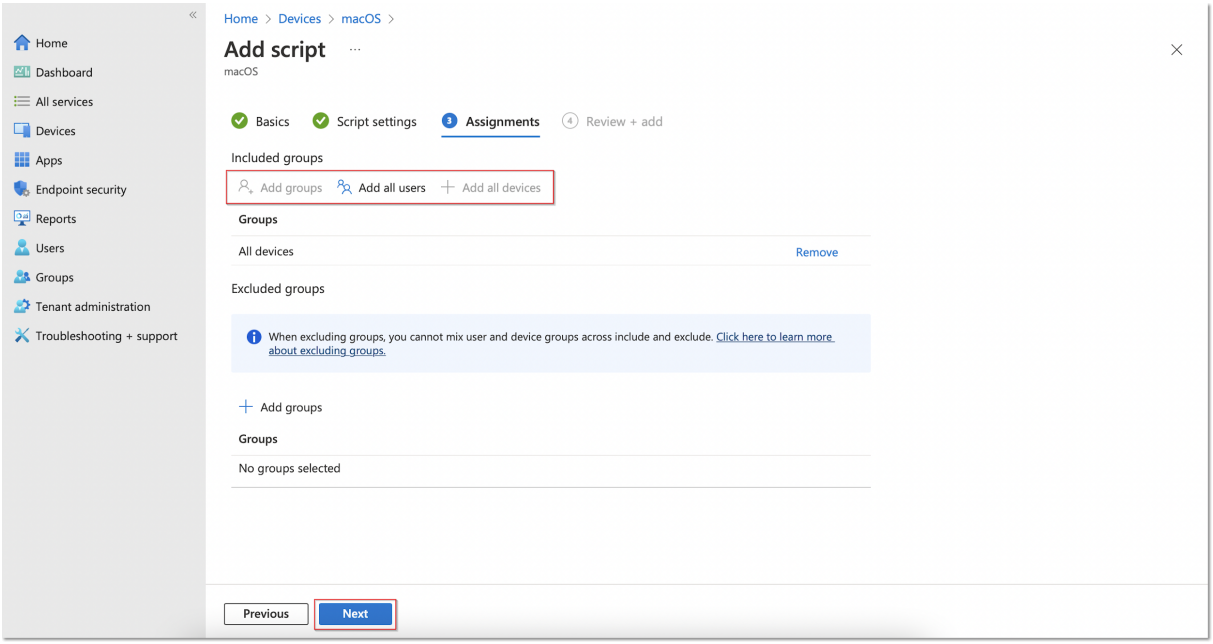


16. On the **Script settings** tab, add the following information and then click **Next**:

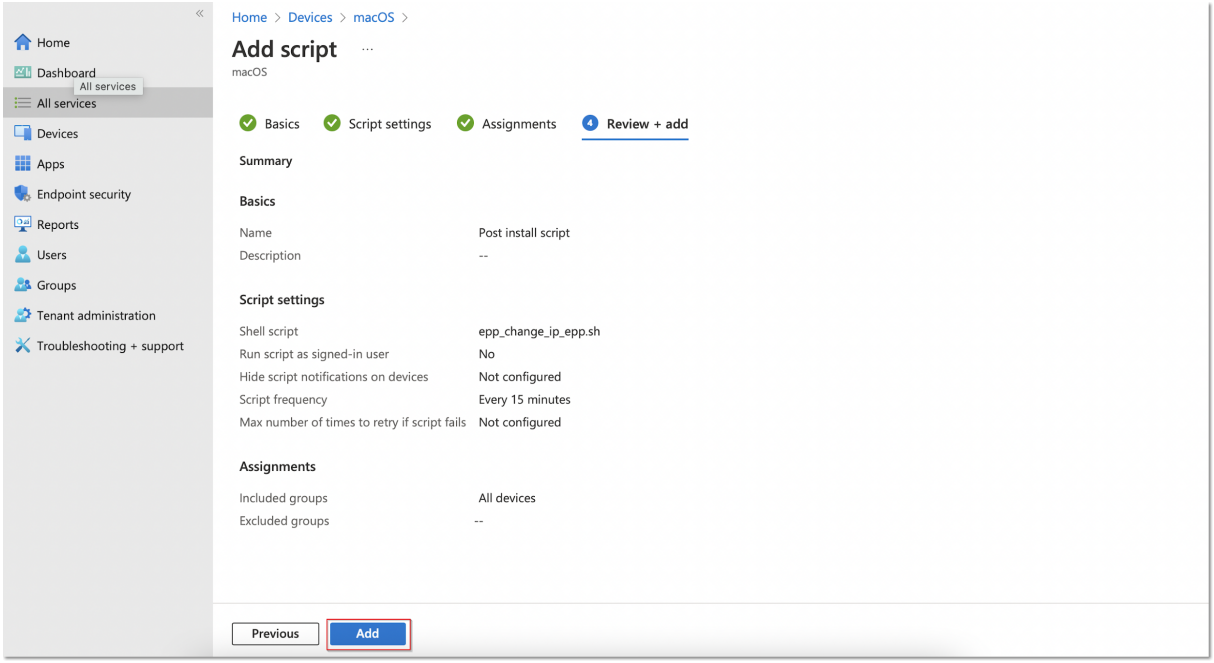
    - Upload and select the **New Jamf PostInstall** script from your computer
    - Set the **Run script as sign-in user** setting to **No**



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



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

EndpointProtector.com