


Learn how Sophos is awesome  
and causes no problems at  
all...

For fun and profit...

(or... how I learned lots about System Extensions I was  
happier not knowing about...)



TCR 00:02:54:22

**(a classic April Fools from 1957)**

Prologue...



## Graham Gilbert

Systems Engineer at Airbnb

---

### Session Title: Rolling out Catalina within 30 days – are we nuts?

**Overview:** Most people know that Apple considers major operating system releases to be security fixes. It can often take weeks for critical security issues to be fixed on older releases (that is if they're fixed at all). So knowing this, how do we keep our fleets secure without ruining the productivity of our users, running our IT teams into the ground and destroying the available bandwidth in our offices?

We will take you all the way back to our planning sessions, take a look at how we qualify the new operating system in our environment and how we deploy it to many thousands of devices globally with minimal impact to the end user. Airbnb has deployed the last three major releases of macOS in this manner, so we can continue to keep the company's, our hosts and our guests secure, having nearly 100% of active devices updated within 30 days.

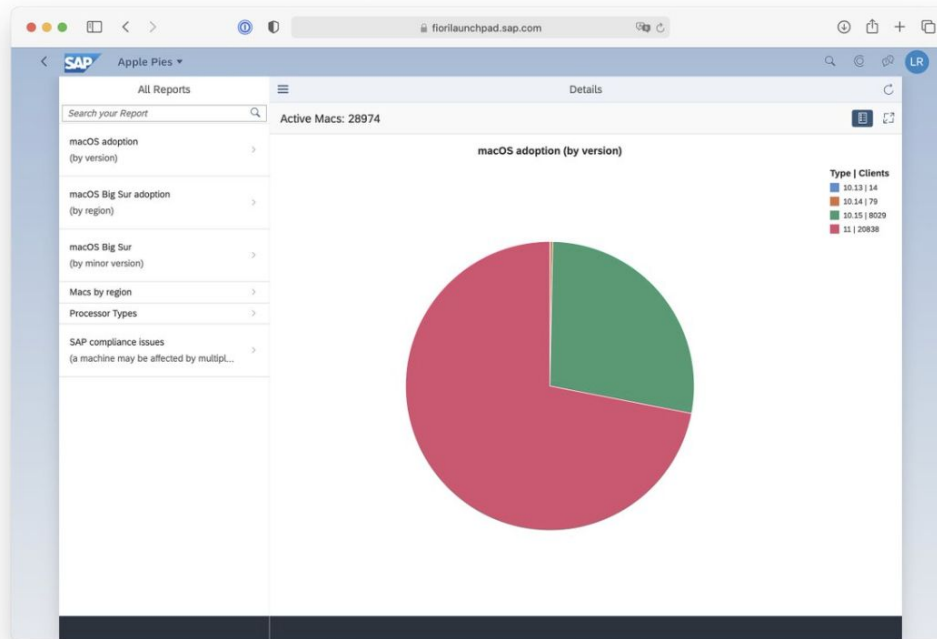


Laura Rösler  
@lauraroessler



After 3 months with macOS Big Sur, almost  $\frac{3}{4}$  of our Mac fleet is on macOS 11. 🍏💻

#MacAtSAP #ApplePies #bigsurprise #BigSur  
#LifeAtSAP

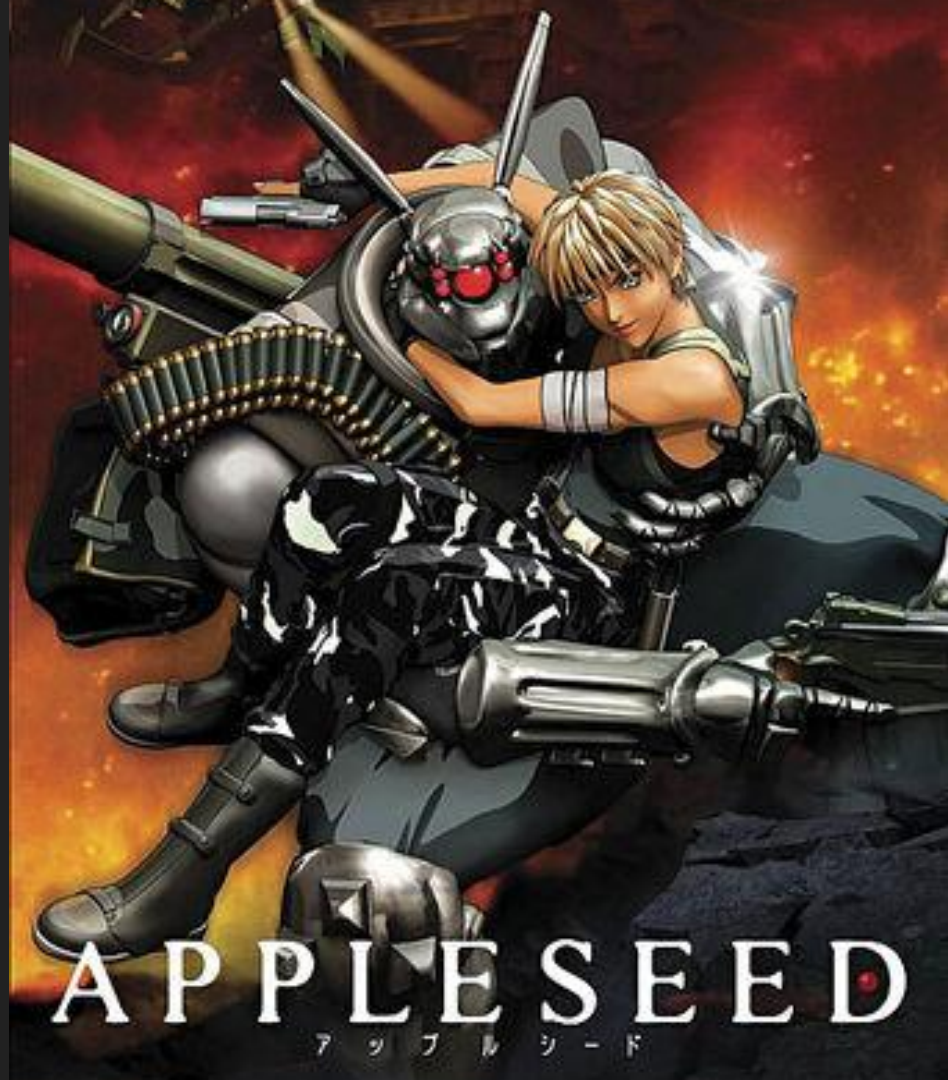




# Prepare for the unpredictable



AppleSeed...



Folks,

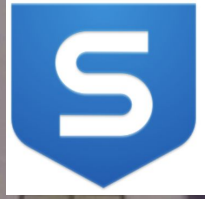
Apple has just announced that macOS V11 will be available from this Thursday (12th November).

We are not yet ready to support Big Sur (first time I've had to say that in a very long time, so apologies...), we plan to open a private EAP w/c 23rd November and hopefully make this public a week or two later dependent on feedback.





\* GROANS \*



Steve

My dream of an early  
Big Sur Roll out

\* GROANS \*

A close-up shot of a man with long, wavy brown hair and a full, dark beard. He is wearing a green tunic with a blue sash. He is looking upwards and to the right with a slightly distressed or questioning expression. The background is blurred, showing what appears to be a stone wall or a similar textured surface.

**What  
Year  
is  
it?**

And then not much  
happened...

(apart from membership of an Early Access Program)

Intermission...

# SYSTEM EXTENSIONS

(the joy of SEXTS?)





Kernel  
Extensions

System  
Extensions

Corporate needs you to find the differences  
between this picture and this picture.



They're the same picture.

# About system extensions and macOS

Some system extensions aren't compatible with current versions of macOS or won't be compatible with a future version of macOS. Find out what to do if you see an alert about system extensions or kernel extensions.

System extensions work in the background to extend the functionality of your Mac. Some apps install kernel extensions, or kexts – a kind of system extension that works using older methods that aren't as secure or reliable as modern alternatives. Your Mac identifies these as legacy system extensions.

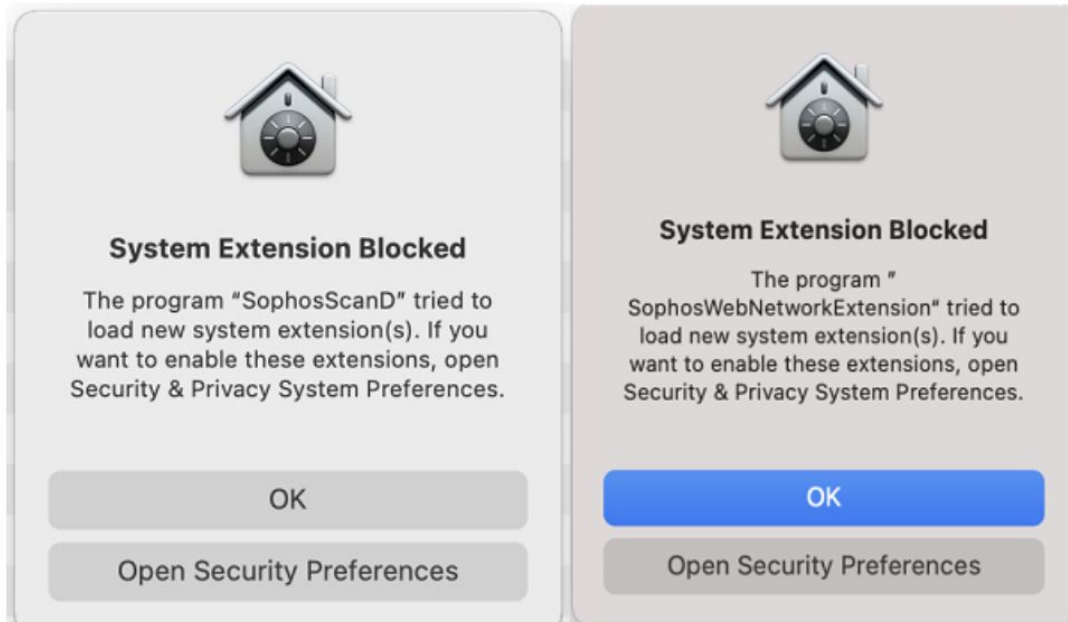
In 2019, Apple informed developers that macOS Catalina will be the last macOS to fully support legacy system extensions, and we've been working with developers to transition their software.

# Additional Security Requirements

The change to System Extensions in Big Sur requires additional security permissions beyond what is detailed in [macOS 10.15+ Security Permissions Required](#). Apple has enforced these permissions, and they cannot be added automatically by vendors. These changes are detailed here.

**Important:** If the extensions are not allowed, protection will not function. If the Full Disk Access permissions are not added, Scanning will not function properly. Without Proxy permission, Web Protection cannot function.

1. During install or after upgrade to Big Sur (With Sophos Endpoint installed), a prompt will display to allow the System Extensions for SophosScanD and SophosWebNetworkExtension.





Intercept X Endpoint > Recommended Reads More

+ New

# Sophos Mac Endpoint: How to Configure JAMF Privacy Preferences for 10.15+ Compatibility

FloSupport over 1 year ago

Note: This information is provided as-is for the benefit of the Community. Please contact Sophos Professional Services if you require assistance with your specific environment.

## Overview

This article describes the steps to configure JAMF to allow configure permissions for Sophos Mac Endpoint on macOS 10.15+

Applies to the following Sophos products and versions

- Sophos Central Mac Endpoint 10.0.0 and above,
- Sophos Central Intercept X 10.0.0 and above,
- Sophos Central Device Encryption 1.5.2 and above,
- Sophos Anti-Virus for Mac OS X 9.9.7 and above

## Table of Contents

### Thread Info

+6

64 replies

33 subscribers

33450 views

0 members are here

- jamf
- MacOS
- Big Sur

### Options

RSS

### Suggested

Sophos Mac Endpoint: How to configure Apple Profile Manager to allow Sophos to work with macOS 10.15+

Disclaimer: This information is p...

# SimpleMDM :)

Added support for System Extensions

And so my work was done...



## Or was it?

- When I built a test machine from scratch - the profiles did their job, and Sophos worked as expected :)
- But when folks *upgraded* to Big Sur, they were being prompted to approve one or both system extensions...
- ...even when MDM had delivered the System Extension profile :(

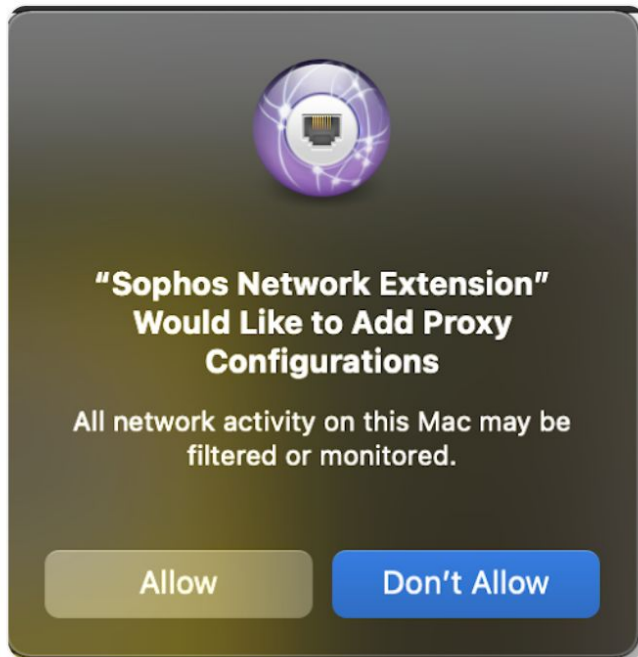
PLUS...



Stephen Quirke 11 Feb, 18:52

Following

Interesting... (as the system extension should be pre-approved...) I've clicked  to see how upset doing so makes Sophos...



my guess is, this is required for the web filtering that we haven't enabled yet...



Srikanth Venugopalan 12 Feb, 01:31

I got this after the recent big sure update. I clicked don't allow too  
Let me know what I should look for explicitly



Intercept X Endpoint

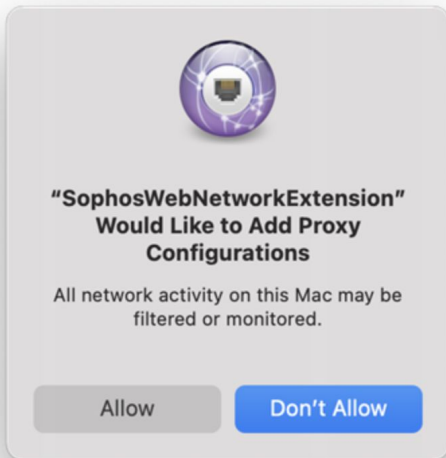
Big Sur EAP > Discussions More

## Configuration Profile for Proxy Configuration



[mscottblake](#) 4 months ago

When you install the 10.0.2 EAP on a macOS 11 Big Sur computer, you are presented with a dialog requesting access for SophosWebNetworkExtension to create a proxy configuration. Is there a way to eliminate this dialog with a configuration profile from an MDM?



# COMMUNITY SUPPORTED?

- I'd not noticed the difference before...
- ...but all the *good* stuff is in the community supported pages
- These are vendor reviewed before being published...
- ...so should be considered supported workflows.

# Managing Sophos on macOS in 2021...



**(Kill the pop-ups...)**

# RELEASE GROUPS

Group "A"



# With a little help from Slack...



**Ken**  5 days ago

Ah I see, the biggest issue we are running into now is users upgrading who already have Sophos installed. Comps on big sur with our config profile already on it don't seem to ask those system ext questions. Does that sound like the behavior we've all been experiencing?



**Julian Müller** 5 days ago

Sounds about right



**grahamrpugh** 5 days ago

Yep, same here. A very tricky race condition. If you can control your workflow I would advocate uninstalling Sophos before upgrading to Big Sur. That's a big "if" though 😊



**Julian Müller** 5 days ago

I am still not sure why you are uninstalling Sophos [@grahamrpugh](#). You can push the sysext profile to devices running 10.15.4 and up. So for devices that are running these version they can simply upgrade?



**grahamrpugh** 5 days ago

Oh, and that works? We can try that.



**Julian Müller** 5 days ago

Yea. Sysext profiles are supported since 10.15.4 😊



**mscottblake**  5 days ago

Sophos won't use the SysExt until 11, but will accept them starting with 10.15.4



# And even more help?



**Paul Smernoff** 06:15

I would like to offer some comprehensive documentation I pieced together on JAMF management of Sophos for Big Sur as a sign of my appreciation for this community, the many contributors from whom I learned, and those who posted questions to make subsequent offers of answers a reality. PM me and I will supply you with a twenty-eight page PDF, a deployment methodology flowchart, and a thirty-six minute audio commentary (in video form) on the flowchart.



4




1




# The tl:dr

- The #Sophos channel knows more about Sophos on Mac than Sophos does
  - Sophos Community Pages are more useful official Sophos pages
  - System Extensions are more annoying than Kernel Extensions
  - It's all about timing - you need to get the right profiles on disk at the right time!
  - Remember, whatever you do you can't win...
- 
- <https://github.com/ThoughtWorks-Identity/configuration-profiles>

Thanks... :)

 @steve2cv

 @squirke

 [blog.quirke.org](http://blog.quirke.org)

