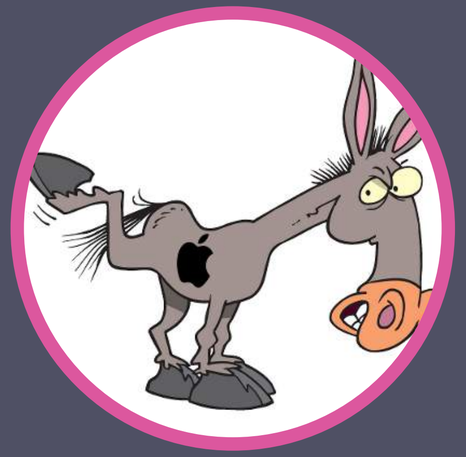
dataJAR

Beyond Device Management

Ben Toms

Head of Innovation and Platform | ben@datajar.co.uk



macmule

macmule.com | macmule | @macmuleblog

macOS Big Sur and Apple Silicon

macOS Big Sur

Documentation

profiles command

security command

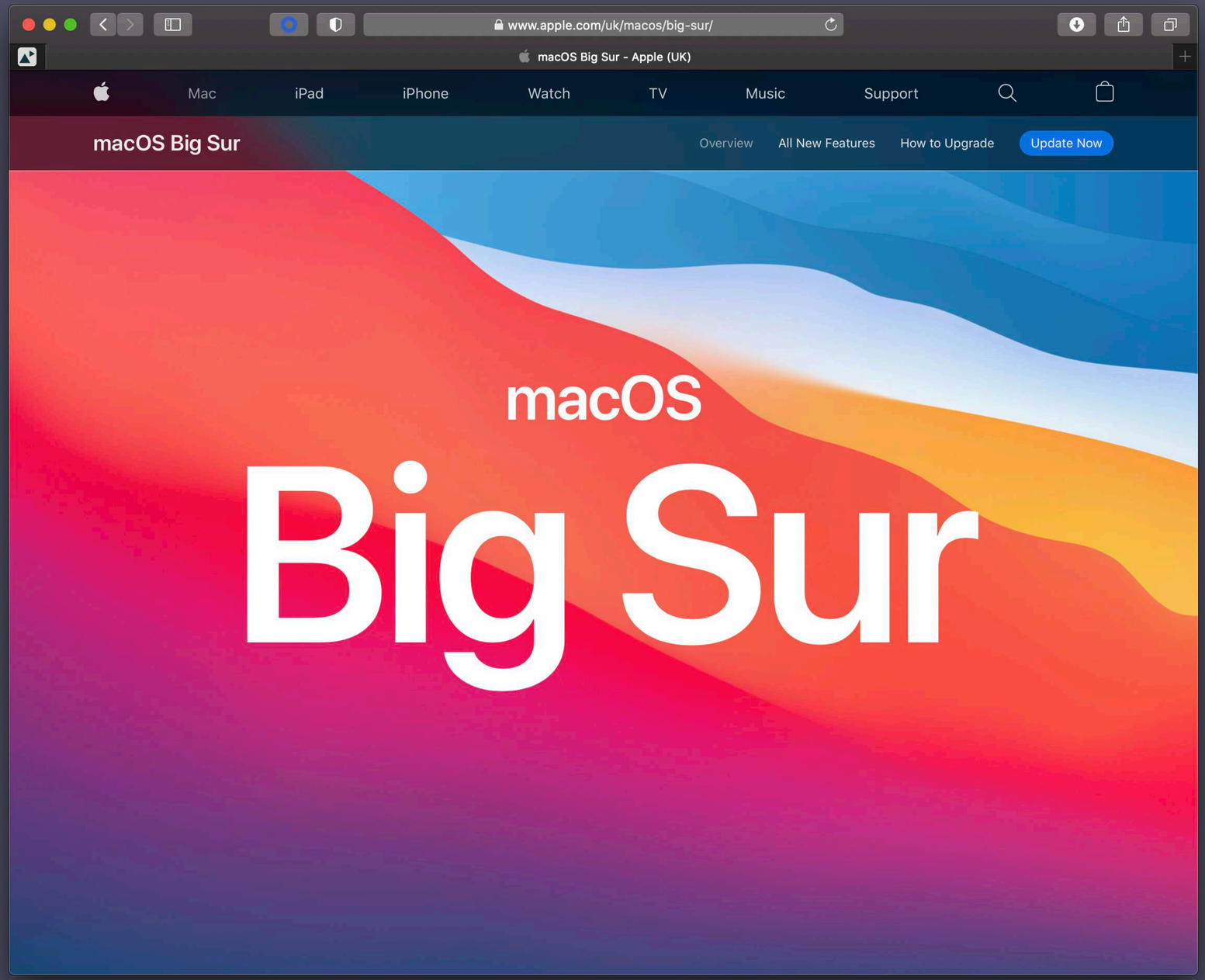
networksetup command

softwareupdate command

Summary

macOS Big Sur

https://www.apple.com/uk/macos/big-sur/



https://www.apple.com/uk/macos/big-sur/features/

www.apple.com/uk/macos/big-sur/features/

macOS Big Sur - Features - Apple (UK)

macOS Big Sur

Overview All New Features How to Upgrade Update Now

Beta

Translation

Translate entire web pages in Safari.[3] When you encounter a compatible page, just click the translation icon in the address field to translate into English, Spanish, Chinese, French, German, Russian or Brazilian Portuguese.

Safari extensions on the App Store

An all-new extensions category on the App Store showcases Safari extensions with editorial spotlights and top charts, making it easier to discover great extensions from developers. All extensions are reviewed, signed and hosted by Apple for your security.

WebExtensions API support

New support for the WebExtensions API and migration tools allows developers to bring Chrome extensions to Safari — letting you personalise your browsing experience with new Safari extensions from your favourite developers.

Grant extensions website access

Keep the websites you visit and tabs you use even more private. Safari asks you which websites a Safari extension can work with — and you can grant access for one day or all the time.

Privacy Report

Safari uses Intelligent Tracking Prevention to identify trackers and help prevent them from profiling or following you around the web. A new Privacy Report shows how Safari protects your browsing across every website you visit. Go to the Privacy Report from your Safari menu and you'll get an in-depth overview of every cross-site tracker prevented over the last 30 days.

Privacy Report for each website

See the privacy practices for every website you visit. Just click the Privacy Report button in your Safari toolbar for a summary of all cross-site trackers prevented by Intelligent Tracking Prevention.

https://macmule.com/2015/11/18/deploy-updating-safari-extensions-on-safari-9/

macmule.com/2015/11/18/deploy-updating-safari-extensions-on-saf

Deploying & Updating Safari Extensions For Safari 9+ | macmule

EXTENSION ATTRIBUTE (5)
HOW TO (70)
INFO (7)
MUSING (15)
OSX SERVER (3)
PROJECT (18)
TALKS (29)
TIPS (12)
VULNERABILITY (4)

SIGN UP TO THE MULE'S MAILING LIST

Enter your email address to subscribe to this blog and receive notifications of new posts by email.

Email Address

SIGN ME UP!

Proudly powered by WordPress
Theme: Writr by WordPress.com.

2.1 Fool's Gold
2.2 Fool Me Once...
3 Updating Extensions
3.1 Fool's Errand
4 Not Suffering Fools Gladly

What Happened?

Back on 15/10/2014 I posted how to update "Safari Extensions" by replacing them on disk, I updated that method for Safari 8 & posted it on 25/09/15 here.

Safari 9 was released shortly after that last post on 30/9/15. With which, came the expected "About the security content of Safari 9" article.

Within that article, you'll find the below:

- Safari Extensions

  Available for: OS X Mavericks v10.9.5, OS X Yosemite v10.10.5 and OS X El Capitan v10.11

  Impact: Safari extensions may be replaced on disk

  Description: A validated, user-installed Safari extension could be replaced on disk without prompting the user. This issue was addressed by improved validation of extensions.

  CVE-ID

  CVE-2015-5780 : Ben Toms of macmule.com

Erm... Whoops! I didn't submit anything about my workaround to Apple, so someone either passed it on to Apple or someone at Apple read the post.

There are two main changes affecting Safari Extensions that came in with Safari 9.0 & these are dealt with in the following two sections.

(The starting formatted text in each section are taken from the What's New In Safari 9 developer documentation).

https://support.apple.com/en-gb/guide/mac-help/mchl0f9af76f/mac

support.apple.com/en-gb/guide/mac-help/mchl0f9af76f/mac

What is a signed system volume? - Apple Support

Mac iPad iPhone Watch TV Music Support

macOS User Guide

Communities Contact Support

macOS Big Sur 11.0

Search the user guide

Table of Contents

What is a signed system volume?

macOS Big Sur builds on the protection provided for your Mac in Mojave and Catalina by adding cryptographic technology that prevents access to or execution of files that don't have a valid cryptographic signature from Apple. All system files are protected on the signed system volume (SSV). This advanced system volume technology provides even greater security against malicious software and tampering with the operating system.

It also allows software updates to complete in the background while you work, which reduces the time it takes for your Mac to restart and complete updates.

See also

Ways to avoid malware and harmful apps on Mac

What is secure virtual memory on Mac?

Helpful? Yes No

Support > macOS User Guide > What is a signed system volume?

https://support.apple.com/en-gb/HT211911

support.apple.com/en-gb/HT211911

What's new for enterprise in macOS Big Sur – Apple Support

Mac iPad iPhone Watch TV Music Support

What's new for enterprise in macOS Big Sur

Find out more about the enterprise content that Apple has released for macOS Big Sur.

macOS updates improve the stability, performance or compatibility of your device and are recommended for all users. Device administrators can manage software updates using an MDM solution.

For information about general improvements, find out more about updates to macOS Big Sur.

macOS Big Sur 11.2

- On Mac computers with an Intel processor, you can now use the `startosinstall` command inside the macOS installer app located on a non-boot volume while booted to Recovery.
- Setting a custom umask now works as expected.
- MDM can now push a Kernel Extension Policy payload to a Mac with the Apple M1 chip and update boot security settings automatically.
- Resolves an issue where Mac computers managed by MDM were sometimes unable to retrieve software updates using System Preferences.
- Network Extension Content Filters can now monitor traffic from built-in binaries.
- Resolves an issue where users were unable to unlock System Preferences panes after upgrading to macOS Big Sur from macOS Catalina.

macOS Big Sur 11.1

- You can now install macOS on a Mac with Apple silicon while logged in with a mobile account.
- Addresses an issue where the PIN would not be accepted when attempting to authenticate with a smart card.

https://support.apple.com/en-gb/HT211911

support.apple.com/en-gb/HT211911

What's new for enterprise in macOS Big Sur – Apple Support

administrator credentials.

- Supports the RebuildKernelCache and KextPaths keys in the RestartDevice MDM command dictionary.
- Provides MDM support to allow standard users to permit Screen Recording or Input Monitoring in the Privacy pane of Security & Privacy preferences.
- Apple Push Notification service (APNs) traffic will correctly fall back to using a proxy if a direct connection is blocked by a firewall that doesn't send a TCP reset to clients.
- Hyperlinks in PDFs containing percent-encoded characters now open properly.
- Fixes an issue where attempting to change a password using the Kerberos SSO Extension would fail with an error message saying "Password Change Failed. Configuration file does not specify default realm".
- Addresses an issue where, after allowing a user to unlock a FileVault-protected startup volume, the user would not always appear in the list of users in the login window.
- Resolves an issue where, in certain cases, the Relocated Items folder could not be deleted.
- Addresses an issue where "Password requirements" in System Preferences didn't show when a password had met the requirements when multiple local policies were used.

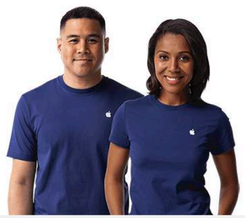
Published Date: February 09, 2021

Helpful? Yes No

Contact Apple Support

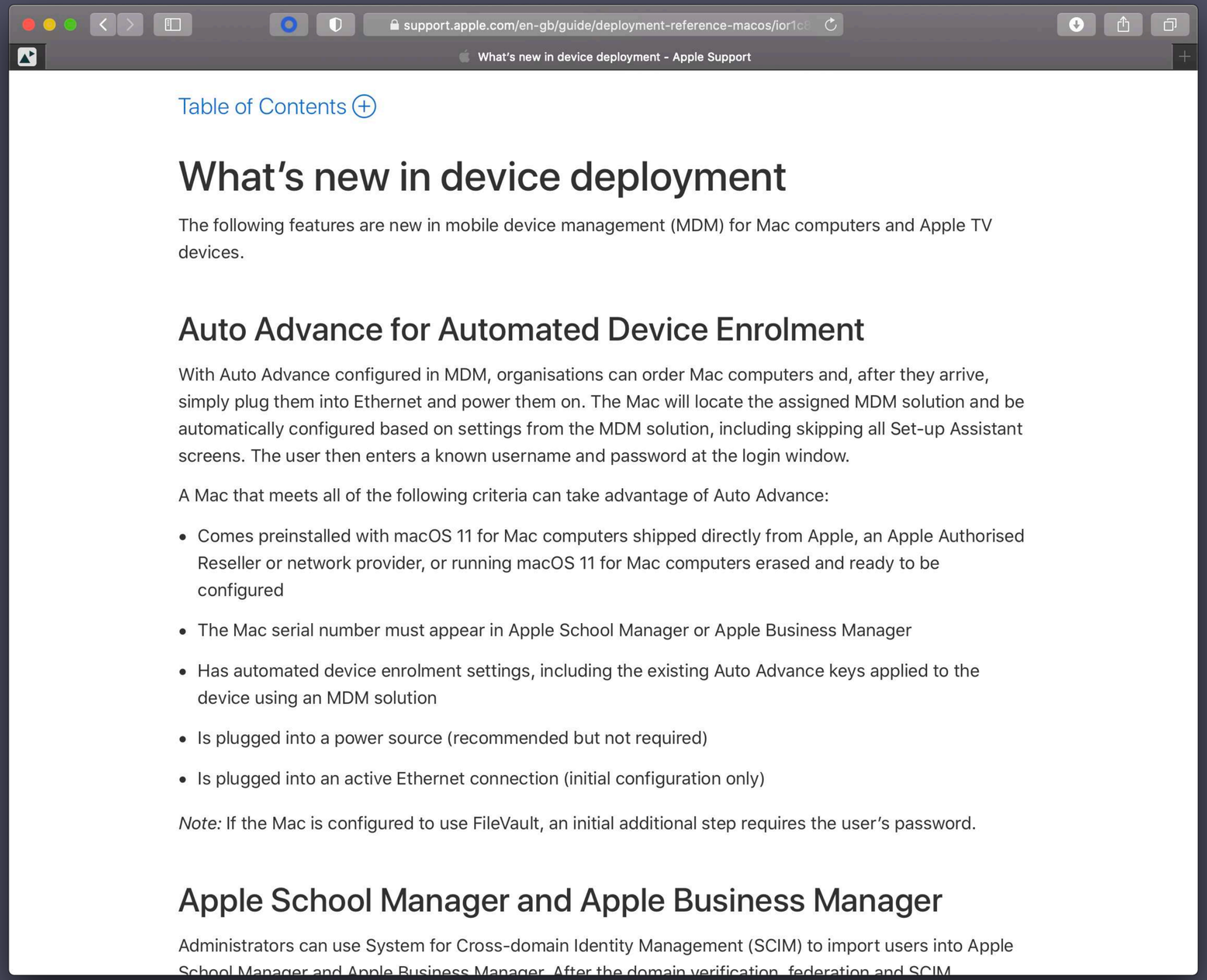
Need help? Save time by starting your support request online and we'll connect you to an expert.

Get started ›

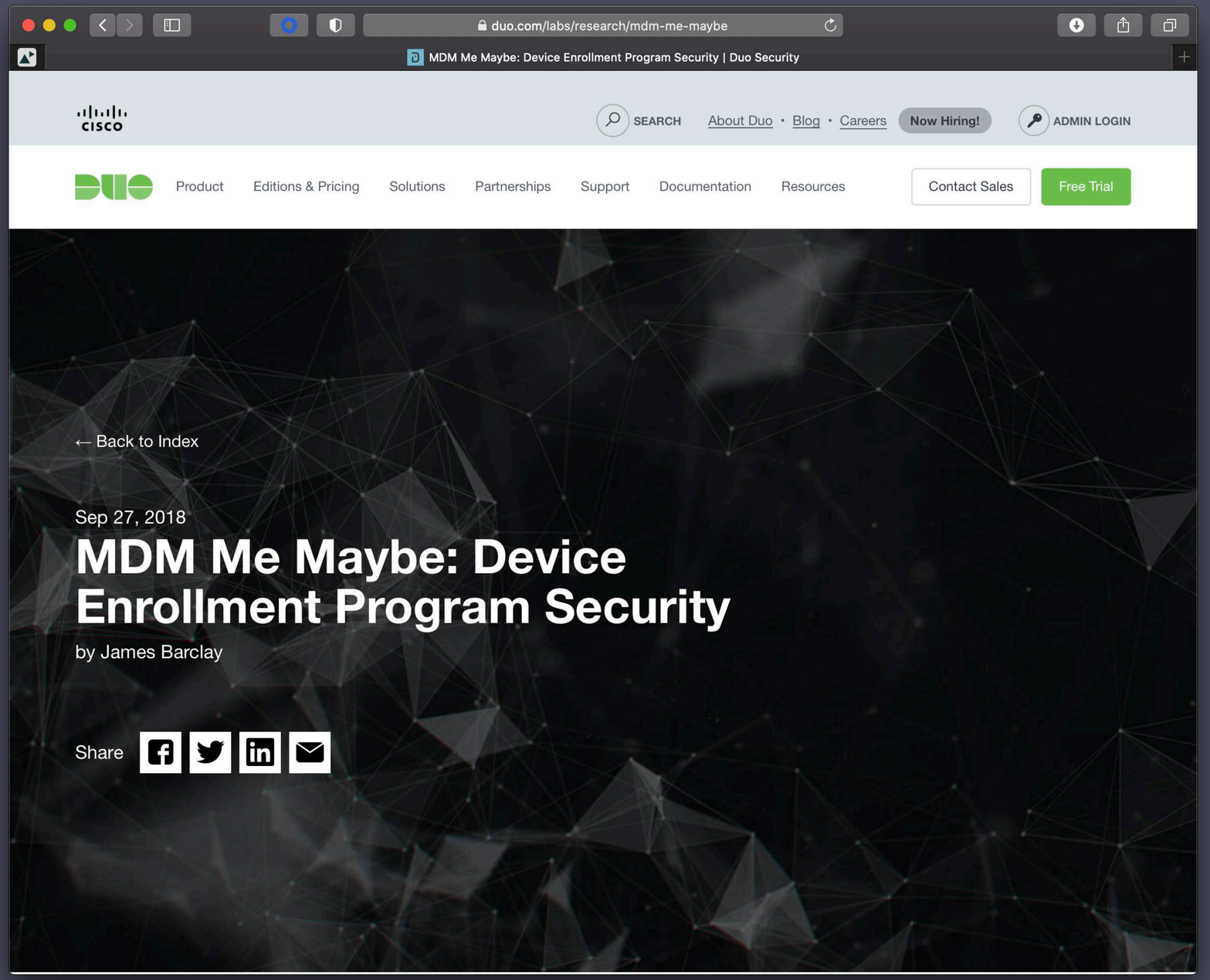


Support › What's new for enterprise in macOS Big Sur

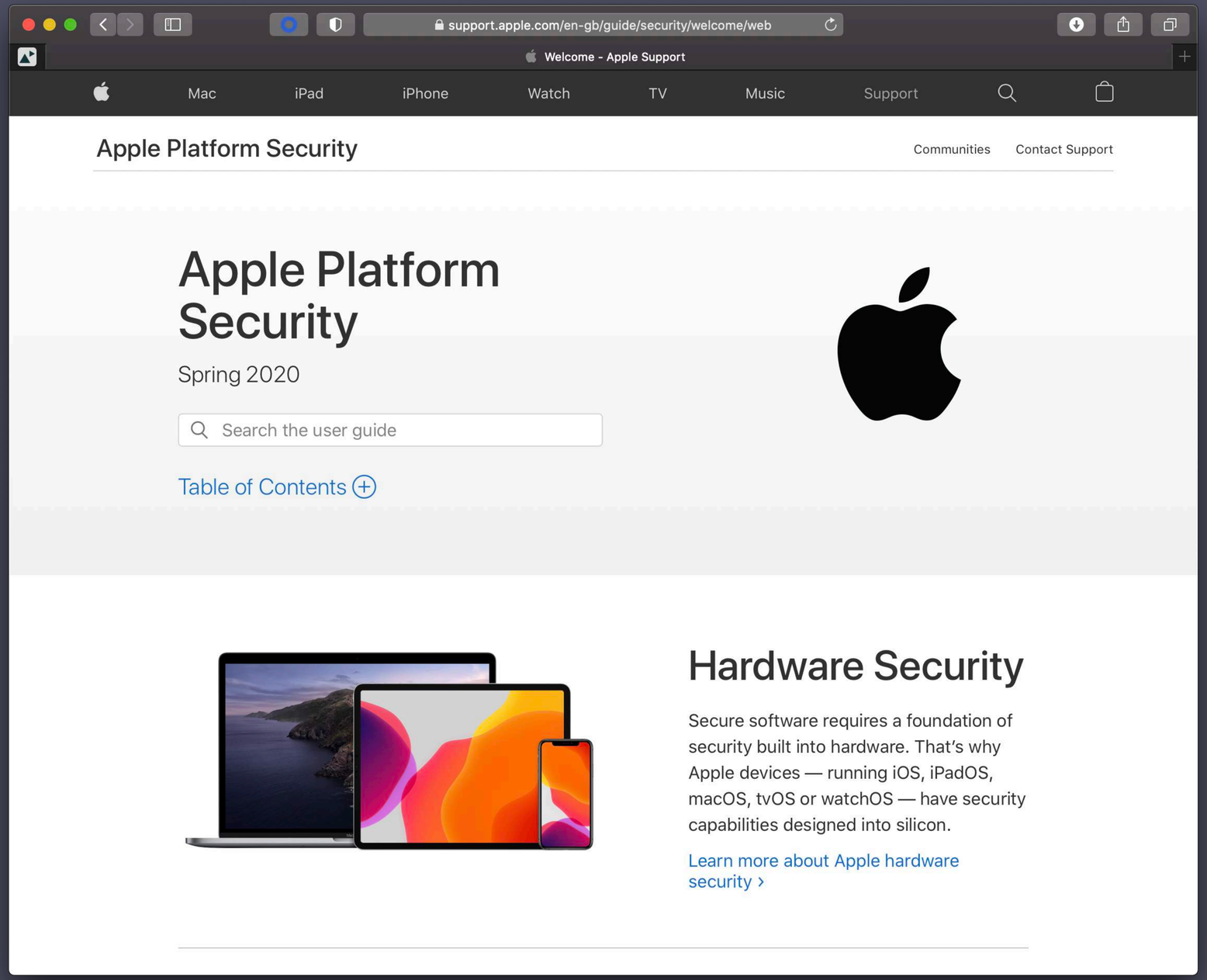
https://support.apple.com/en-gb/guide/deployment-reference-macos/ior1c8a0c6f4/web



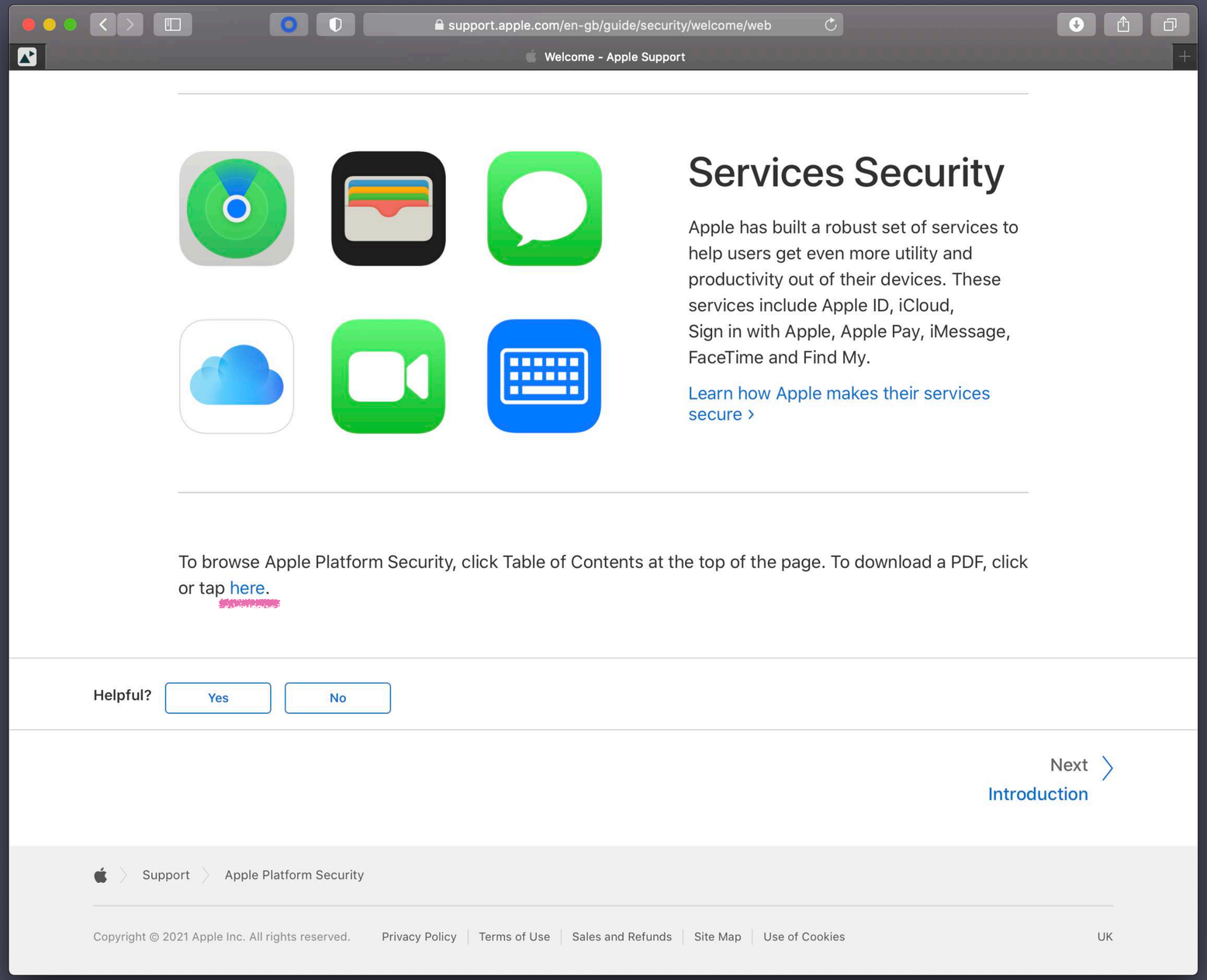
https://duo.com/labs/research/mdm-me-maybe



https://support.apple.com/en-gb/guide/security/welcome/web



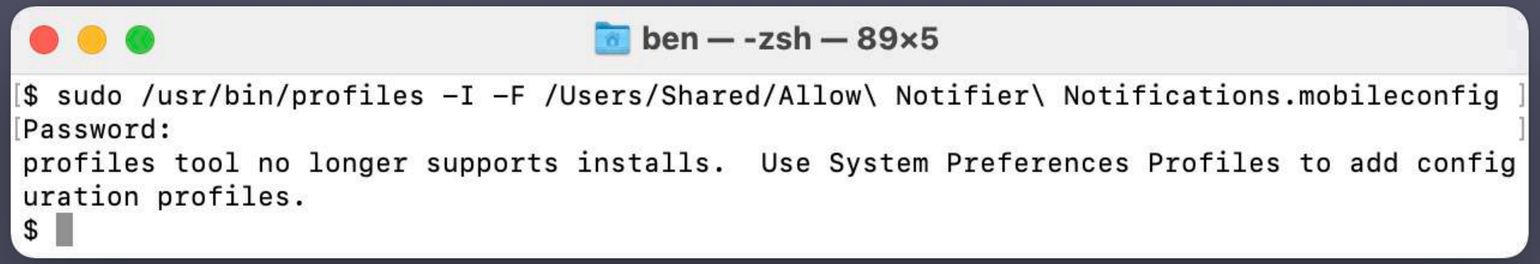
https://support.apple.com/en-gb/guide/security/welcome/web



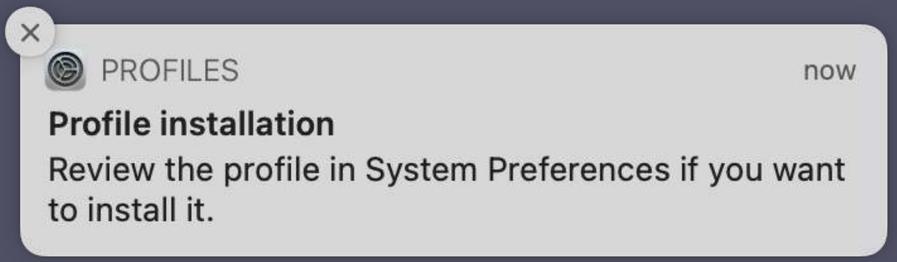
https://support.apple.com/en-gb/guide/security/welcome/web

Configuration Profiles

Configuration Profiles



Configuration Profiles



Configuration Profiles

Profiles

Search

Downloaded

Allow Notifier...
1 setting

Device (Managed)

Google Chrome
1 setting

Jamf Connect 2
1 setting

Jamf Connect...
1 setting

Jamf Connect...
2 settings

Managed Auto...
1 setting

Managed Disa...
1 setting

Managed Dock

Allow Notifier Notifications

dataJAR Ltd Unsigned

Ignore

Install...

Received 9 Mar 2021 at 11:18

Settings Notification Settings

DETAILS

Notification Settings

Description	Allow Notifier Notifications
Identifier	uk.co.dataJAR.NotifierNotifications
Notifications Enabled	True
Show In Lock Screen	True
Alert Type	Banners
Badges Enabled	True
Sounds Enabled	True
Critical Alert Enabled	False
Show In Notification	True

This Mac is supervised and managed by DATA JAR LTD.

Certificates

Certificates

```
[sh-3.2# sudo /usr/bin/security add-trusted-cert -d -r trustRoot -k /Library/Keyc]
hains/System.keychain /Users/ben/Downloads/some_ca.cer
SecTrustSettingsSetTrustSettings: The authorization was denied since no user int
eraction was possible.
sh-3.2#
```

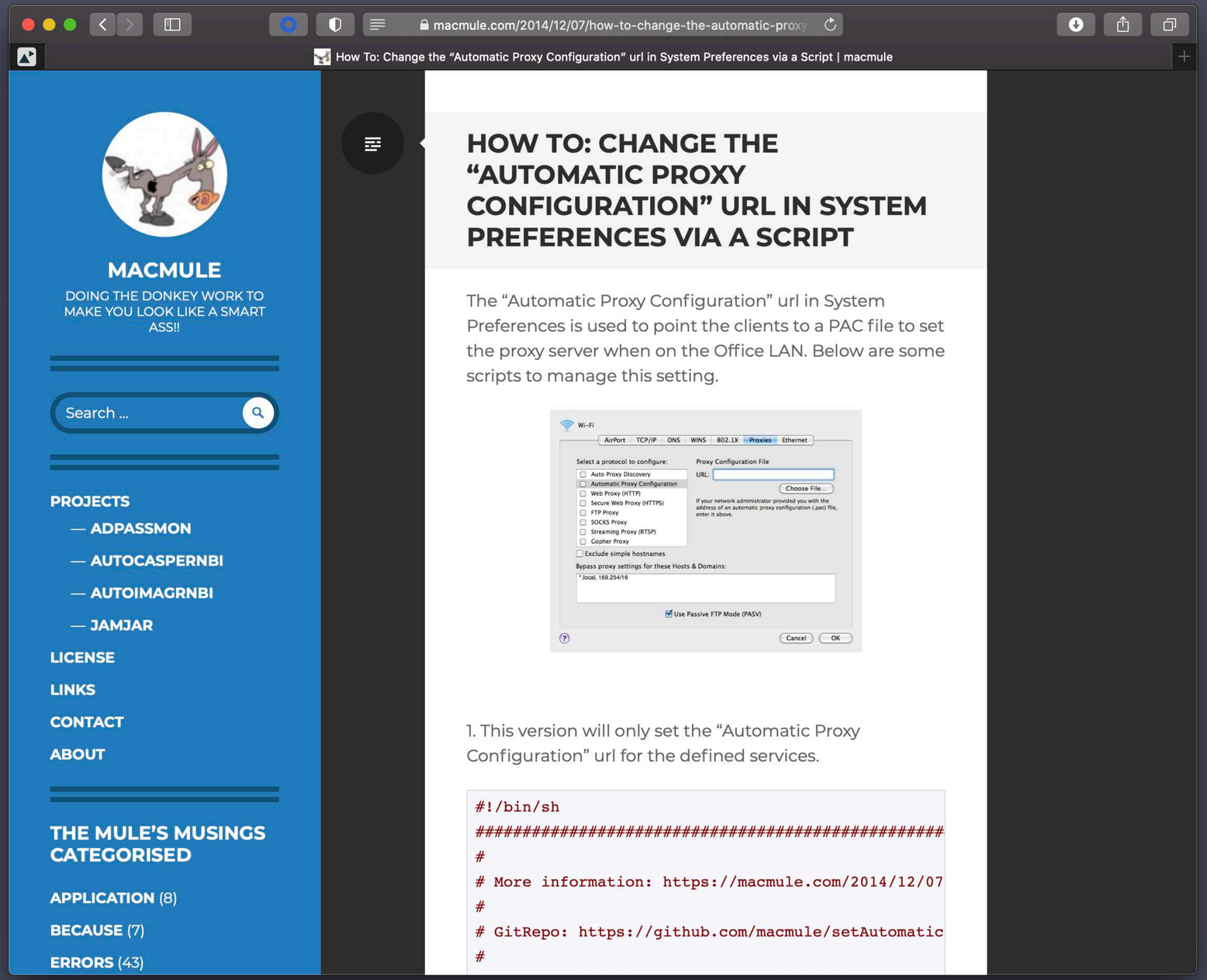
Certificates

networksetup

networksetup

```
$ /usr/sbin/networksetup -setautoproxyurl Wi-Fi "http://test"
** Error: Command requires admin privileges.
$
```

https://macmule.com/2014/12/07/how-to-change-the-automatic-proxy-configuration-url-in-system-preferences-via-a-script/



softwareupdate

softwareupdate

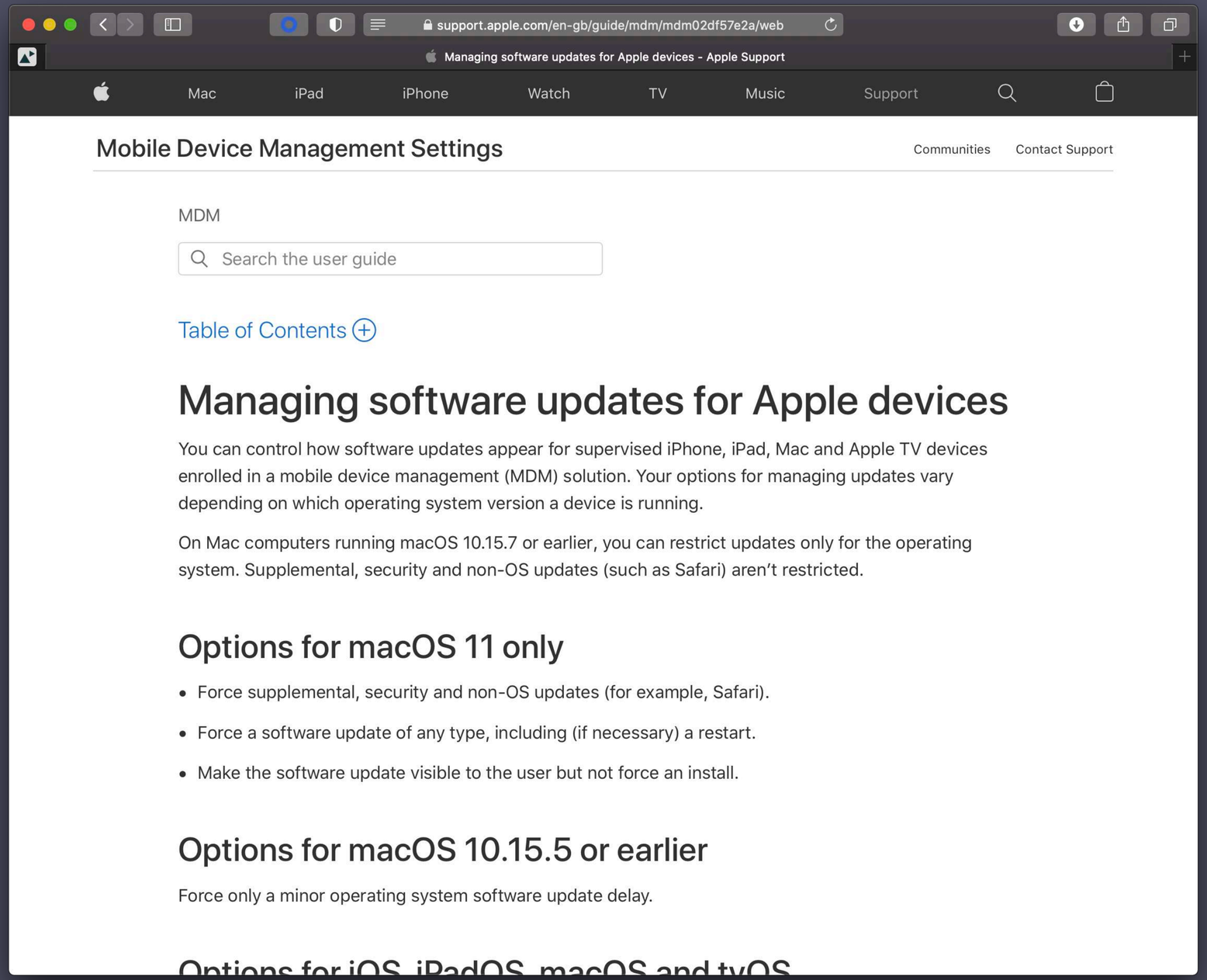
catalina

```
$ sudo softwareupdate --set-catalog https://mysus.com
Changed catalog to https://mysus.com

Changing the Software Update catalog is deprecated.
The ability to specify a custom catalog will be removed in a future release of macOS.
$
```

softwareupdate

softwareupdate



softwareupdate

github.com/jamf/NetSUS

jamf/NetSUS: NetBoot and Software Update Server

Community Contribution Polic...	Add files via upload	5 years ago
CreateNetSUSInstaller.sh	Re-Add DHCP for NetBoot	2 years ago
LICENSE	LICENSE	3 years ago
README.md	Update README.md	15 days ago

README.md

NetSUS Downloads

Installer: https://github.com/jamf/NetSUS/releases/download/5.0.2/NetSUSLPInstaller_5.0.2.run

OVA: https://github.com/jamf/NetSUS/releases/download/5.0.2/NetSUSLP_5.0.2.ova

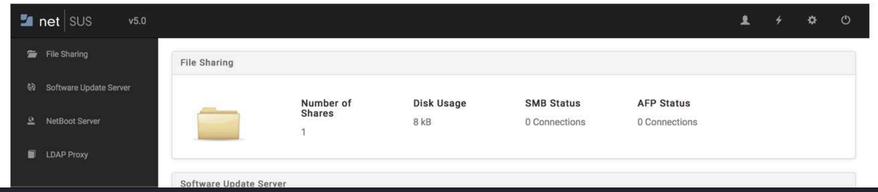
Deprecation Notice

NetBoot and Software Update services have been deprecated by Apple, and as such this project will no longer be receiving further updates.

On 19-March-2021 this repository will be archived.

What is NetSUS?

The NetSUSLP allows you to host an internal software update server (SUS), a NetBoot server, file shares, and a LDAP Proxy server **all on the same Linux system**. For a list of supported Linux distributions see Requirements.



Contributors 19

+ 8 contributors

Languages

- PHP 48.7%
- Shell 20.0%
- Python 18.6%
- JavaScript 8.4%
- CSS 4.0%
- Roff 0.3%

Summary

Apple Silicon

Apple Silicon

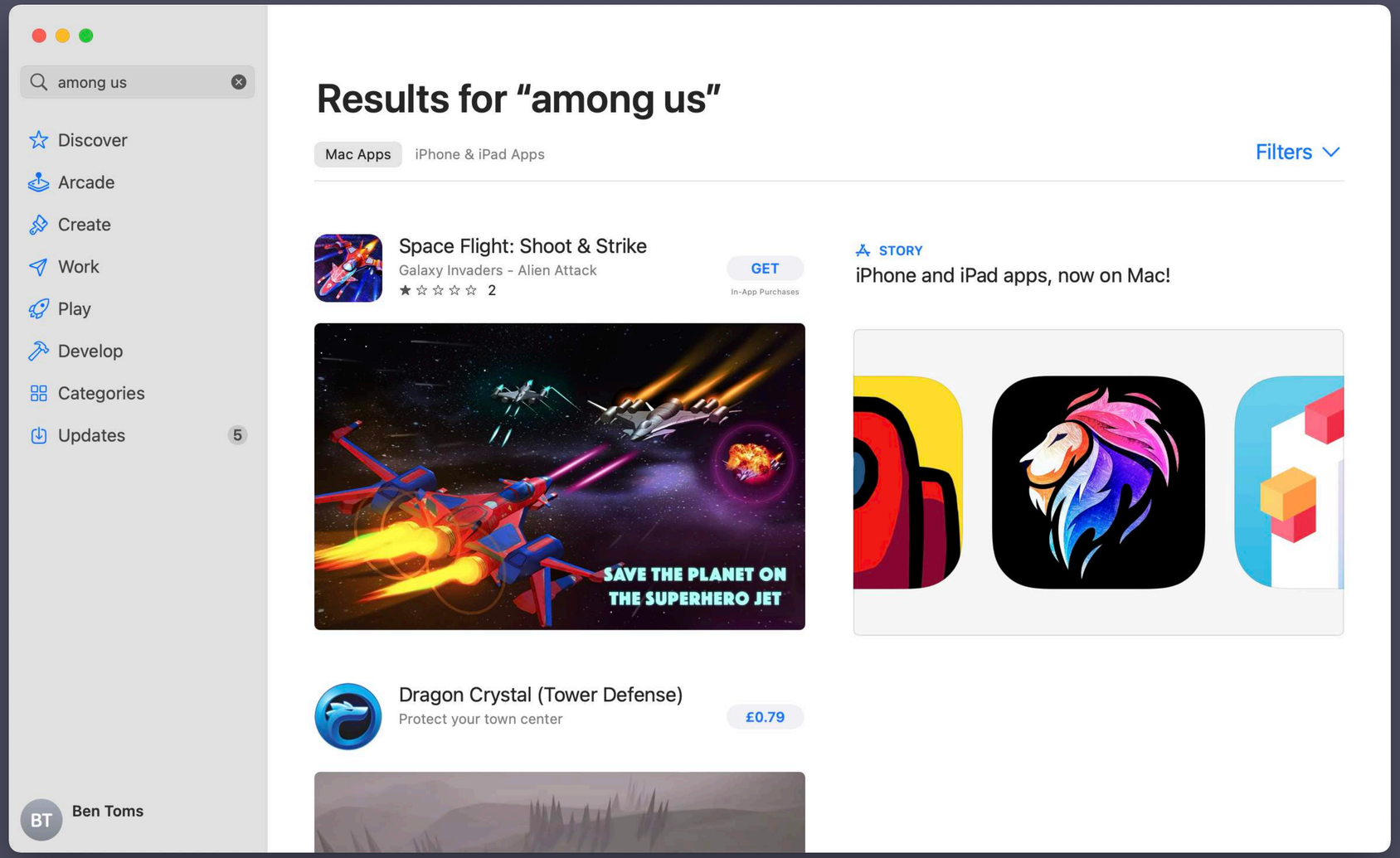
iOS and iPadOS apps

Rosetta

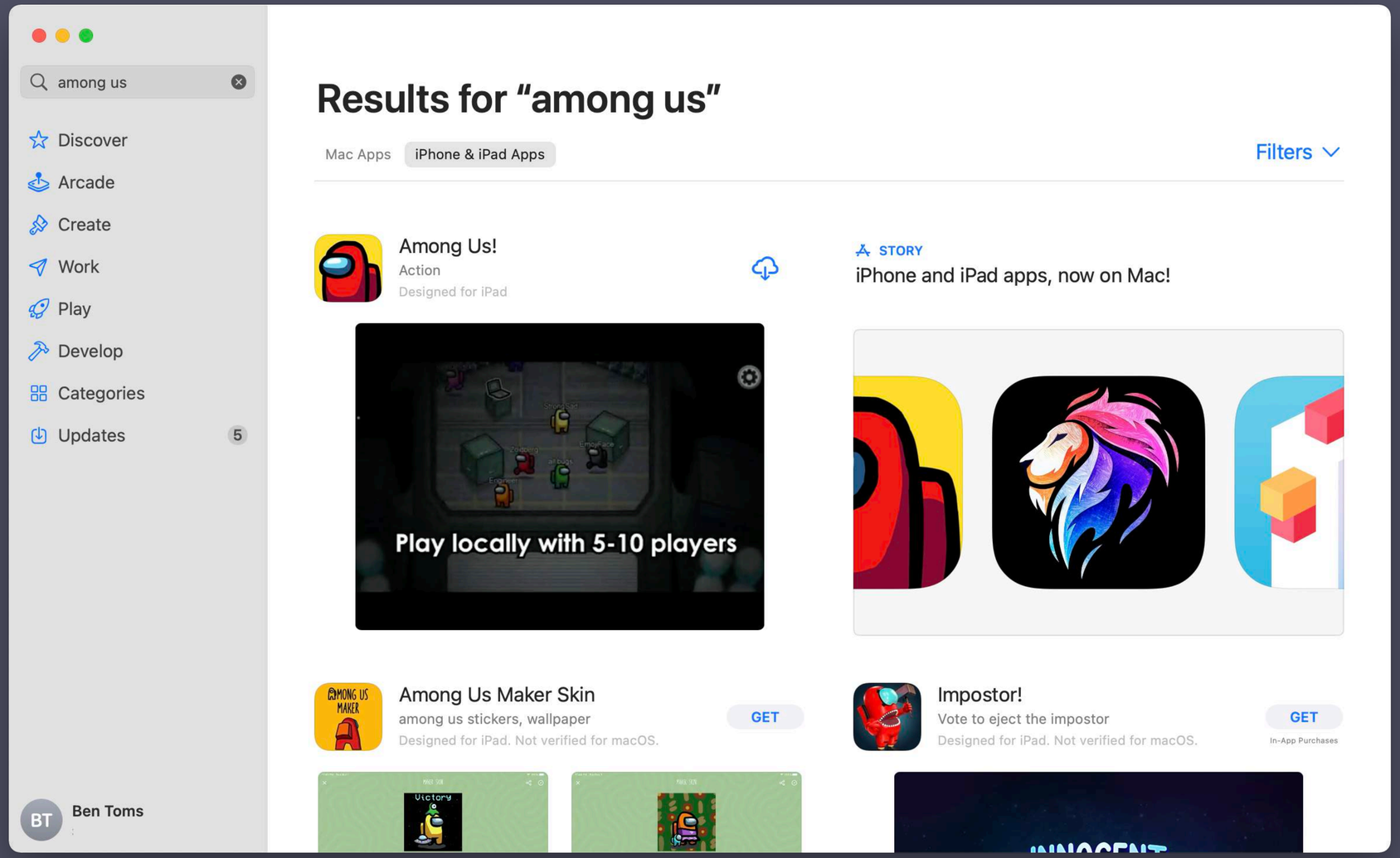
Volume Ownership

iOS and iPadOS Apps

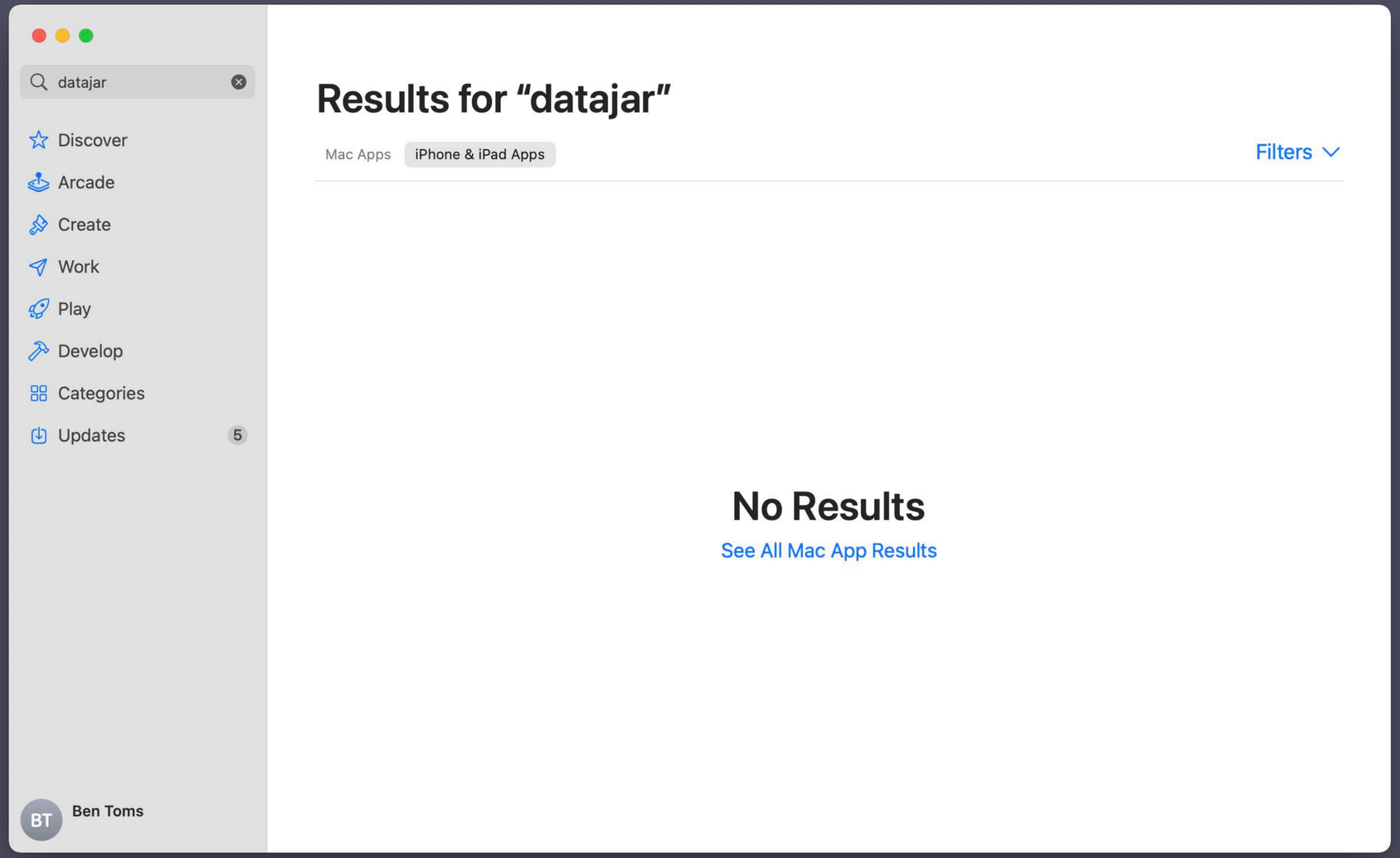
iOS and iPadOS Apps



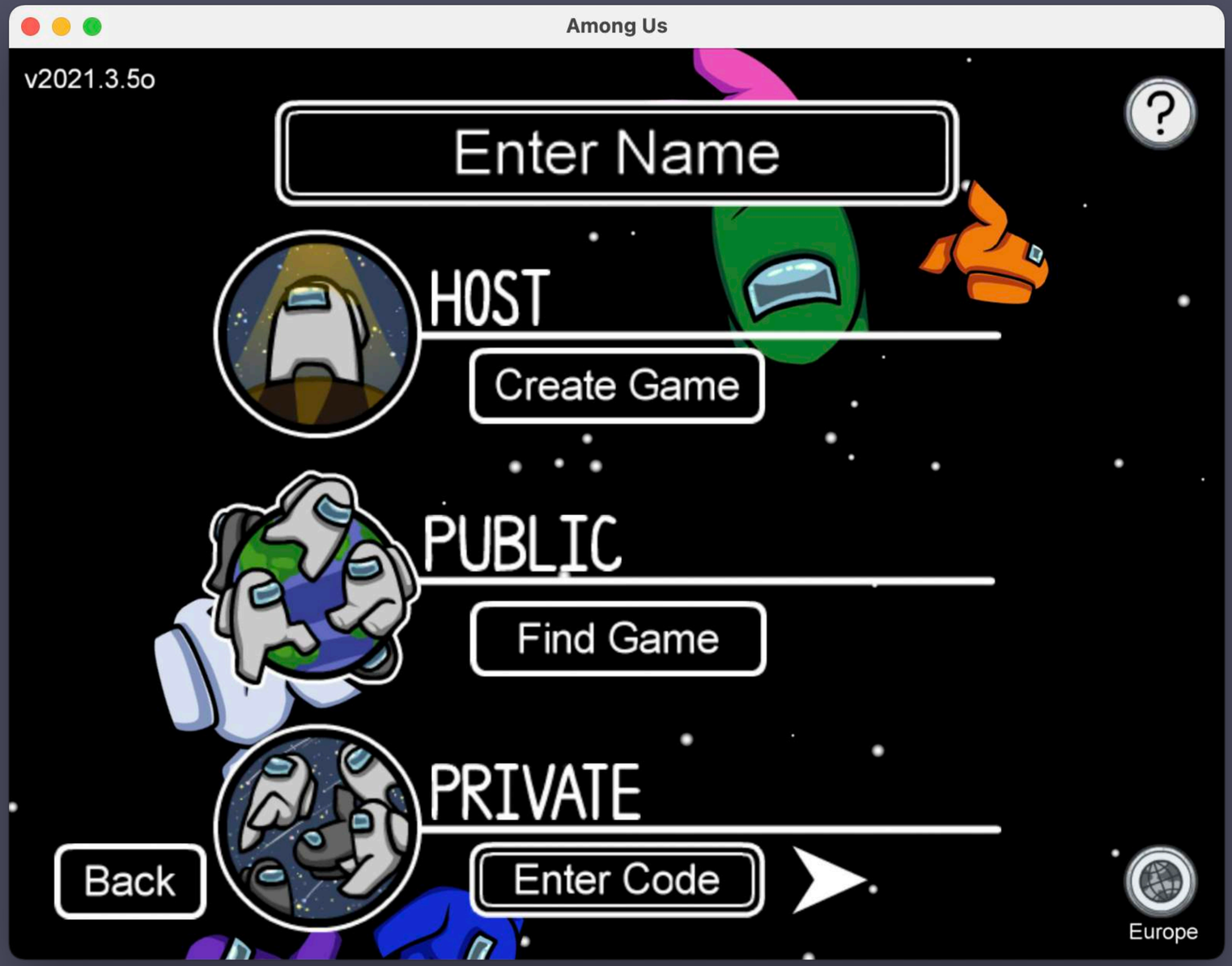
iOS and iPadOS Apps



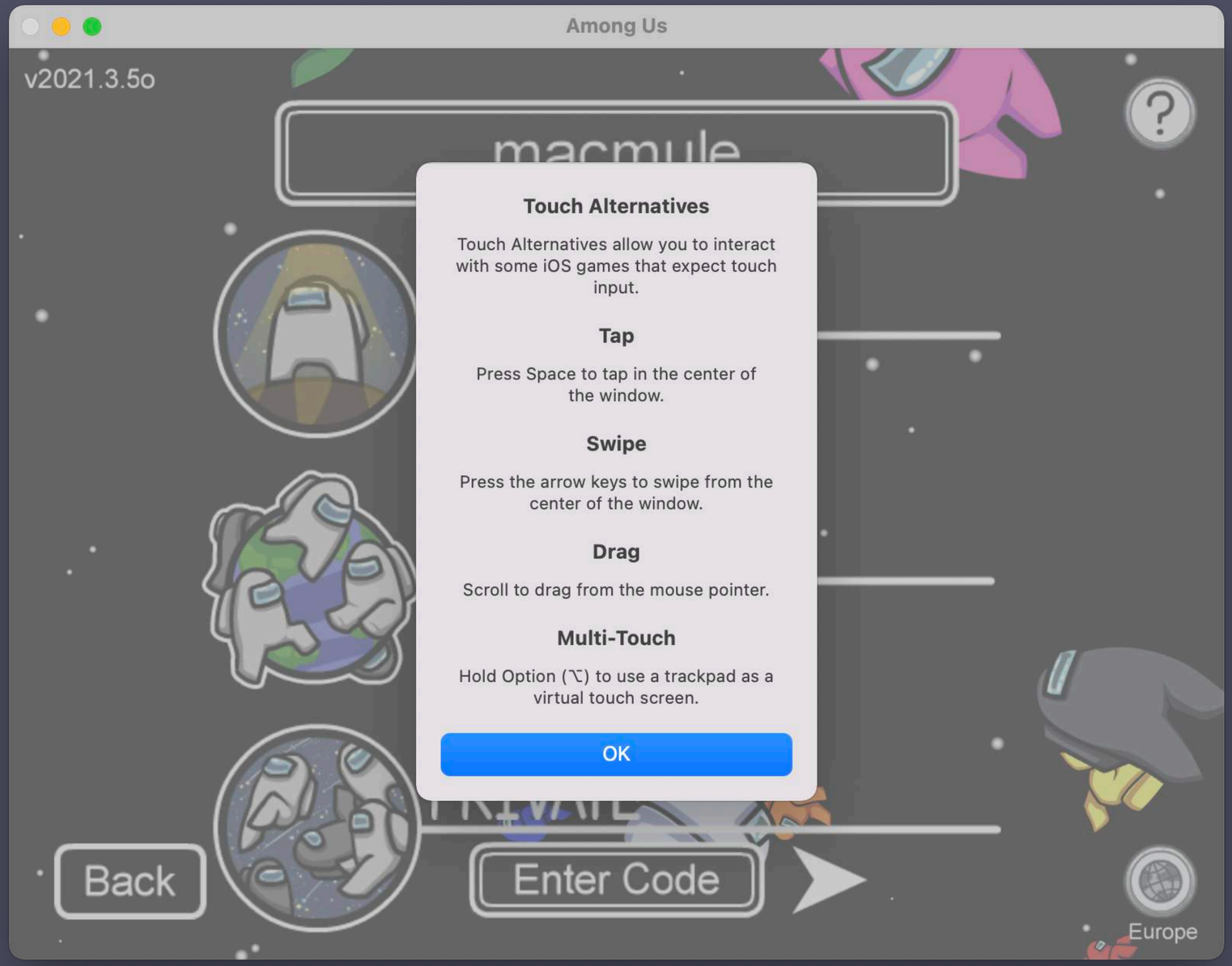
iOS and iPadOS Apps



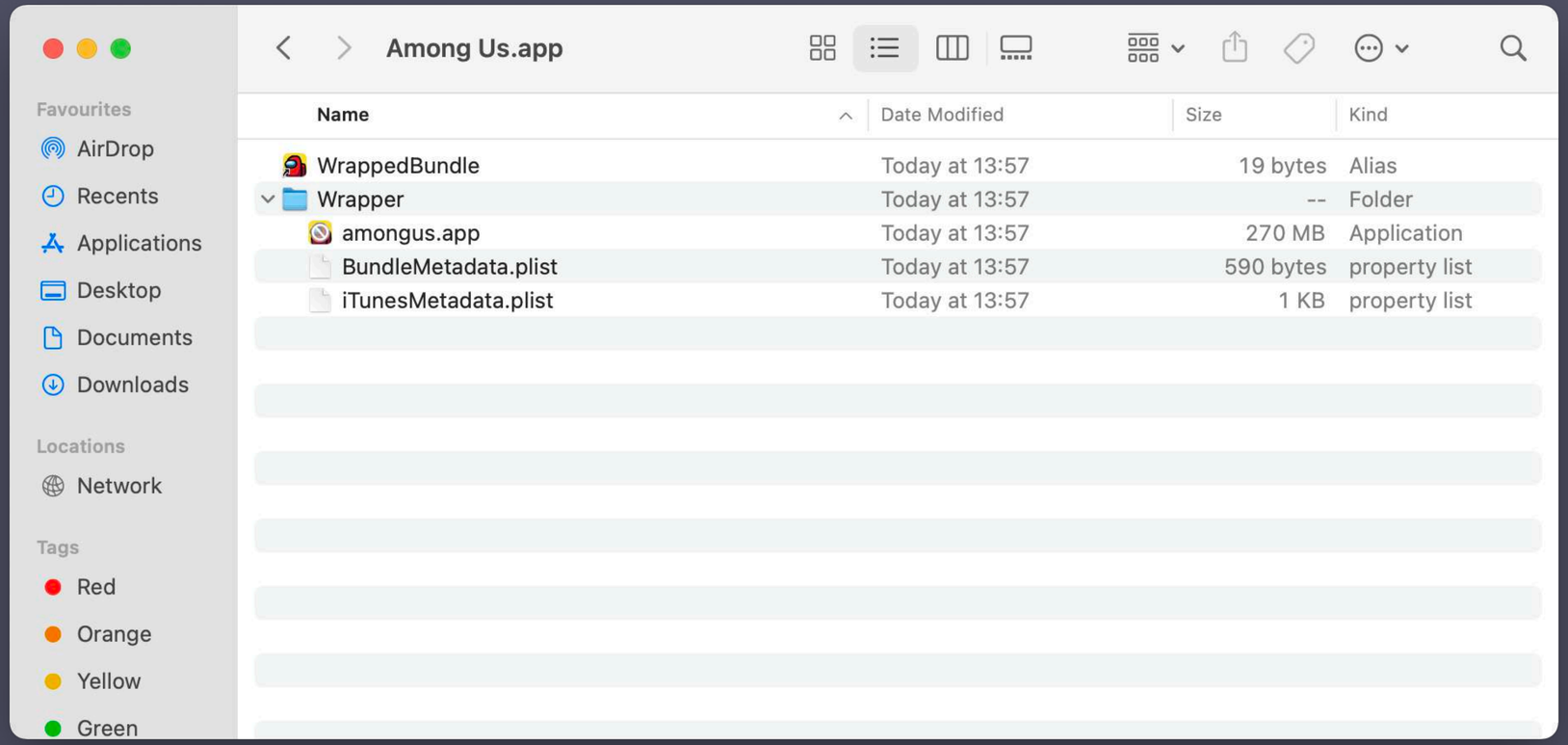
iOS and iPadOS Apps



iOS and iPadOS Apps



iOS and iPadOS Apps



iOS and iPadOS Apps

Inventory | Management | History

- General
- Hardware
  MacBook Air (M1, 2020)
- Operating System
  macOS 11.2.2
- User and Location
- Security
- Purchasing
- Storage
  1 Drive
- Extension Attributes
- Disk Encryption
  Encrypted

Applications

Computer Inventory Collection Settings

NAME	VERSION	PATH	APP STORE
Activity Monitor.app	10.14	/System/Applications/Utilities/Activity Monitor.app	No
AirPort Utility.app	6.3.9	/System/Applications/Utilities/AirPort Utility.app	No
Among Us.app	2021.3.5	/Applications/Among Us.app	No
App Store.app	3.0	/System/Applications/App Store.app	No
Audio MIDI Setup.app	3.5	/System/Applications/Utilities/Audio MIDI Setup.app	No
AutoCasperNBI.app	1.5.2	/Applications/AutoCasperNBI.app	No
AutoDMG.app	1.9	/Applications/AutoDMG.app	No
AutoImagrNBI.app	1.5.2	/Applications/AutoImagrNBI.app	No
Automator.app	2.10	/System/Applications/Automator.app	No
Bluetooth File Exchange.app	8.0.3	/System/Applications/Utilities/Bluetooth File Exchange.app	No
Books.app	3.1	/System/Applications/Books.app	No
Boot Camp Assistant.app	6.1.0	/System/Applications/Utilities/Boot Camp Assistant.app	No
Calculator.app	10.16	/System/Applications/Calculator.app	No
Calendar.app	11.0	/System/Applications/Calendar.app	No
Chess.app	3.18	/System/Applications/Chess.app	No

Rosetta

Rosetta

ben — less ◂ man productbuild — 89×28

NOTE: Some of the other requirements imply their own minimum system versions, which may override the values set here. This is noted below where applicable.

o The **arch** key specifies the supported architectures, e.g. x86_64 and/or arm64. Note that i386 infers x86_64, for compatibility reasons.

NOTE: On Apple Silicon, the macOS Installer will evaluate the product's distribution under Rosetta 2 unless the **arch** key includes the arm64 architecture specifier. Some distribution properties may be evaluated differently between Rosetta 2 and native execution, such as the predicate specified by the **sysctl-requirements** key. If the distribution is evaluated under Rosetta 2, any package scripts inside of product will be executed with Rosetta 2 at install time.

NOTE: Starting on macOS 11.0 (Big Sur), **productbuild** will automatically specify support for both arm64 and x86_64 unless a custom value for **arch** is provided.

o The **ram** key specifies the minimum amount of RAM required, in gigabytes.

o The **gl-renderer** key specifies a predicate, against which each of the OpenGL hardware renderers will be checked. For the product to be installed, at least one of the renderers must match the requirements of the predicate. The given predicate string must be convertible to

:

Volume Ownership

Volume Ownership

“Access to the Owner Identity Key (OIK) is referred to as "Ownership." Ownership is required to allow users to resign the LocalPolicy after making policy or software changes. The OIK is protected with the same key hierarchy as described in Sealed Key Protection (SKP), with the OIK being protected by the same Key encryption key (KEK) as the Volume encryption key (VEK).”

Page 36 - Apple Platform Security 2021

Volume Ownership

Account created via Setup Assistant

Account has logged into the Mac

Volume Ownership

Work in conjunction with an accounts administrative rights

Volume Ownership

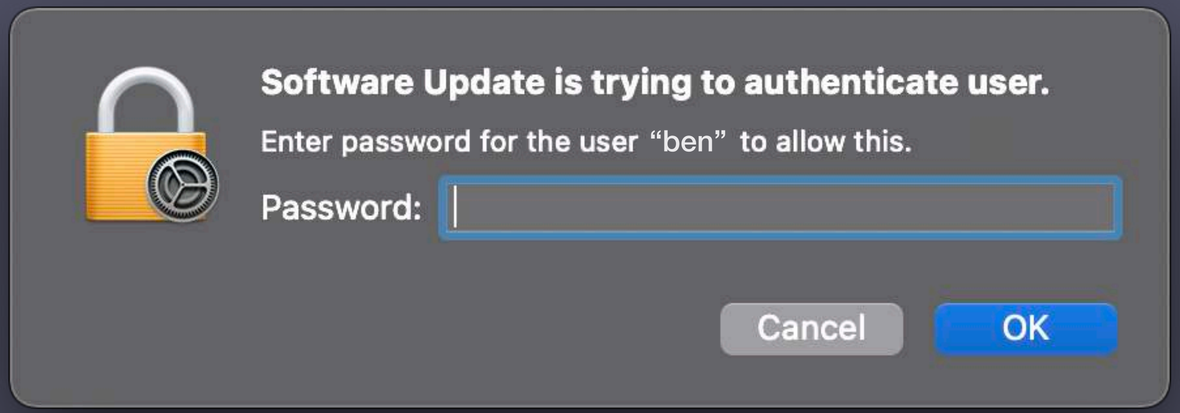
Change Boot Policy Security

Approve Kernel Extensions

Install Software Updates

Install an OS to a partition

Volume Ownership



Volume Ownership

https://github.com/
macadmins/nudge

Volume Ownership

apple-platform-security-guide (page 181 of 196)

Search

Lost Mode

If a supervised iOS or iPadOS device with iOS 9 or later is lost or stolen, an MDM administrator can remotely enable Lost Mode on that device. When Lost Mode is enabled, the current user is logged out and the device can't be unlocked. The screen displays a message that can be customized by the administrator, such as displaying a phone number to call if the device is found. When the device is put into Lost Mode, the administrator can request the device to send its current location (even if Location Services are off) and, optionally, play a sound. When an administrator turns off Lost Mode, which is the only way the mode can be exited, the user is informed of this action through a message on the Lock Screen or an alert on the Home screen.

Remote wipe, and remote lock

iOS, iPadOS, and macOS devices can be erased remotely by an administrator or user (instant remote wipe is available only if the Mac has FileVault enabled). Instant remote wipe is achieved by securely discarding the media key from Effaceable Storage, rendering all data unreadable. A remote wipe command can be initiated by mobile device management (MDM), Microsoft Exchange ActiveSync, or iCloud. On a Mac, the computer sends an acknowledgment and performs the wipe. With a remote lock, MDM requires that a six-digit passcode be applied to the Mac, rendering any user locked out until this passcode is typed in.

Note: Remote lock isn't available for a Mac with Apple silicon.

When a remote wipe command is triggered by MDM or iCloud, the device sends an acknowledgment and performs the wipe. For remote wipe through Microsoft Exchange ActiveSync, the device checks in with the Microsoft Exchange Server before performing the wipe. Remote wipe isn't possible in the following situations:

- With User Enrollment
- Using Microsoft Exchange ActiveSync when the account that was installed with User Enrollment
- Using Microsoft Exchange ActiveSync if the device is supervised

Users can also wipe iOS and iPadOS devices in their possession using the Settings app. And as mentioned, devices can be set to automatically wipe after a series of failed passcode attempts.

MacBook Pro

MacBook Pro

https://macadmins.org

#applesilicon

#bigsur

#code42

#datajar