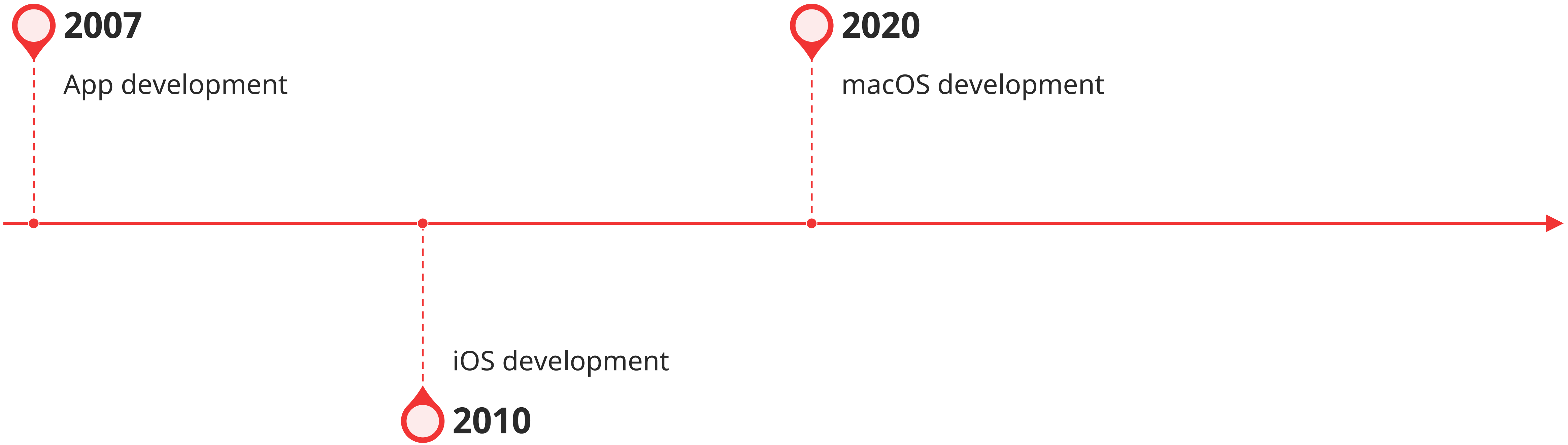
Vasyl Liutikov

Implementing MDM: a view from the perspective of the macOS developer

AnyDesk

Vasyl Liutikov



2007

App development

2010

iOS development

2020

macOS development

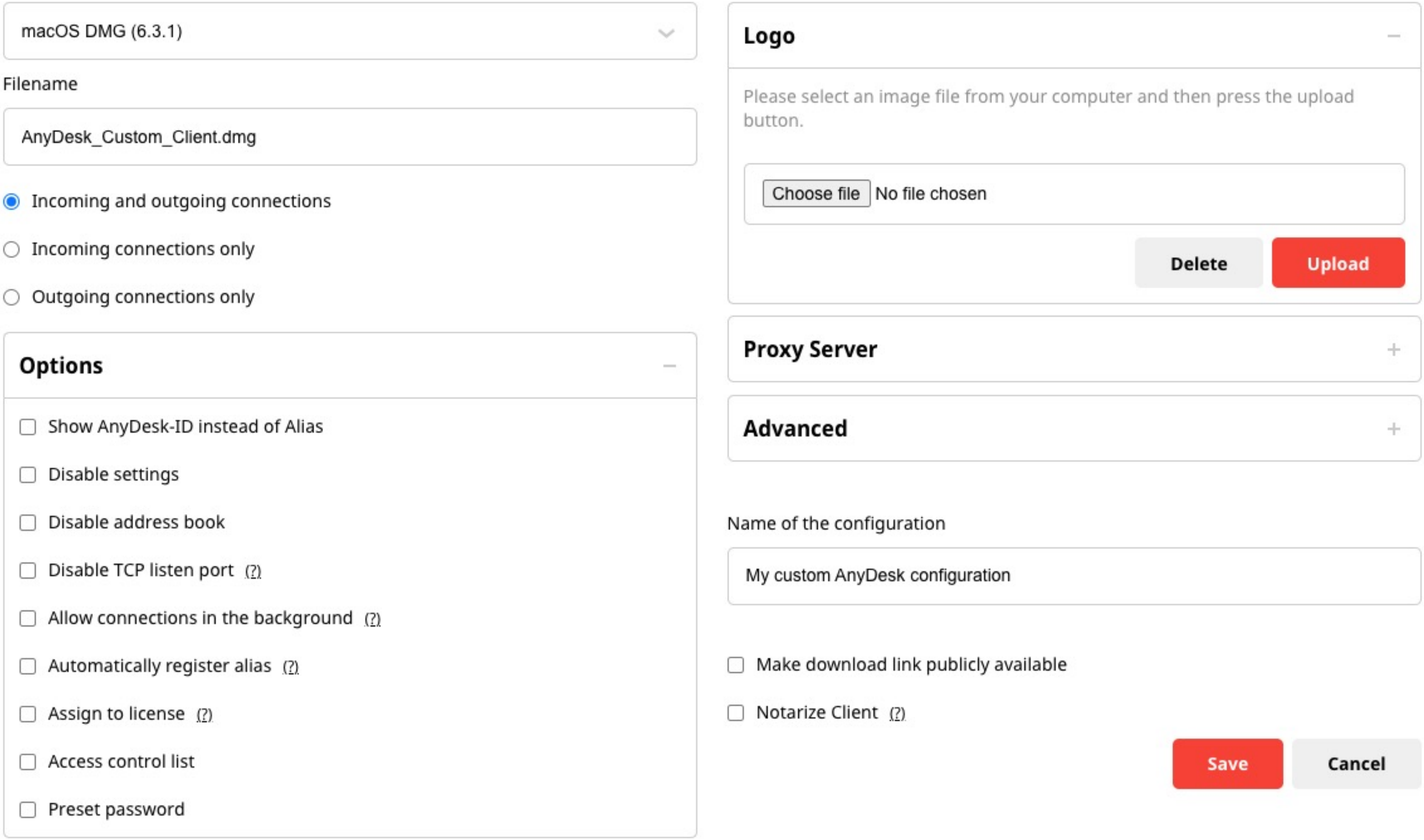
- AnyDesk is ...

More than 400 000 000 downloads

More than 900 000 000 sessions per month

More 67 000 000 km bridged across the globe per month

Works on Windows, Linux, Android, FreeBSD, Raspberry Pi, Chrome OS, iOS, tvOS and macOS



macOS DMG (6.3.1)

Filename

AnyDesk_Custom_Client.dmg

● Incoming and outgoing connections

○ Incoming connections only

○ Outgoing connections only

Options

□ Show AnyDesk-ID instead of Alias

□ Disable settings

□ Disable address book

□ Disable TCP listen port (?)

□ Allow connections in the background (?)

□ Automatically register alias (?)

□ Assign to license (?)

□ Access control list

□ Preset password

Logo

Please select an image file from your computer and then press the upload button.

No file chosen

Proxy Server +

Advanced +

Name of the configuration

My custom AnyDesk configuration

□ Make download link publicly available

□ Notarize Client (?)

The three main problems are:

- The app distribution
- The app provisioning
- The app permissions

Mac app distribution

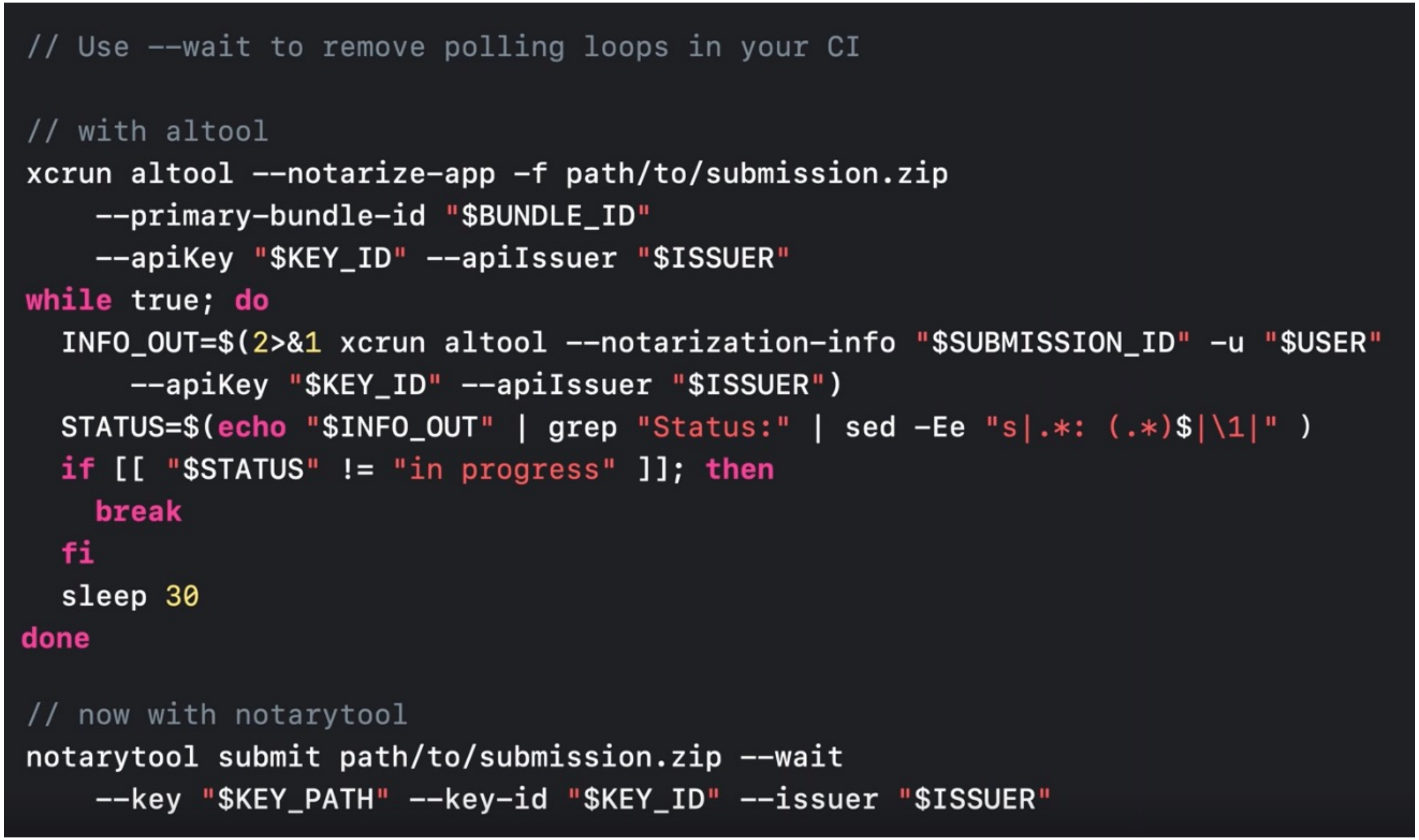
Steps:

- Build the app
- Sign it with Developer id certificate
- Notatize and stamp it
- Create PKG file

Alternatives?

- Munki
- Home brew cask

Changes in notarization



```
// Use --wait to remove polling loops in your CI

// with altool
xcrun altool --notarize-app -f path/to/submission.zip
    --primary-bundle-id "$BUNDLE_ID"
    --apiKey "$KEY_ID" --apiIssuer "$ISSUER"
while true; do
  INFO_OUT=$(2>&1 xcrun altool --notarization-info "$SUBMISSION_ID" -u "$USER"
      --apiKey "$KEY_ID" --apiIssuer "$ISSUER")
  STATUS=$(echo "$INFO_OUT" | grep "Status:" | sed -Ee "s|.*: (.*)$|\1|" )
  if [[ "$STATUS" != "in progress" ]]; then
    break
  fi
  sleep 30
done

// now with notarytool
notarytool submit path/to/submission.zip --wait
    --key "$KEY_PATH" --key-id "$KEY_ID" --issuer "$ISSUER"
```

https://developer.apple.com/videos/play/wwdc2021/10261/
https://developer.apple.com/documentation/security/notarizing_macos_software_before_distribution/customizing_the_notarization_workflow

SUEnableAutomacticChecks

NSUserDefaults

- `defaults write -app MacApp SUEnableAutomaticChecks -bool false`

- `[defaults setBool:NO forKey:@"SUEnableAutomaticChecksKey"];`

- `<key>SUEnableAutomaticChecks</key>`
- ` <false/>`

- `BOOL isProvision = [defaults objectIsForcedForKey:@"SUEnableAutomaticChecksKey"];`

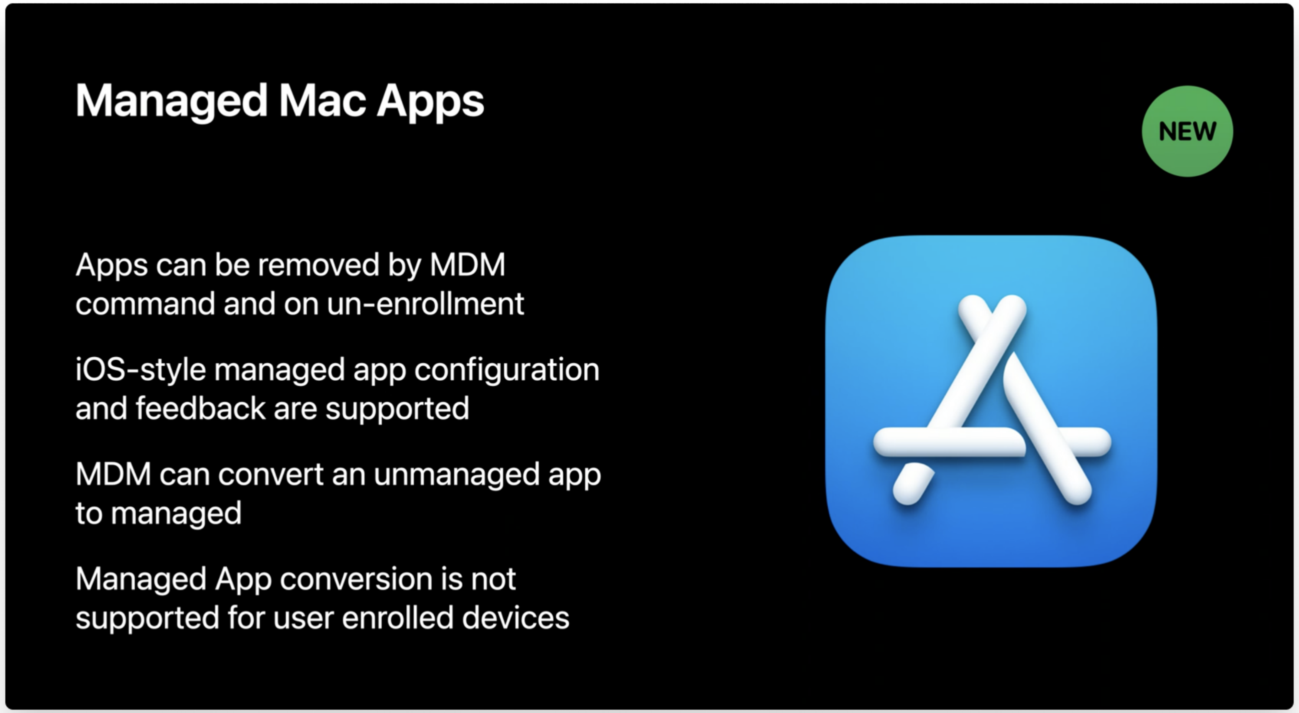
https://support.apple.com/en-gb/guide/mdm/mdmcdc2bfa19/web

iOS?

- `com.apple.configuration.managed`

- Session 301 Extending Your Apps for Enterprise and Education
- https://developer.apple.com/videos/play/wwdc2013/301/?t=1411

- MacOS 11 managed app?
- https://developer.apple.com/videos/play/wwdc2020/10639



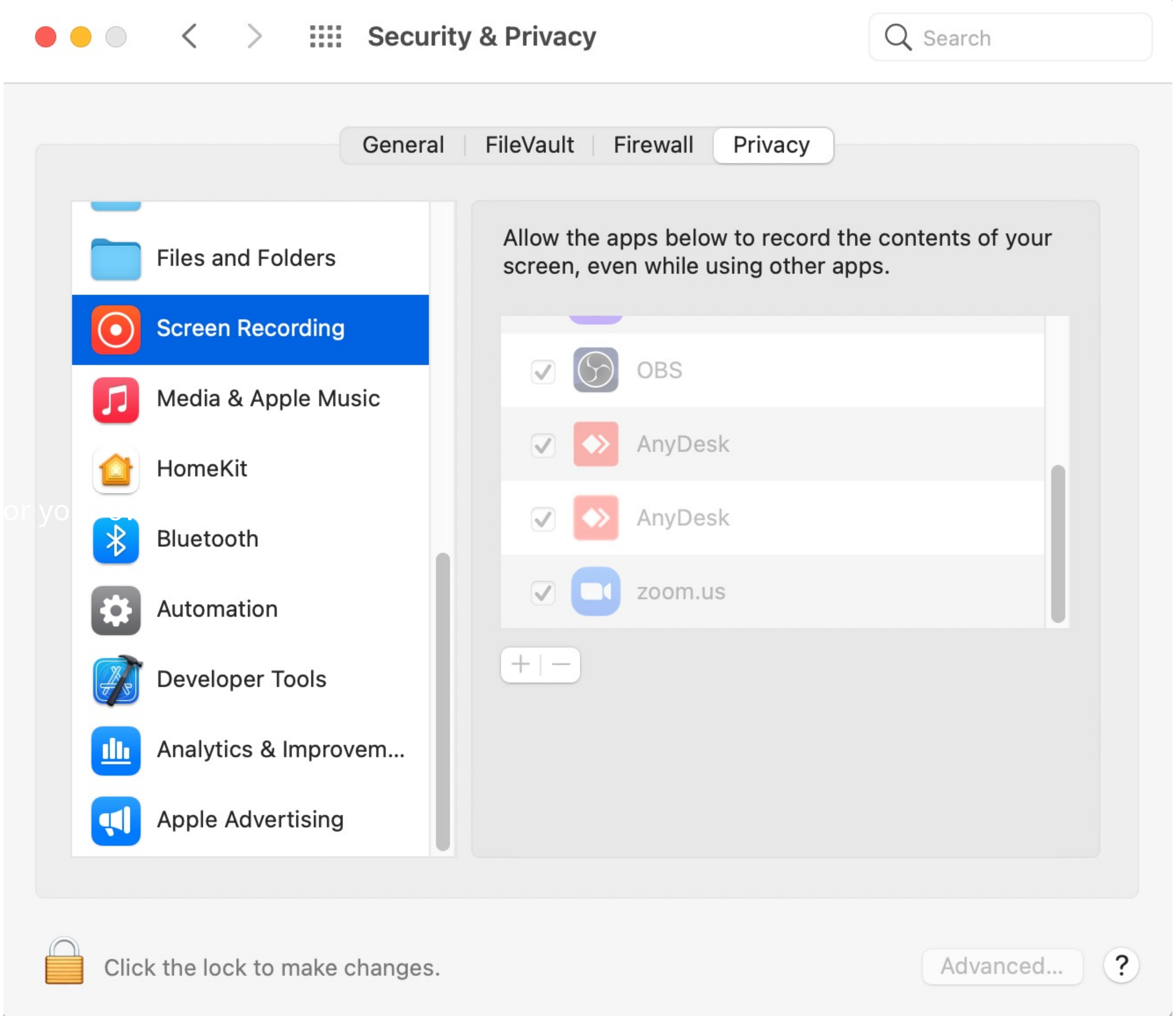
Managed Mac Apps

Apps can be removed by MDM command and on un-enrollment

iOS-style managed app configuration and feedback are supported

MDM can convert an unmanaged app to managed

Managed App conversion is not supported for user enrolled devices



Allow the apps below to record the contents of your screen, even while using other apps.

☑ OBS

☑ AnyDesk

☑ AnyDesk

☑ zoom.us

Click the lock to make changes.

PPPC - Privacy Preferences Policy Control

- Advances in macOS Security
- https://developer.apple.com/videos/play/wwdc2019/701/

- More info
- https://support.apple.com/guide/mdm/mdm38df53c2a/web

- Example
- https://support.apple.com/guide/mdm/mdm9ddb7e0b5/1/web/1.0#mdm0ab57a6be

- Payload best practices for Apple devices
- https://support.apple.com/guide/mdm/mdm8hdx05218/1/web/1.0

Screen recording permission example

```
<key>ScreenCapture</key>
<array>
        <dict>
                <key>Identifier</key>
                <string>com.apple.Terminal</string>
                <key>IdentifierType</key>
                <string>bundleID</string>
                <key>CodeRequirement</key>
                <string>identifier "com.apple.Terminal" and anchor apple</string>
                <key>Authorization</key>
                <string>AllowStandardUserToSetSystemService</string>
        </dict>
</array>
```

Workarounds?

- Disable SIP - system integration protection
- Edit manually TCC database tccutil
- `/Users/[username]/Library/Application Support/com.apple.TCC/TCC.db`

-
  ```
  sqlite3 "/Users/vliutikov/Library/Application Support/com.apple.TCC/TCC.db" 'SELECT * FROM access;’
  ```

-
  ```
  sqlite3 "/Users/vliutikov/Library/Application Support/com.apple.TCC/TCC.db" 'SELECT * FROM access
  where service=="kTCCServiceCamera";’
  ```

- Reset all permissions
- `sudo tccutil reset All [app.bundle.id]`

Useful software

- Suspicious Package
- https://www.mothersruin.com/software/SuspiciousPackage/

- Apple Configurator 2
- iMazing profile editor
- https://imazing.com/profile-editor

- Privacy Preferences Policy Control (PPPC) Utility
- https://github.com/jamf/PPPC-Utility

Some MDM providers

- Jamf
- https://jamf.com

- Mosyle
- https://mosyle.com/

- Simple MDM
- https://simplemdm.com/

- Microsoft Intune
- https://partner.microsoft.com/solutions/microsoft-intune

Demo

Thank you!

Time for Q&A

Let’s keep in touch