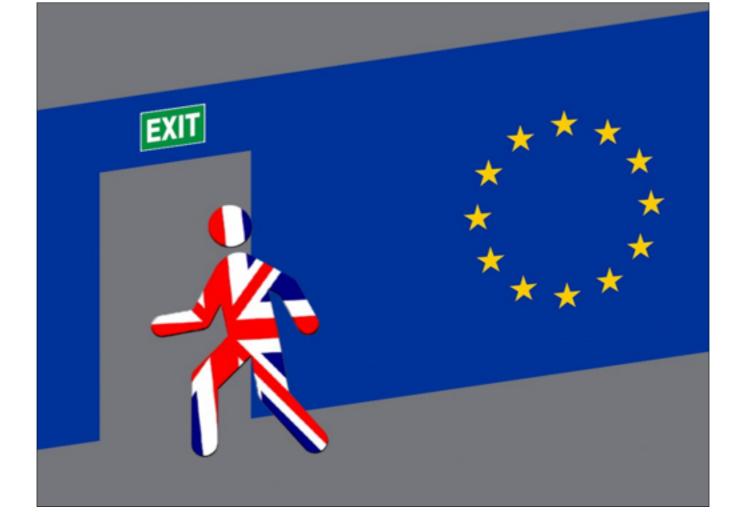# Apple Configuration Profiles - What Works, And What Doesn't

Ben Goodstein
Senior Systems Administrator
Unix Services Team, NSMS
IT Services, University of Oxford
@fuzzylogiq - Twitter, MacAdmins Slack, GitHub

2016

It's been a funny old year...

The UK voted to leave the European Union

This guy is now "The Leader of the Free World"

And this guy suddenly found out he didn't have a job any more.

Sal Saghoian - Product Manager of Automation Technologies at Apple

Q. What does the termination of the position of Product Manager of Automation Technologies mean for the future of user automation in macOS?

A. Ask Apple. Seriously, if you have any questions or concerns about the future of user automation, ask Apple...The macOS user automation technologies include: UNIX CLI (shell, python, ruby, perl), System Services, Apple Events (JavaScript, AppleScript, ...

Source: https://macosxautomation.com/about.html

"What would you do if the entire OS that is macOS - if all of it was protected, like it is on iOS/tvOS/watchOS?

What if you couldn't change ntp.conf? Or ssh_config? Or mess with the default User Template? What if everything that is macOS was locked away?

How would you manage it?"

What you can script now,
you might not always be
able to script.

...and since Configuration Profiles are the official Apple supported way of configuring iOS and macOS devices...

It's time to get serious about Configuration Profiles

SIP and APFS

What is a Configuration Profile?

- XML (.mobileconfig file)

- Property List (Plist)

- Configures settings for iOS or macOS

- Contains one or more "payloads"

- Can be encrypted

- Can be signed

some settings payloads are common to iOS or macOS, others are for one or the other

How can we create them?

- Hand edit XML

- mcxToProfile

- Apple Configurator (iOS)

- Profile Manager (macOS)

- 3rd Party MDM Server (iOS and macOS)

What's MDM?
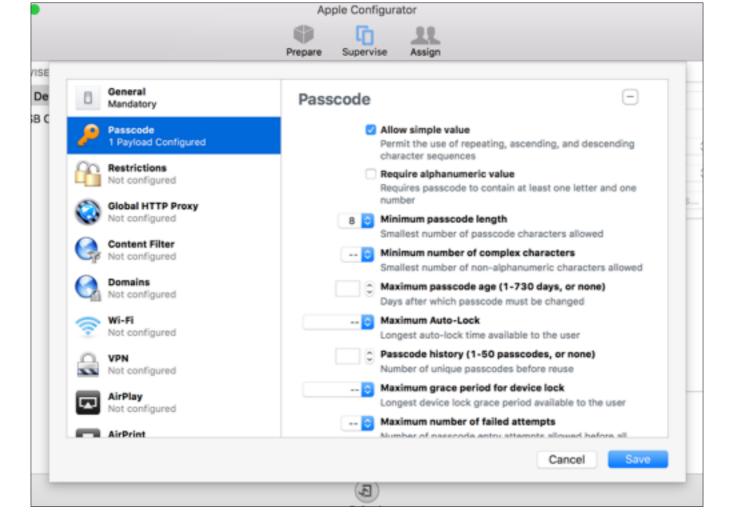
- Mobile Device Management

- Apple MDM:

  - MDM server

  - Config profiles for settings

  - Certificates for signing/encrypting

  - Apple Push Notifications to initiate profile pull/run commands (Erase Device, Lost Mode etc.)
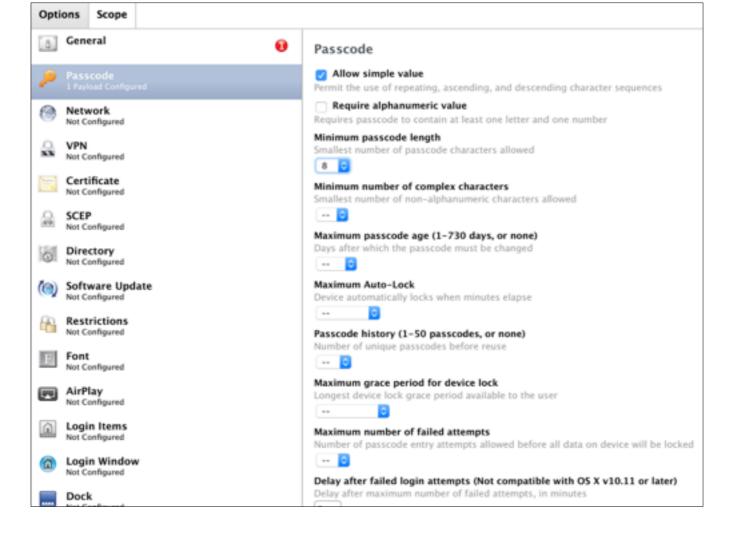
How do we install and inspect them?
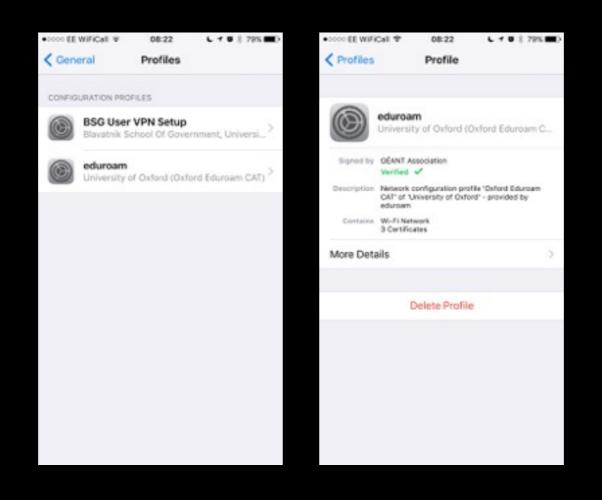
- Can be delivered via email, HTTP etc. (BYOD)

- Can be delivered via an MDM server e.g. Profile Manager/JSS (Enterprise)

- Appear in System Preferences

- "profiles" tool on the command line

  - pkg/munki can install them
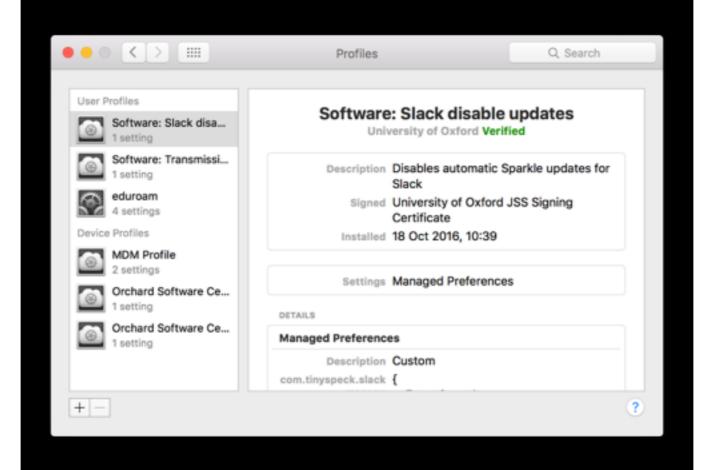
BSG VPN settings in the wiki - BYOD

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
        <key>PayloadVersion</key>
        <integer>1</integer>
        <key>PayloadUUID</key>
        <string>Ignored</string>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadIdentifier</key>
        <string>Ignored</string>
        <key>PayloadContent</key>
        <array>
            <dict>
                <key>PayloadContent</key>
                <dict>
                    <key>URL</key>
                    <string>https://scep.example.com/scep</string>
                    <key>Name</key>
                    <string>EnrollmentCAInstance</string>
                    <key>Subject</key>
                    <array>
                        <array>
                            <array>
                                <string>O</string>
                                <string>Example, Inc.</string>
                            </array>
                        </array>
```

Prepare   Supervise   Assign

VISE

De

3B C

General
Mandatory

Passcode
1 Payload Configured

Restrictions
Not configured

Global HTTP Proxy
Not configured

Content Filter
Not configured

Domains
Not configured

Wi-Fi
Not configured

VPN
Not configured

AirPlay
Not configured

AirPrint

Passcode

☑ **Allow simple value**
Permit the use of repeating, ascending, and descending character sequences

☐ **Require alphanumeric value**
Requires passcode to contain at least one letter and one number

8 ⬍ **Minimum passcode length**
Smallest number of passcode characters allowed

-- ⬍ **Minimum number of complex characters**
Smallest number of non-alphanumeric characters allowed

⬍ **Maximum passcode age (1-730 days, or none)**
Days after which passcode must be changed

-- ⬍ **Maximum Auto-Lock**
Longest auto-lock time available to the user

⬍ **Passcode history (1-50 passcodes, or none)**
Number of unique passcodes before reuse

-- ⬍ **Maximum grace period for device lock**
Longest device lock grace period available to the user

-- ⬍ **Maximum number of failed attempts**
Number of passcode entry attempts allowed before all

Cancel   Save

Options | **Scope**

🔲 **General** ❗

🔑 **Passcode**
1 Payload Configured

🌐 **Network**
Not Configured

VPN
Not Configured

Certificate
Not Configured

SCEP
Not Configured

Directory
Not Configured

Software Update
Not Configured

Restrictions
Not Configured

Font
Not Configured

AirPlay
Not Configured

Login Items
Not Configured

Login Window
Not Configured

Dock
Not Configured

Passcode

☑ **Allow simple value**
Permit the use of repeating, ascending, and descending character sequences

☐ **Require alphanumeric value**
Requires passcode to contain at least one letter and one number

Minimum passcode length
Smallest number of passcode characters allowed
`8 ⬍`

Minimum number of complex characters
Smallest number of non-alphanumeric characters allowed
`-- ⬍`

Maximum passcode age (1–730 days, or none)
Days after which the passcode must be changed
`-- ⬍`

Maximum Auto-Lock
Device automatically locks when minutes elapse
`-- ⬍`

Passcode history (1–50 passcodes, or none)
Number of unique passcodes before reuse
`-- ⬍`

Maximum grace period for device lock
Longest device lock grace period available to the user
`-- ⬍`

Maximum number of failed attempts
Number of passcode entry attempts allowed before all data on device will be locked
`-- ⬍`

Delay after failed login attempts (Not compatible with OS X v10.11 or later)
Delay after maximum number of failed attempts, in minutes

Profiles

User Profiles

Software: Slack disa...
1 setting

Software: Transmissi...
1 setting

eduroam
4 settings

Device Profiles

MDM Profile
2 settings

Orchard Software Ce...
1 setting

Orchard Software Ce...
1 setting

Software: Slack disable updates
University of Oxford **Verified**

Description   Disables automatic Sparkle updates for Slack

Signed   University of Oxford JSS Signing Certificate

Installed   18 Oct 2016, 10:39

Settings   Managed Preferences

DETAILS

Managed Preferences

Description   Custom

com.tinyspeck.slack   {

Profiles Preference Pane Demo

"profiles" command demo

What works?

- Manually installing profiles

- Device level MDM - mostly

What doesn't?

- User level MDM can be flaky

- Compositing can be hit and miss

- Profile removal isn't always consistent

- Compared to mcx, frequency settings are not as fine-tuned

References

- Apple configuration profile reference
  https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html

- Tim Sutton's OS X Configuration Profile Review
  https://www.afp548.com/2013/05/28/os-x-configuration-profiles-review-and-gotchas-compositing-not-included/

- mcxToProfile
  https://github.com/timsutton/mcxToProfile

- Signing .mobileconfig Profiles With Keychain Certificates
  https://osxdominion.wordpress.com/2015/04/21/signing-mobileconfig-profiles-with-keychain-certificates/

- Managing Configuration Profiles with Munki
  https://github.com/munki/munki/wiki/Managing-Configuration-Profiles

- OSXBYTES: Profile behaviour changes in Yosemite
  https://osxbytes.wordpress.com/2015/02/25/profile-behavior-changes-in-yosemite/

- How APNS works with MDMs that manage OSX and iOS
  https://www.justinrummel.com/how-apns-works-with-mdms-that-manage-osx-and-ios/