

Ryan Slater

Mobile Accounts in 2018? Go Local.

A brief introduction to



White Collar Factory is the London space for Capital One operating over 2 floors

HQ located in Central Nottingham

Tech Focussed company

Global Mac estate just short of 14,000 Macs

UK Mac estate grown to ~450 from less than 50 in 3 years and rapidly expanding

Geographically spread team of Mac Engineers + System Architects both sides of the Atlantic and both sides of the US; a few of which have spoken at events and can be found online

What's my background?

Ex-professional services Systems Engineer for a leading Apple Enterprise Authorised Reseller and service provider. A number of years spent travelling the UK for consultancy projects and system integration.

Now working as an Infrastructure Engineer at Capital One Europe, with a focus on great user experience, mainly on the Mac platform.

Mobile Accounts In Context

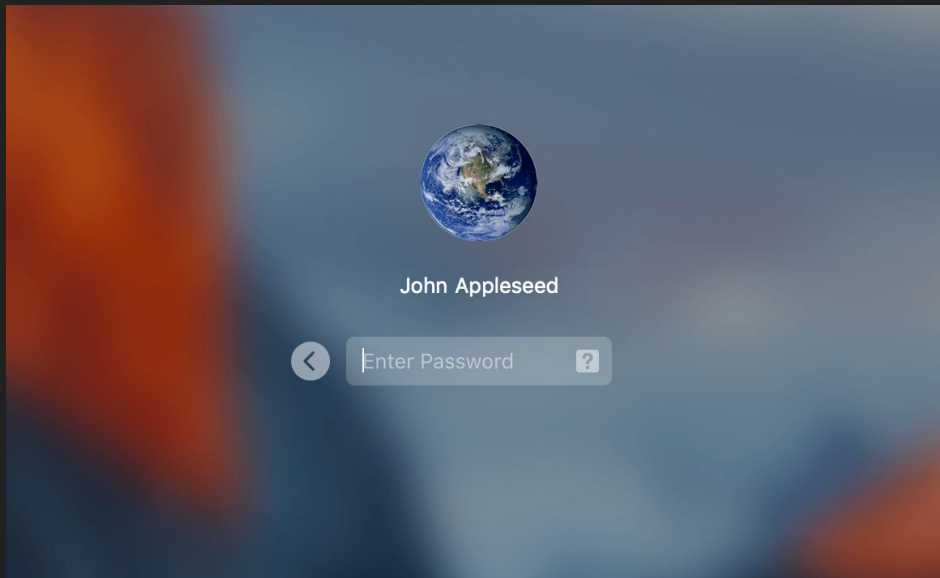
This talk is only pertinent to personal experience with Active Directory derived user accounts.

Your own experiences may differ.

Setting the Scene

Why Local accounts?


- Binding is old news in 1:1 environments (Edu and Shared clients are an exception!)
- Mobile Accounts encounter unexpected results
- Bind + Mobile account requirements make off site DEP build workflows *hard* to implement
- Core MacOS features are being broken (remember Mobile Homes?)
- As always, the future is uncertain



Setting the Scene - The Main Issue

“I ran an update and can’t login”

Growing pains since the changes to FileVault2 incorporating Secure Token, mean both an immediate issue for a handful of earlier adopters but a major problem moving forward as the rest of the estate follow.

What happens?	Resolution? Not simple.
<ul style="list-style-type: none">- OS Updates get rolled out- Reboot to FileVault Unlock screen- Users attempt to unlock storage by signing in, but the password box shakes. 	<ul style="list-style-type: none">- Trip to the IT bar with a critical issue for on-site users- Remote workers have no bar - immediately makes troubleshooting more difficult- Enabling users feature under FileVault2 pane in System Preferences > Security, Unresponsive- No quick workaround beyond using escrowed recovery keys, setting up local accounts manually etc.

netResult =
“Unhappy Users”

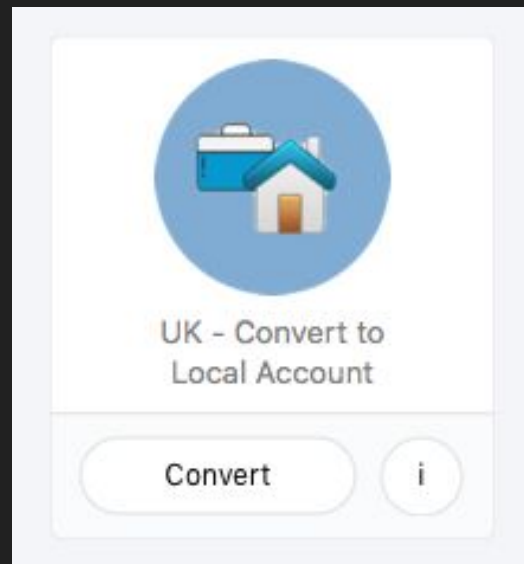
Unable to login means unable to work.

Impact? **Major.**

Alleviating the Problem

So what do we do?

- Service needs to be both informative but simple to understand - we also need to still enforce password policy.
- Rich Trouton wrote a [script](#) (modelled off Pat Gallagher + Lisa Davies' scripts) to remove SMB / AD attributes from user accounts. Credit also goes to Kevin Hendricks for Cocoa Dialog Progress Bar.
- This script provided the functionality behind an easy, working conversion button via Jamf Pro Self Service
- Jeffrey Compton, Capital One US added some prompts via AppleScript to inform the users what's happening and allow some level of customisation
- Few final bugs to fix, then we're good!



Alleviating the Problem

But what about SSO?

- We still need Kerberos tickets for Auth + SSO!
- Solutions are available to ensure Local User accounts are Enterprise workable - as most members of the community are already aware.
- Conveniently, Enterprise Connect is widely used across the global Mac estate, meaning:-
 - No extra distribution requirements
 - User base is already familiar with EC experience
 - User experience doesn't actually change



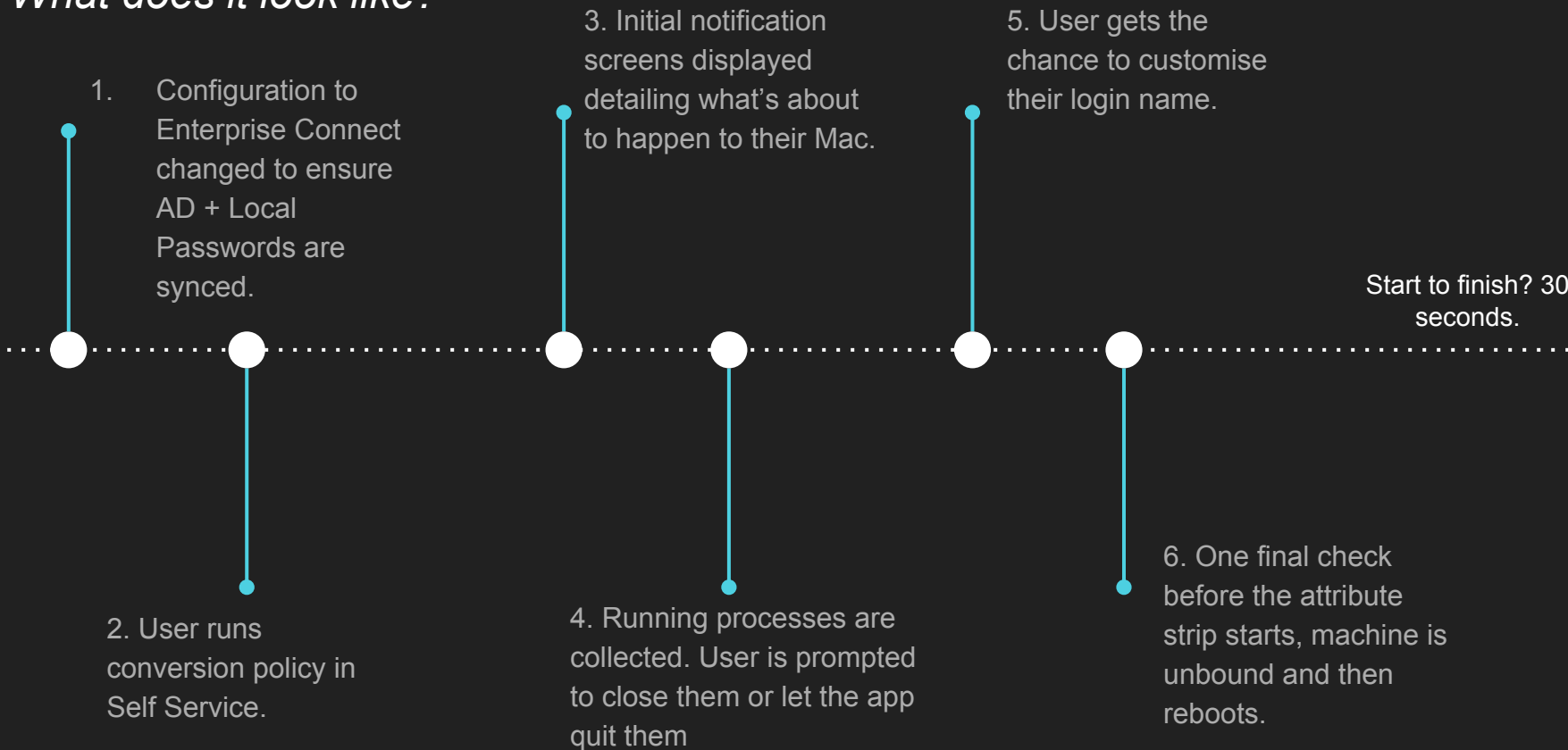
Enterprise Connect by Apple



NoMAD by Orchard & Grove (Or
now Jamf Connect by Jamf!)

Alleviating the Problem

What does it look like?



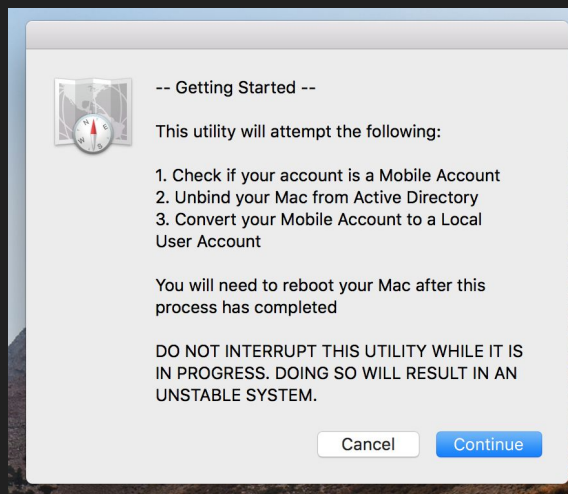
Alleviating the Problem

What does it look like?

Computer level profile for Enterprise Connect

```
Custom Settings
Description Custom
com.apple.Enterprise {
  -Connect Forced = (
    {
      "mcx_preference_settings" =
      {
        adRealm =
        "cof.ds.capitalone.com";
        passwordChangeScriptPath =
        "/Library/Application Support/COF/bin/
        pwChangeCleanupEC.sh";
        syncLocalPassword = 1;
      };
    };
  };
}
```

Welcome Screen



Apps Open Warning



Alleviating the Problem

What does it look like?

Customise me

-- Account Customization --

Would you like to customize your login name or use the ones we recommend? You'll be able to sign in with your Login Name or your EID.

Full User Name - Ryan Slater
Account Name - ryan

If customised {

-- Name Setup --

Please enter your full name using letters and spaces e.g. Bob Alice

You will be re-prompted until you enter an acceptable name.

If you wish to cancel, type the word "cancel" into field below and click Continue.

};

Final Confirmation

-- Final Check --

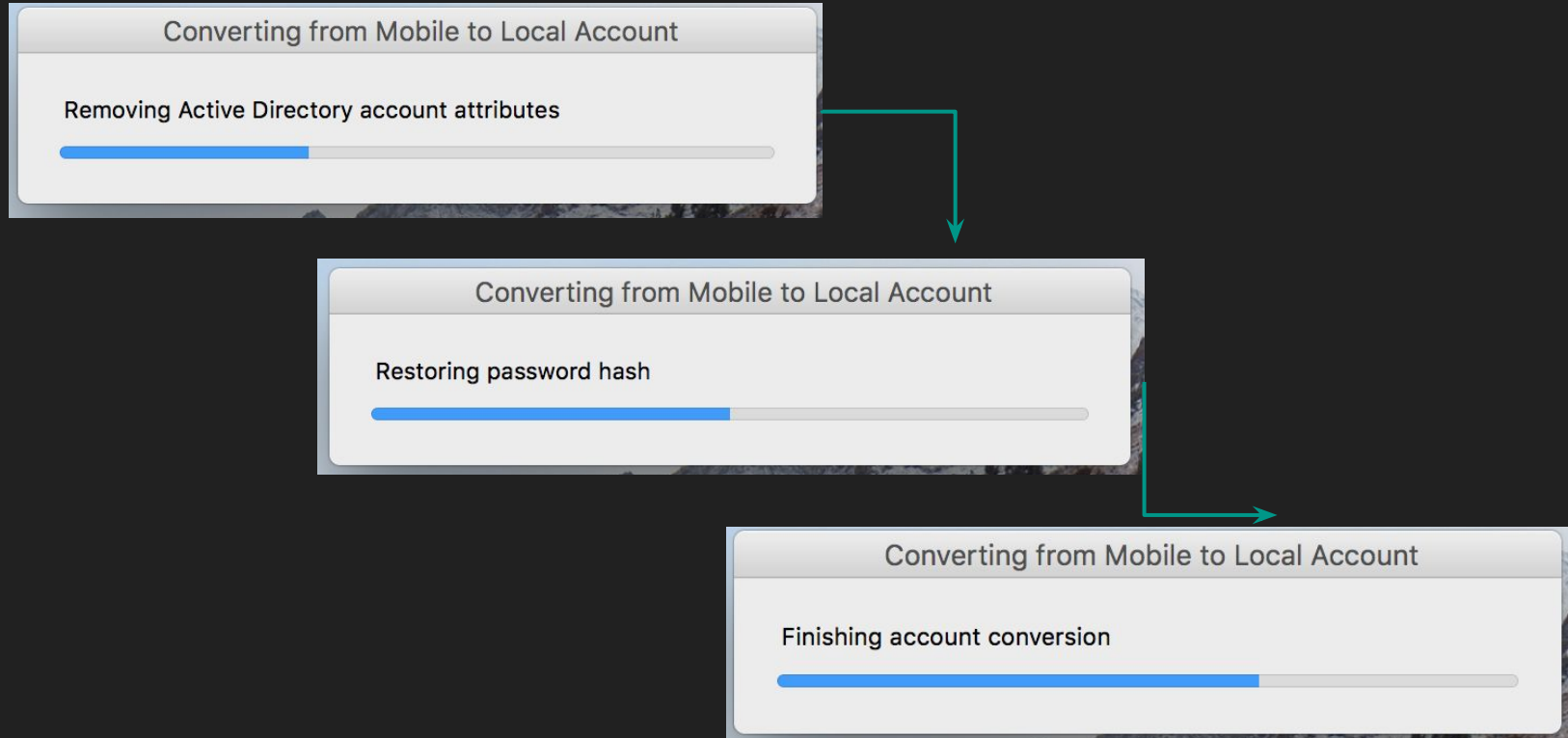
Please check the following details and make sure you would like to proceed.

This is your final chance to stop the process. Remember, your account Short Name will be the one you sign into your Mac with!

New User Full Name = Ryan Slater
New Account Short Name = ryanslater
New Home Directory = /Users/ryanslater

Alleviating the Problem

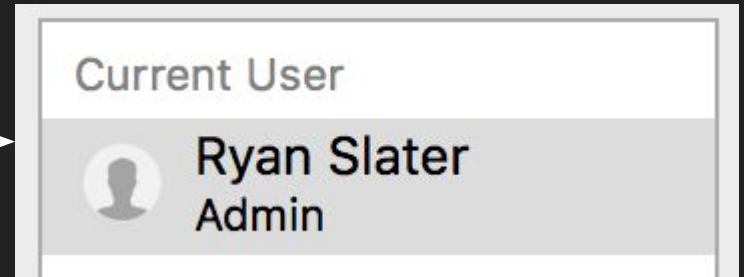
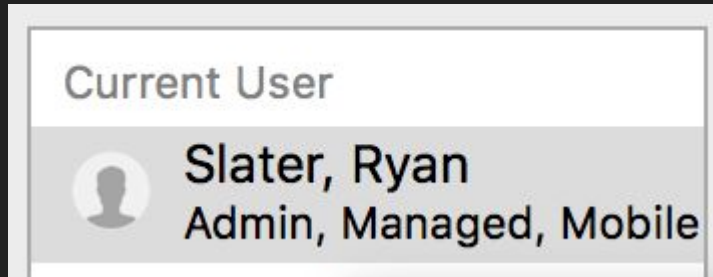
What does it look like?



Alleviating the Problem

What does it look like?

Post Conversion > System Preferences > Users &
Groups



So we're done, right?

“Why's it asking me to reset my password?”

- The script works! We've gone local. I can login and access all of my resources
- Just one problem; if the user has existed on the machine for more than 1 password reset cycle, it forces them to change their password on login. Why?
- AD mobile accounts store their user configuration for offline availability (like what you see when you read in DSCL) in a hidden file under their user home space (/Users/name/.account). This file is *.account*
- Inside *.account*, the *passwordLastSetTime* key stores a UNIX Time for the date the account was first logged into - which never gets updated when the users reset passwords via Enterprise Connect

```
<key>passwordLastSetTime</key>  
<real>1534345278.7464139</real>
```

Fun fact: Unix time is the number of seconds since 01/01/1970

- Could not find a way to edit this key to just add the current time *gracefully* as it's XML nested inside an attribute (accountPolicyData). The hammer-style approach however, works perfectly.

```
currentUser=$(stat -f %Su /dev/console)  
rm -f /Users/$currentUser/.account
```

What do we gain?

Apple centric user experience moving forward, and hopefully less potential issues in the future

A fully working supportable FileVault2 system again

Password complexity and change cycles still enforced and clients remain hardened

Opened the ability business wide to start adopting an Apple Device Enrollment implementation method, remember - binding makes it *harder*

Reaffirmed knowledge that testing is critical. Things work perfectly when you test yourself in a controlled environment. You can't test user experience if you designed it

What could we do better?

An App based version to further customise the UI / look + feel of the solution and therefore a better, branded and trustable user experience

Implement the Apple Device Enrollment methodology and 'Go Local' from day 1

Any Questions?

Again - welcome to Capital One.
Enjoy the rest of your evening!

Access to public version of script:
<https://github.com/igeejpsc/mobile2local>

Ryan Slater
ryan@ryanslater.co.uk
<https://ryanslater.co.uk>

