Profiles

MACTECH

Max Buxton

Max Buxton has been a full time Macintosh consultant for over 15 years. Before working as a consultant, Max was as a software tester and application engineer for computer software development companies.

He's been a certified member of the Apple Consultants Network since 2003. He's been a peer, colleague and friend of Andy for much of that time, and 3 years ago was persuaded to join the Call Andy! team.

When he's not configuring customer systems, Max enjoys exploring the back roads of New England on his motorcycle.

MACTECH

Agenda

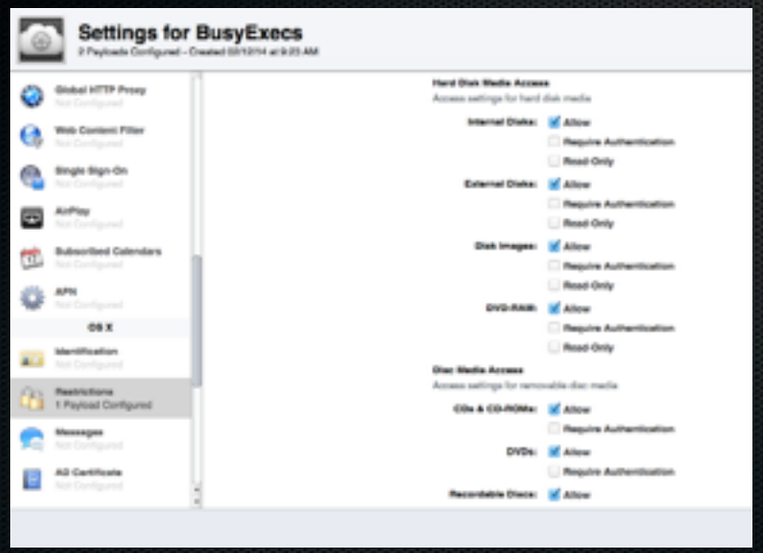
- Profiles explained
- Delivering Profiles
- MDMs
  - Apple Configurator
  - Profile Manager
  - 3rd Party
- New Application Management in iOS 7 / Mac OS X 10.9
- Q & A

MACTECH

Reasons for using Apple Configurator & Profile Manager
- AC is the only choice for tethered solutions
- PM is an inexpensive way to learn the concepts and test
- In many cases PM could be the best solution
- Meraki is an alternative since its free but has other features and is more complicated

Completely new model for App Distribution – applicable to all MDM solutions

What are Profiles?




```
<key>PayloadDisplayName</key>
<string>Restrictions</string>
<key>logout-eject</key>
<dict/>
<key>mount-controls</key>
<dict>
  <key>blankcd</key>
  <array/>
  <key>blankdvd</key>
  <array/>
  <key>cd</key>
  <array/>
  <key>dvd</key>
  <array/>
  <key>dvdram</key>
  <array/>
  <key>disk-image</key>
  <array/>
  <key>harddisk-external</key>
  <array/>
  <key>harddisk-internal</key>
  <array/>
 </dict>
</dict>
<dict>
  <key>PayloadType</key>
  <string>com.apple.DiscRecording</string>
  <key>PayloadVersion</key>
  <integer>1</integer>
  <key>PayloadIdentifier</key>
  <string>com.apple.mdm.ml.kkheconsulting.com.8aca65e0-7032-013
  <key>PayloadEnabled</key>
  <true/>
  <key>PayloadUUID</key>
  <string>60c20226-fa71-aafc-8332-1302aa02d6bc</string>
  <key>PayloadDisplayName</key>
  <string>Media Access:  Disc Recording</string>
  <key>BurnSupport</key>
  <string>on</string>
</dict>
<dict>
```

MACTECH

Just a text file

In XML format

XML files that store key-value pairs in a property list (.plist) format and have a .mobileconfig suffix

Both OS X and iOS use the same file format for configuration profiles

Each configuration profile contains one or more payloads

What are Profiles?

- .MobileConfig files
- Replacement for MCX?
- Profiles contain settings and preference bundles for devices including:

GENERAL
	the list of configurable settings grows with every iOS, OS X and Server app release
	the choices require a great deal of study to grasp all of the options
	when does it make sense to manage centrally with profiles and when manually
	profile management is for both OS X and iOS systems
RESTRICTIONS
	many apply only to supervised devices
	be careful about locking down users unnecessarily, especially BYOD users
WIFI
	can be used as inducement to enroll devices
WEB CLIPS
CREDENTIALS and KEYS

Profile Settings

- Restrictions on device features
- Wi-Fi settings
- VPN settings
- Email server settings
- Exchange settings
- LDAP directory service settings
- CalDAV calendar service settings
- Wallpaper
- Web clips
- Credentials and keys

MACTECH

GENERAL
	the list of configurable settings grows with every iOS, OS X and Server app release
	the options require a great deal of study to grasp all of the options
	when does it make sense to manage centrally with profiles and when manually
	profile management is for both OS X and iOS systems
RESTRICTIONS
	many apply only to supervised devices
	be careful about locking down users unnecessarily, especially BYOD users
WIFI
	can be used as inducement to enroll devices
WEB CLIPS
CREDENTIALS and KEYS

Profiles: Why use them?

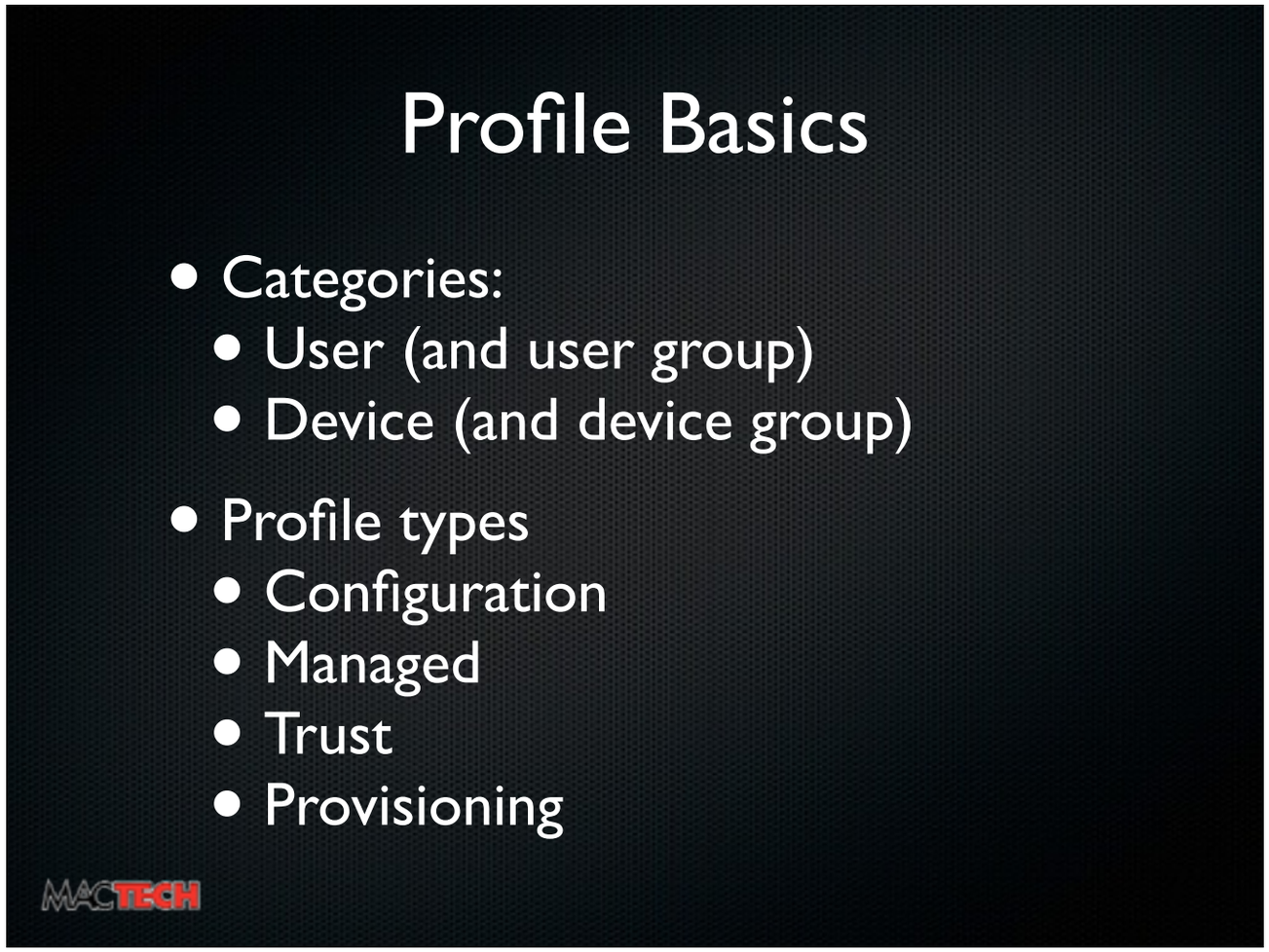
- Small staff
- Widely distributed systems
- Granting access
- Restricting features

MACTECH

Reasons for using Profiles:

Biz – help users w/config they would have to figure out (it's a wiki in an xml file)
Ed – acceptable use

Small staff can manage a large number of devices
Centrally located staff can manage widely distributed systems
Granting access to organization's network and services
Restricting features for security or to limit access to specific types of data



User profiles, which contain settings for individual users or user groups, such as account names, passwords, and parental controls.

Device profiles, which contain settings for individual devices or device groups, such as directory bindings, energy saver, and restrictions.

Managed profiles are configuration profiles installed on devices by an MDM server. Like other configuration profiles, they can be locked to prevent end users from removing them. When you deploy managed profiles, the primary MDM profile manages anything delivered by MDM after enrollment and contains several “rights” to the system, including:

> Erase all data on the computer; Add or remove configuration profiles; Add or remove provisioning profiles; Lock screen, and; Query information about different settings including security, computer, network, installed applications, and installed profiles

Trust profiles are profiles generated by an MDM server that contain critical information, certificates, and security keys that, when installed on managed devices, help ensure that communication between the MDM server and the managed device is secure and authentic.

Provisioning profiles are needed when testing apps still under development

SIGNING

> trust, convenience
> make sure profiles are valid, and coming from known host, and encrypted

Signed Profiles:

> The payload data on a configuration profile can contain sensitive information
>
> A profile that’s signed can be replaced only by another profile with the same identifier that’s also signed by the same source

Terms and things you need to know:

- .mobileconfig
  - xml files that store profile info
  - based on OS X preference file format
  - profiles are made up of payloads
- Trust profile
  - needed for self-signed servers
- Enrollment profile
  - provided by MDM for enrollment
  - binds the device to the MDM

MACTECH

All Mac and IOS profiles are stored in .mobileconfig files (can be obscured, if signed).

Self-signed servers need a profile that loads the self-signed certificate (before anything else)

Apple Configurator - still a required tool in most setups

APNS - responsible for notifying device that profiles are available…
.MOBILECONFIG
	XML file
TRUST PROFILE
	not needed with a server using a 3rd party trusted cert (recommend for larger deployments)
ENROLLMENT PROFILE
	useful if you're not enrolling through a portal like PM's ../mydevices/
APPLE CONFIGURATOR
	current version 1.5
	successor to IPCU - which is still used for OS X Lion, ML and PCs
	multipurpose tool for configuring iOS devices at a single location*
		*can be first step for devices that will be distributed widely as well

Profile Delivery

- Tethering
  - Apple Configurator or iPCU
- Manually
    - Email, ARD, imaging, CLI
- User via self-service portal
- MDM

MACTECH

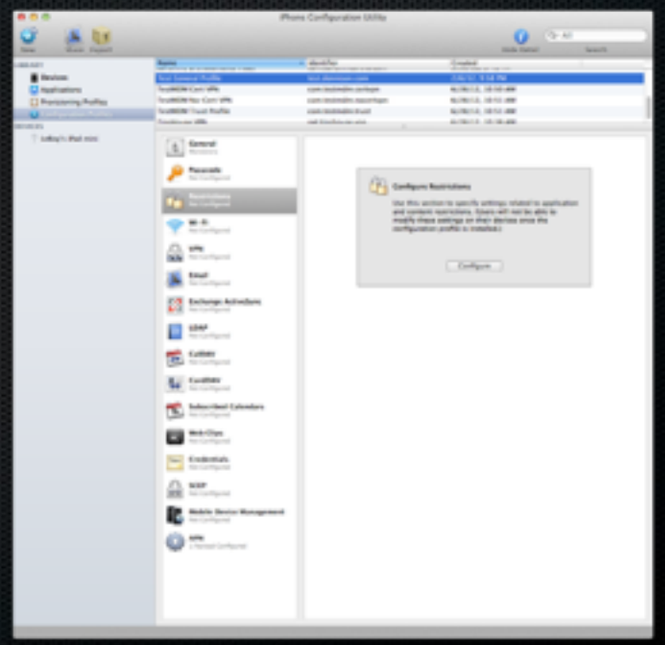
or email/web, USB stick/etc (it's just a file…)

Profile Delivery

Three Apple Tools

iPhone Configuration Utility (iPCU)

- Utility for creating and installing profiles and apps
- Available for Mac OS X and Windows
- Mac Download: http://support.apple.com/kb/DL1465
  - Note: for use with Lion & Mountain Lion; for Mavericks, use Apple Configurator



MACTECH

Last version (3.5) released 3/7/2012

A Provisioning Profile is necessary in order to install development applications on development iPhones and iPads

Why Apple Configurator

- "Supervise" a device over the air
  - Certain attributes can only be managed if device is supervised (Airdrop)
- Lock an over the air MDM enrollment profile so user can't remove it
- Distribute and then revoke apps using just one Apple ID.
- Great way to generate Profiles for use in other tools…

MACTECH

Free from Apple in App Store
Supervision replaces the iOS Activation that binds a device to Apple
Device is now bound to your Apple Configurator (with a certificate even)
	Only certain attributes can only be configured if a device is supervised
App

Apple Configurator

- Three modes:
  - Prepare
  - Supervise
  - Assign

MACTECH

Devices Must Come Back to Apple Configurator

v1.5 released 10 Mar 2014
- Enroll unsupervised & supervised devices in MDM using enrollment URLs
- Integration with new Bretford PowerSync+ carts and stations to report progress & status, and display physical port number
Support for a new iOS setting to require a passcode for initial AirPlay connection

PREPARE
good for initial rollout/provisioning
very good means of making a template and saving it
preferred first step in an iOS deployment
Configure
MDM enrollment
Enable Supervision

SUPERVISE
good for auto-refresh and locking into single app mode (AKA kiosk mode)
good for iPads owned by company (e.g. museum, store, warehouse, etc.)
configured iPad handed out for use and then reset to template upon return

ASSIGN
good for controlling and maintaining user data
check-out to specific user who makes changes, changes saved back to AC on check-in
data transfered to whichever device is checked out by that user
Control user data
Multi-user experience
Personalized experience
Accountability
Supervision features
DANGER OF ERASURE
restoring a template
plugging a supervised device back in
ASSIGNMENT LINKED TO DIRECTORY SERVICE
mac with AC must be bound to directory server

Apple Profile Manager

(http://help.apple.com/profilemanager/mac/3.0/#)

MACTECH

Apple's Profile Manager:

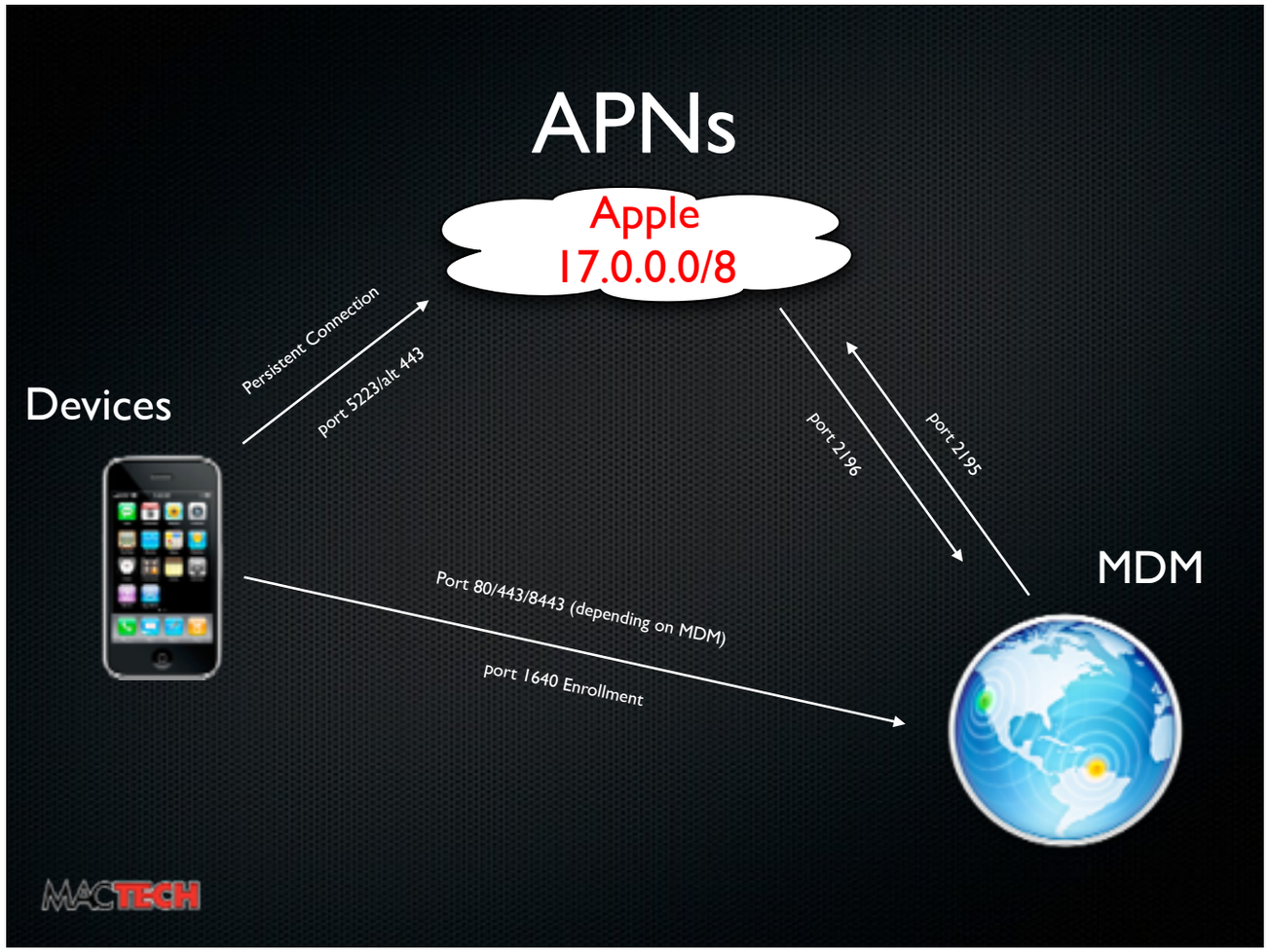
- Components of Profile Manager
  - Administration portal
  - Self-service user portal
  - MDM service
  - App and book distribution
- User and Device groups
- Distribute configuration profiles
  - Manual distribution
  - User self-service
  - Remote device management

MACTECH

Manual approaches are okay in certain cases
	small installations
	one off situations – vpn settings to a vendor who will not enroll
Automatic solutions will be easiest on everyone – once enrollment is completed

Apple Push Notification Service (APNs)

MACTECH


APNs
Apple
17.0.0.0/8
Devices
Persistent Connection
port 5223/alt 443
port 2196
port 2195
MDM
Port 80/443/8443 (depending on MDM)
port 1640 Enrollment
MACTECH

Firewalls

- For APNs traffic to get past your firewall, you'll need to open these ports:
  - OutBound
    - TCP port 5223 (used by devices to communicate to the APNs Servers)
    - TCP port 2195 (used to send notifications to the APNs)
    - TCP port 443 (used as a fallback on Wi-Fi only, when devices are unable to communicate to APNs on port 5223)
  - InBound
    - TCP port 1640 for enrollment (Apple PM)
    - TCP port 2196 (used by the APNs feedback service)

MACTECH

OUTBOUND

some corporate firewalls lock down outbound ports as well
this will prevent APNs from working

APNs: Load Balancing

- Apple Push Notification Service (APNs) servers use load balancing.
- Your devices will not always connect to the same public IP address for notification.
- The entire 17.0.0.0/8 address block is assigned to Apple, so it's best to allow this range in your firewall settings.

MACTECH

Relevant where both ports and destinations are restricted
Can resolve these settings in the testing phase

Apple's Profile Manager:

- Distributing Apps and Books
  - VPP app distribution for education and enterprise
- Enrolling devices and computers
- Importing device and computer lists
- Associating devices with users
- Deploying a trust profile

MACTECH

Quick overview

Part of OS X Server ≥ 10.7
	Fixed IP
	Preferably a third party SSL Cert
	Dedicated machine

Flip between two slides

point to enrollment + button

payload layering

Apple's Profile Manager (more):

- Creating an enrollment profile (and trust if self-signed)
- Creating and installing configuration profiles
  - Apply payloads effectively
  - Payload interactions
  - Payload variables
- User and group management
- Managing in-house enterprise apps for users and user groups

MACTECH

Managed Distribution of Apps and Books

- Although coupled with MDM, independent service
- Linked to Apple's Volume Purchase Program (VPP) for Ed and Biz
- Old model - iTunes Store codes. You buy/user owns
- Managed Distribution - You buy, you give via App Store, you revoke, they buy if they want
- Big key - everyone has an Apple ID
- Works for both Mac and iOS Apps

MACTECH

Compare and Contrast leading MDM solutions

- Countless players
- Compare and contrast
- Find the features you need
- Great resource at: enterpriseios.com

MACTECH

Tek Serve

Wiki: Please contribute!

http://www.enterpriseios.com/wiki/Comparison_MDM_Providers

Main Players

- Meraki
- Absolute
- Apple Profile Manager
- BoxTone
- Centrify
- Filewave
- JAMF Casper Suite
- MaaS360 by Fiberlink
- MobileIron
- SOTI

and on and on...

MACTECH

Main Uses and Differences

- What features should you be looking for?
- What size solution do you need?
- Who will maintain it?
- Where do they excel?
- How do you choose?

MACTECH

New Stuff

Volume Purchase Program

- VPP + MDM: allows you to deploy apps
- Redemption Codes for permanent assignment
- Managed Licenses for flexible assignment
  - Can assign & revoke apps
  - Can assign books (but not revoke)
  - One time conversion from redemption codes to managed licenses allowed

DEP

- Device Enrollment Program (DEP)
- Zero-touch MDM enrollment
- Wireless supervision
- Streamlined setup assistant
- Must be institution-owned devices

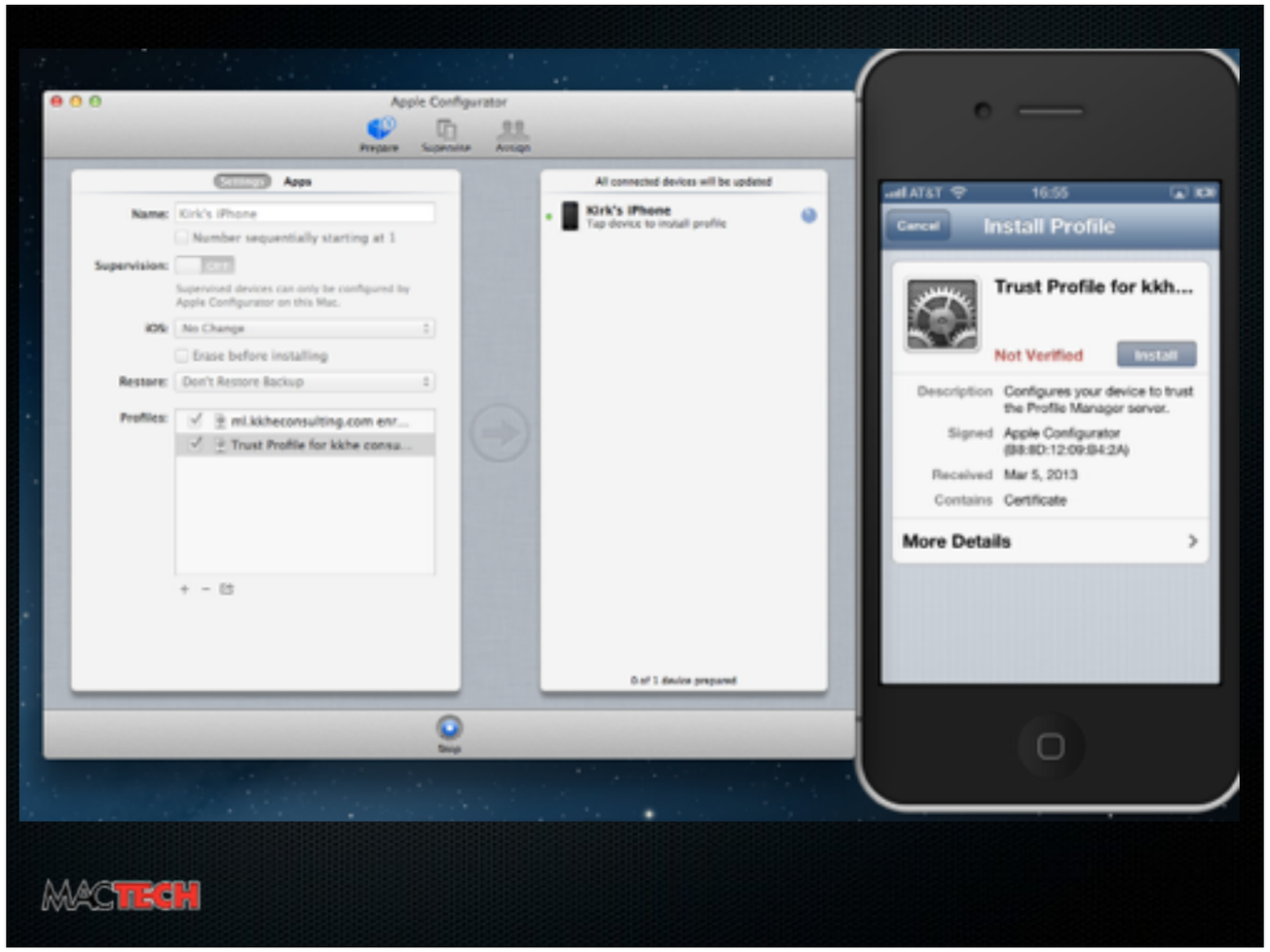
MACTECH

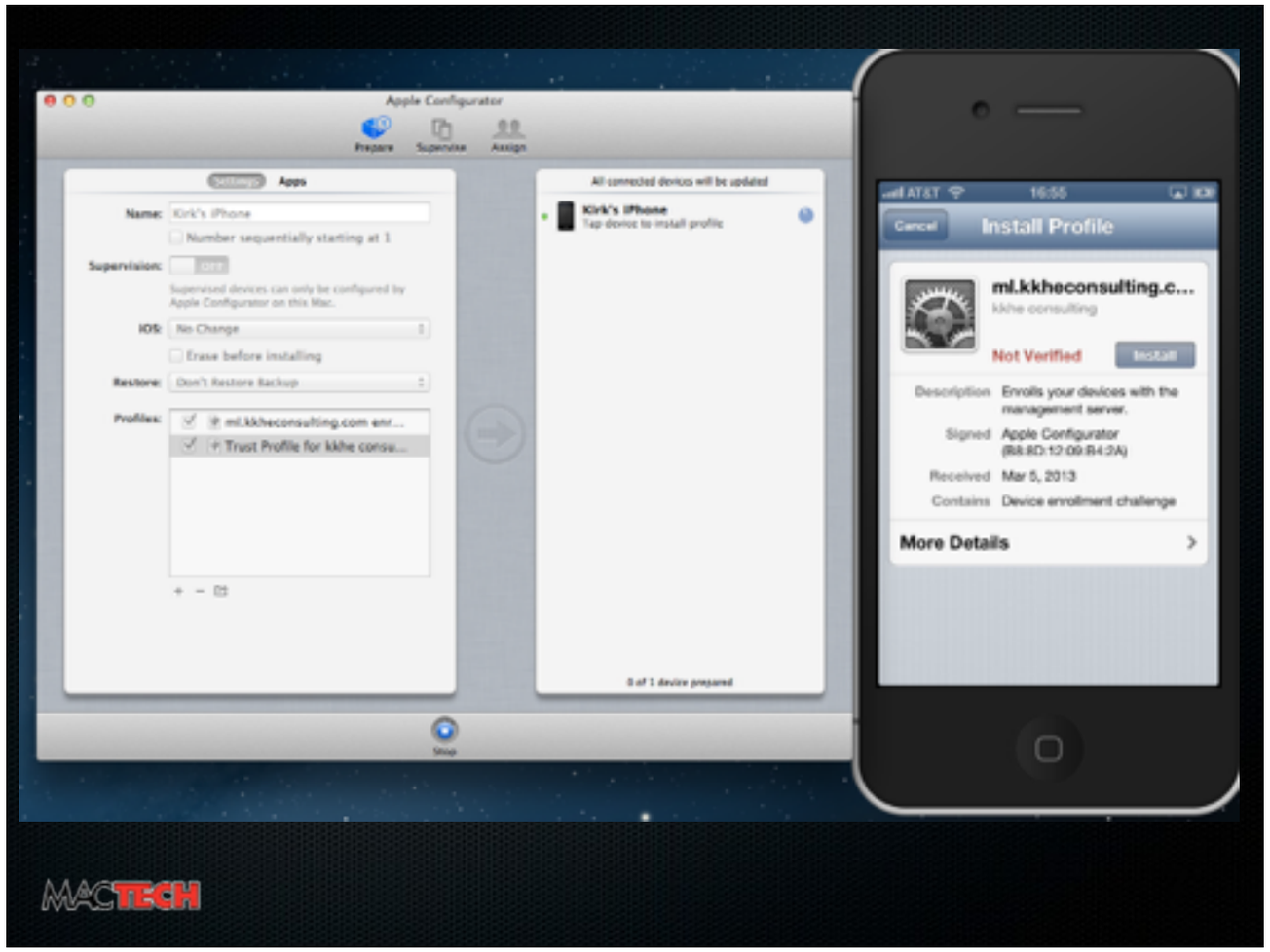

Apple Configurator
Prepare
Supervise
Assign
Prepare Devices
Prep your iOS devices for mass deployment.
Configure your organization's devices. Quickly update them to the latest iOS version, install profiles, install free and volume purchased apps, or restore a device backup.
Learn more
Supervise Devices
Enforce a standard configuration on your iOS devices.
Maintain control over groups of devices that share common apps, settings, and profiles. Automatically restore devices to the specified configuration when reconnected.
Learn more
Assign Devices
Assign iOS devices to users in your organization.
Create and manage users and groups. Assign supervised devices to individual users, back up and restore users' content and settings, and distribute and retrieve users' documents. Learn more
Welcome to Apple Configurator
iOS device configuration, supervision and assignment made easy.
Start Preparing Devices

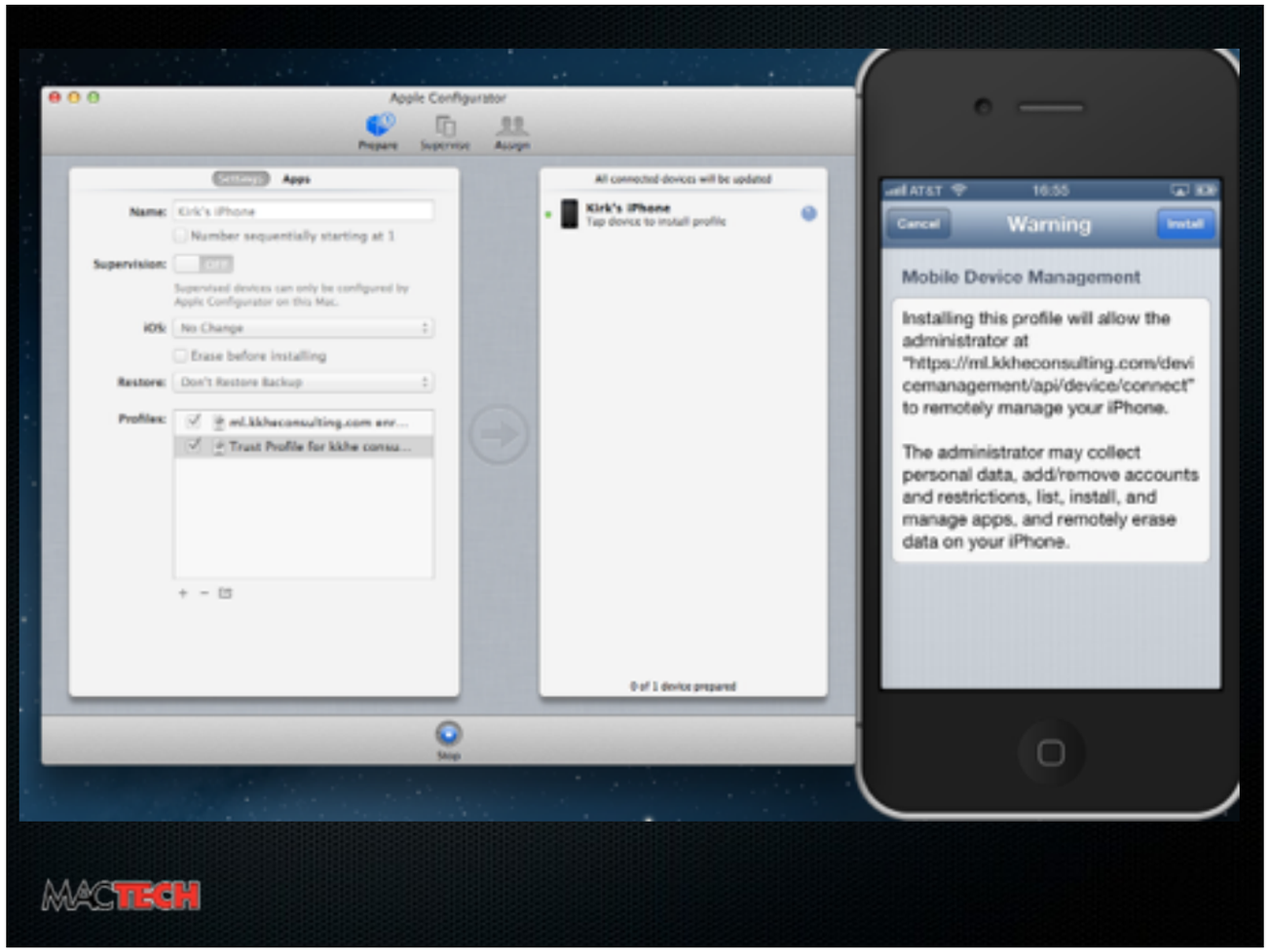

Apple Configurator
Prepare
Supervise
Assign
Settings
Apps
Name:
No Change
Number sequentially starting at 1
Supervision:
OFF
Supervised devices can only be configured by Apple Configurator on this Mac.
iOS:
No Change
Erase before installing
Restore:
Don't Restore Backup
Profiles:
No Profiles
Click + to add a profile
Prepare
AT&T
10:53
Photos
Dropbox
1Password
yelp
Tryphone
Mail
Phone
Music
Safari
MACTECH

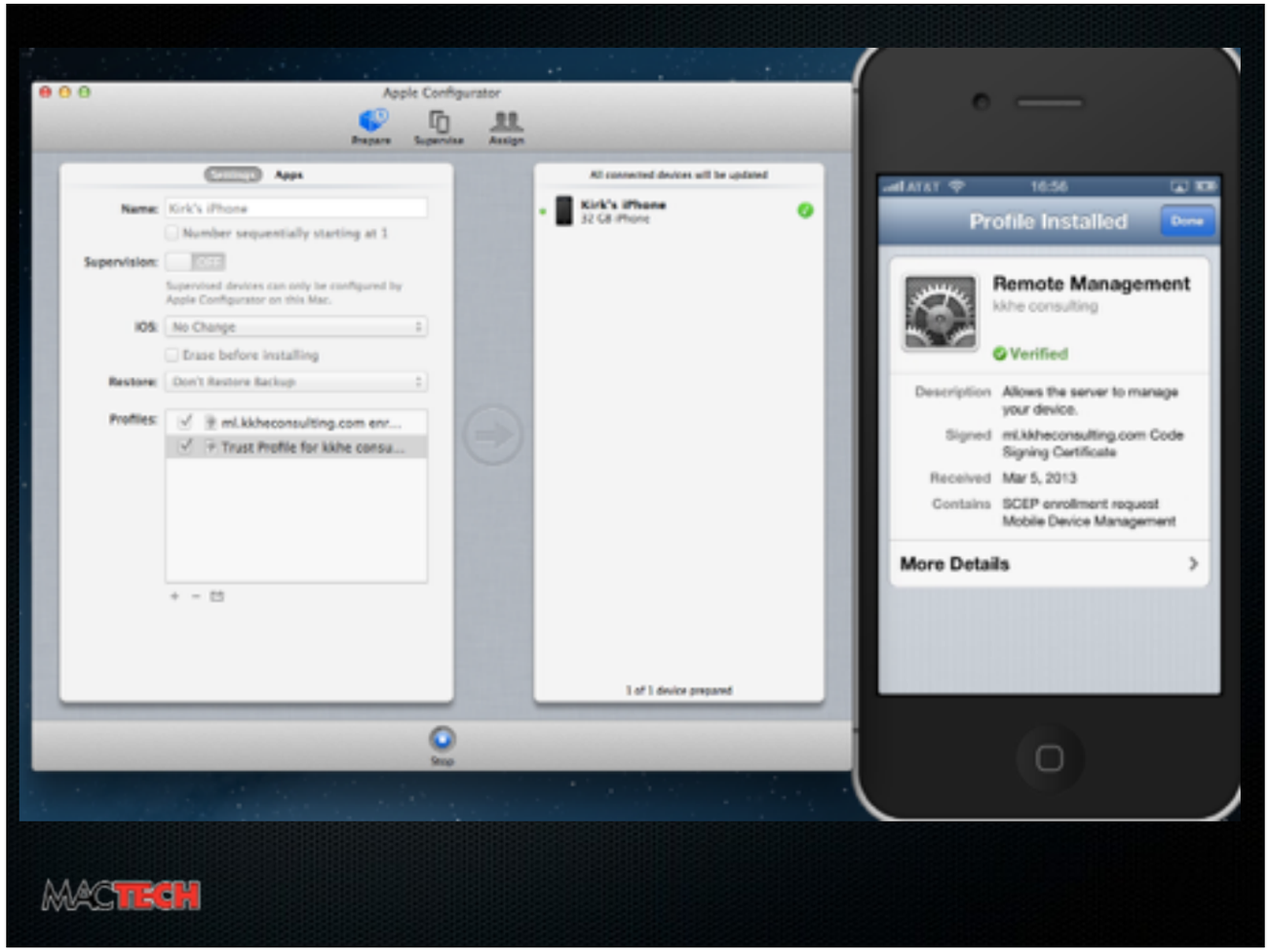

Apple Configurator
Prepare
Supervise
Assign
Apps
Name:
Kirk's iPhone
Number sequentially starting at 1
Supervision:
Off
Supervised devices can only be configured by Apple Configurator on this Mac.
iOS:
No Change
Erase before installing
Restore:
Don't Restore Backup
Profiles:
Prepare
AT&T
10:54
Photos
Dropbox
yelp
Truphone
Mail
Phone
Music
Safari
MACTECH

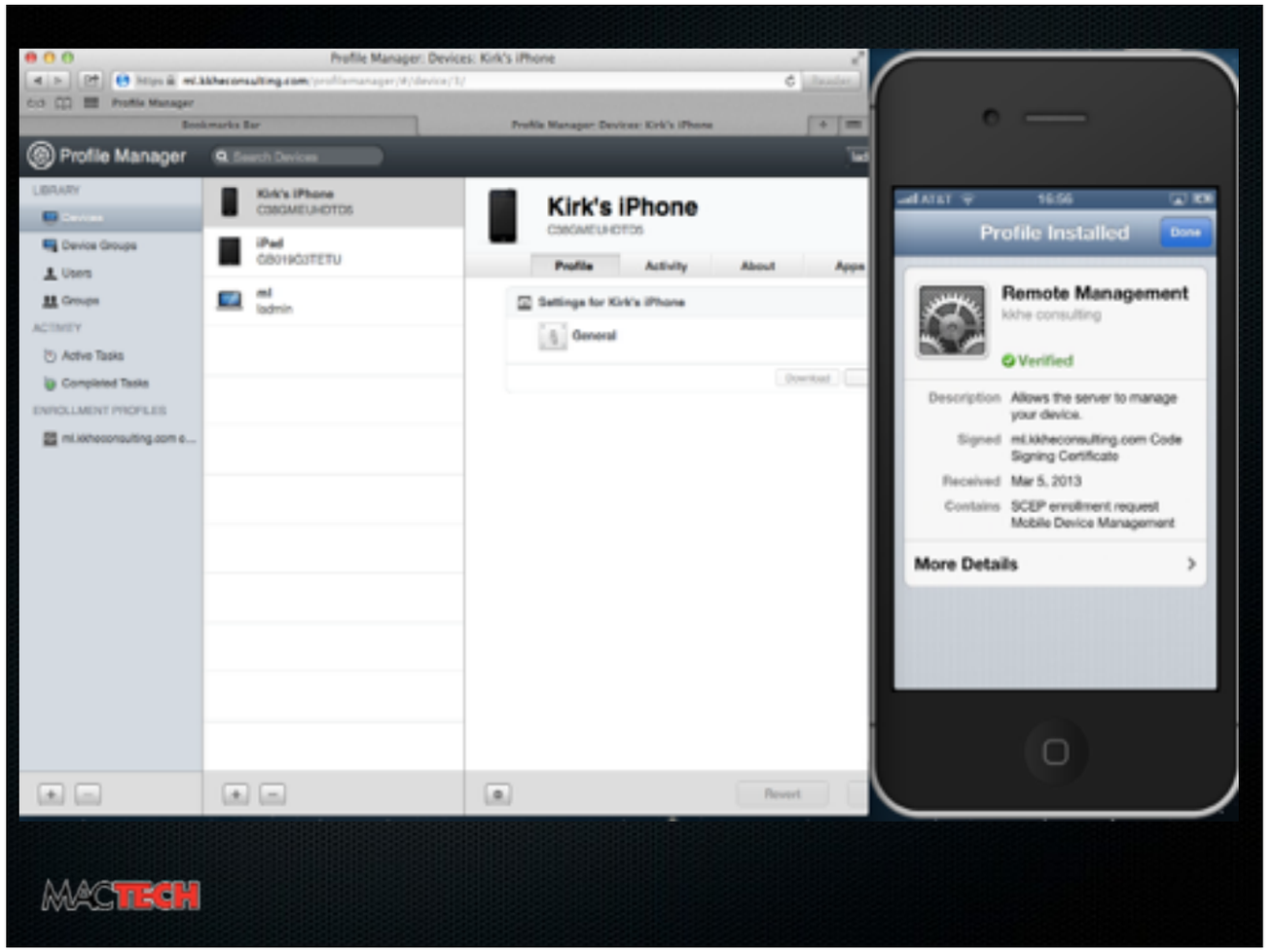

Apple Configurator
Prepare
Supervise
Assign
Settings
Apps
MyMadrid
Sports
Free
Prepare
AT&T
18:54
Photos
WSDOT
Dropbox
1Password
yelp
Authenticator
Truphone
Mail
Phone
Music
Safari

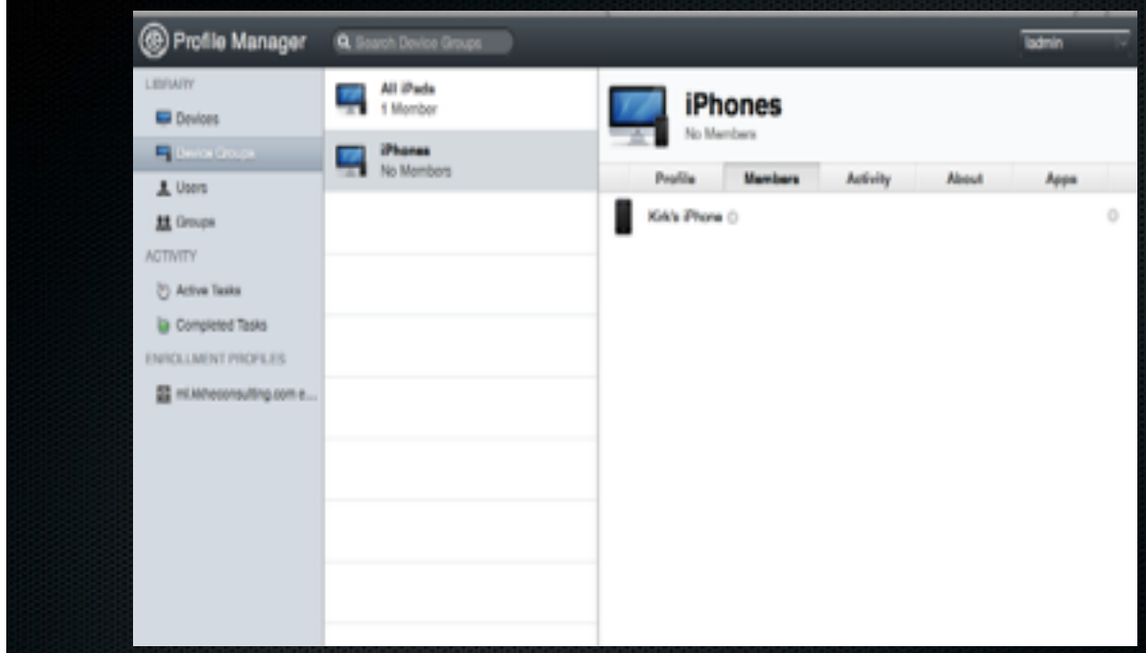

Apple Configurator
Prepare
Supervise
Assign
Settings
Apps
Name:
Kirk's iPhone
Number sequentially starting at 1
Supervision:
Supervised devices can only be configured by Apple Configurator on this Mac.
iOS:
No Change
Erase before installing
Restore:
Don't Restore Backup
Profiles:
ml.kkheconsulting.com env...
Trust Profile for kkhe consa...
All connected devices will be updated
Kirk's iPhone
Tap device to install profile
0 of 1 device prepared
Stop
AT&T
16:55
Cancel
Install Profile
Trust Profile for kkh...
Not Verified
Install
Description
Configures your device to trust the Profile Manager server.
Signed
Apple Configurator (B8:8D:12:09:B4:2A)
Received
Mar 5, 2013
Contains
Certificate
More Details


Apple Configurator
Prepare
Supervise
Assign
Settings
Apps
Name:
Kirk's iPhone
Number sequentially starting at 1
Supervision:
Off
Supervised devices can only be configured by Apple Configurator on this Mac.
iOS:
No Change
Erase before installing
Restore:
Don't Restore Backup
Profiles:
ml.kkheconsulting.com enr...
Trust Profile for kkhe consu...
All connected devices will be updated
Kirk's iPhone
Tap device to install profile
0 of 1 device prepared
Stop
AT&T
16:55
Cancel
Install Profile
ml.kkheconsulting.c...
kkhe consulting
Not Verified
Install
Description
Enrolls your devices with the management server.
Signed
Apple Configurator
Received
Mar 5, 2013
Contains
Device enrollment challenge
More Details

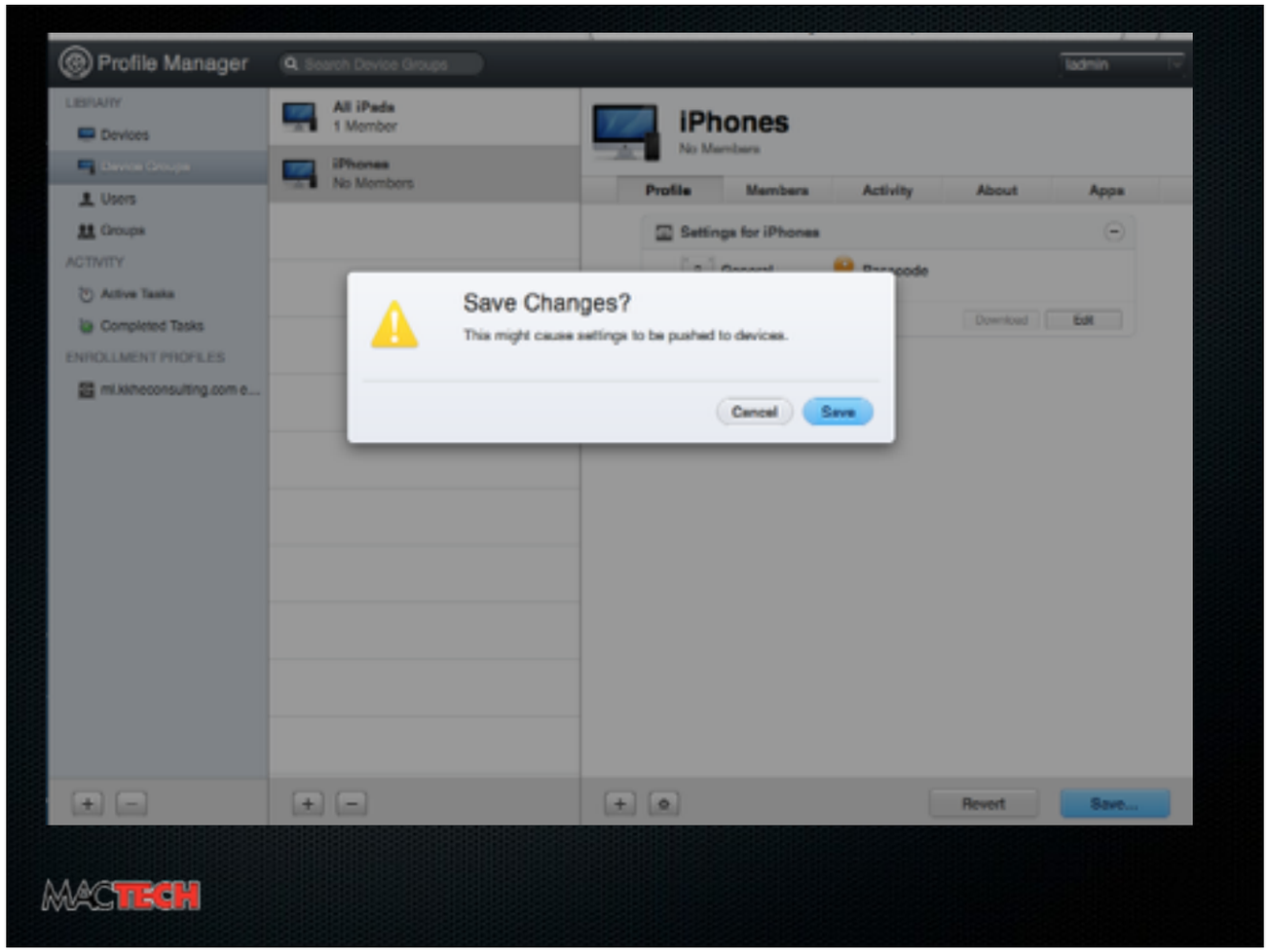

Apple Configurator
Prepare
Supervise
Assign
Setup
Apps
Name:
Kirk's iPhone
Number sequentially starting at 1
Supervision:
OFF
Supervised devices can only be configured by Apple Configurator on this Mac.
iOS:
No Change
Erase before installing
Restore:
Don't Restore Backup
Profiles:
Trust Profile for kkhe consu...
All connected devices will be updated
Kirk's iPhone
Tap device to install profile
0 of 1 device prepared
Stop
AT&T
16:55
Cancel
Warning
Install
Mobile Device Management
Installing this profile will allow the administrator at "https://ml.kkheconsulting.com/devicemanagement/api/device/connect" to remotely manage your iPhone.
The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPhone.
MACTECH

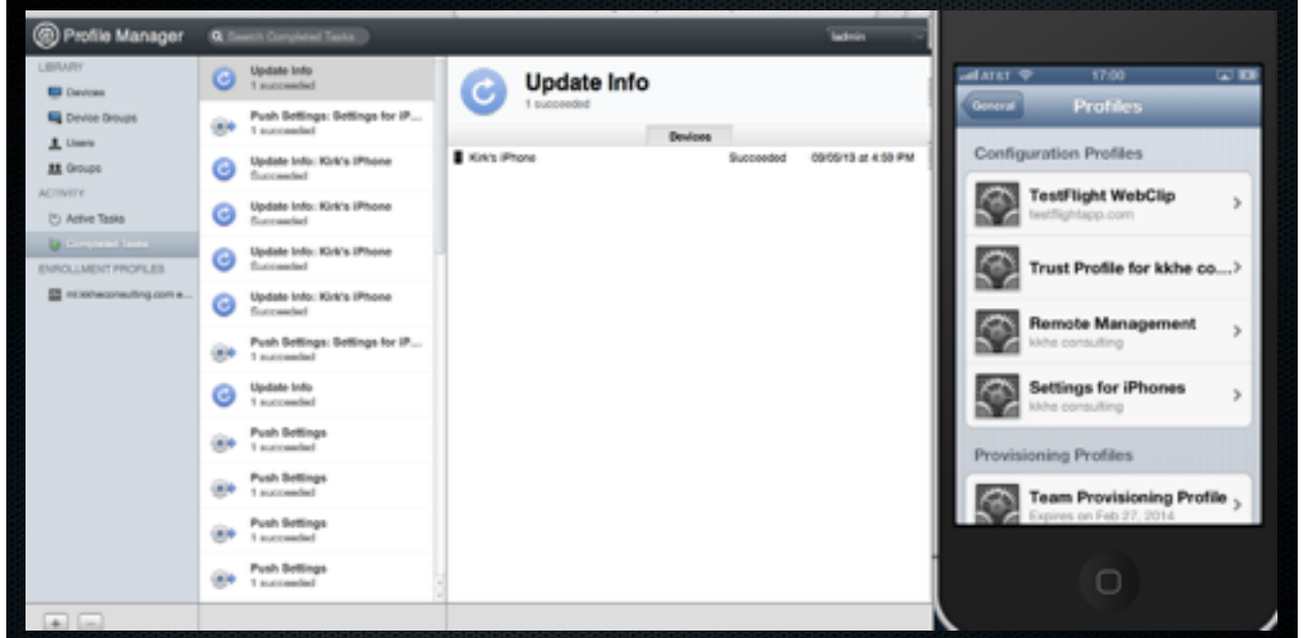

Apple Configurator
Prepare
Supervise
Assign
Apps
Name:
Kirk's iPhone
Number sequentially starting at 1
Supervision:
Supervised devices can only be configured by Apple Configurator on this Mac.
iOS:
No Change
Erase before installing
Restore:
Don't Restore Backup
Profiles:
ml.kkheconsulting.com enr...
Trust Profile for kkhe consu...
All connected devices will be updated
Kirk's iPhone
32 GB iPhone
1 of 1 device prepared
Stop
Profile Installed
Done
Remote Management
kkhe consulting
Verified
Description
Allows the server to manage your device.
Signed
ml.kkheconsulting.com Code Signing Certificate
Received
Mar 5, 2013
Contains
SCEP enrollment request
Mobile Device Management
More Details

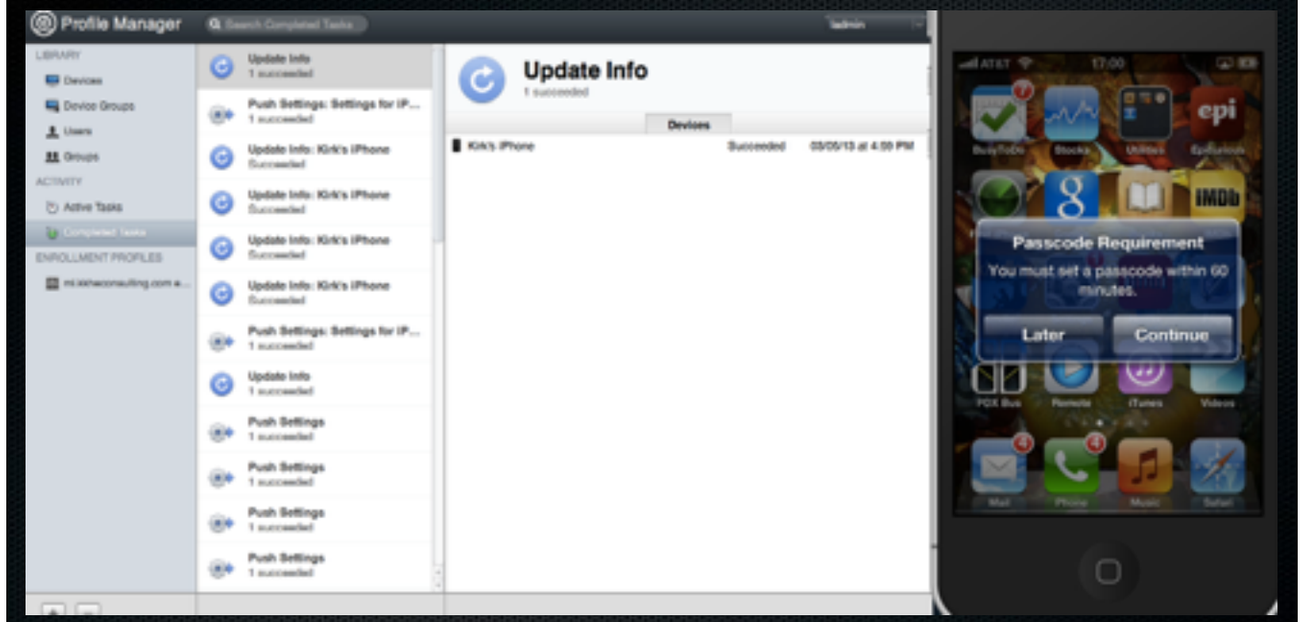

Profile Manager: Devices: Kirk's iPhone
Profile Manager
Kirk's iPhone
Profile
Activity
About
Settings for Kirk's iPhone
General
Profile Installed
Done
Remote Management
kkhe consulting
Verified
Description
Allows the server to manage your device.
Signed
ml.kkheconsulting.com Code Signing Certificate
Received
Mar 5, 2013
Contains
SCEP enrollment request
Mobile Device Management
More Details
MACTECH


Profile Manager
Search Device Groups
admin
LIBRARY
Devices
Device Groups
Users
Groups
ACTIVITY
Active Tasks
Completed Tasks
ENROLLMENT PROFILES
All iPads
1 Member
iPhones
No Members
iPhones
No Members
Profile
Members
Activity
About
Apps
Kirk's iPhone


Settings for iPhones
2 Payloads Configured – Updated 03/05/13 at 4:41 PM
OS X and iOS
General
1 Payload Configured
Passcode
1 Payload Configured
Network
Not Configured
VPN
Not Configured
Certificate
Not Configured
SCEP
Not Configured
Security & Privacy
Not Configured
iOS
Restrictions
Not Configured
Accessibility
Not Configured
Global HTTP Proxy
Allow simple value
Permit the use of repeating, ascending, and descending character sequences
Require alphanumeric value
Requires passcode to contain at least one letter
4
Minimum passcode length
Minimum number of passcode characters allowed
--
Minimum number of complex characters
Minimum number of non-alphanumeric characters allowed
730
Maximum passcode age
Days (1-730) after which the passcode must be changed
--
Maximum Auto-Lock
Device automatically locks when minutes elapse
Passcode history (iOS only)
Number (1-50) of unique passcodes before reuse
--
Maximum grace period for device lock (iOS only)
Maximum amount of time the device can be locked without prompting for passcode on unlock
--
Maximum number of failed attempts
Number of passcode entry attempts allowed before all data on device will be erased
Cancel
OK


Profile Manager
Search Device Groups
ladmin
LIBRARY
Devices
Device Groups
Users
Groups
ACTIVITY
Active Tasks
Completed Tasks
ENROLLMENT PROFILES
ml.kitheconsulting.com e...
All iPads
1 Member
iPhones
No Members
iPhones
No Members
Profile
Members
Activity
About
Apps
Settings for iPhones
Passcode
Download
Edit
Save Changes?
This might cause settings to be pushed to devices.
Cancel
Save
Revert
Save...


Profile Manager
Update Info
1 succeeded
Devices
Kirk's iPhone
Succeeded
09/05/13 at 4:59 PM
Profiles
Configuration Profiles
TestFlight WebClip
Trust Profile for kkhe co...
Remote Management
kkhe consulting
Settings for iPhones
kkhe consulting
Provisioning Profiles
Team Provisioning Profile


Profile Manager
Update Info
1 succeeded
Devices
Kirk's iPhone
Succeeded
Passcode Requirement
You must set a passcode within 60 minutes.
Later
Continue

Questions?

Max Buxton
max@callandy.com

MACTECH