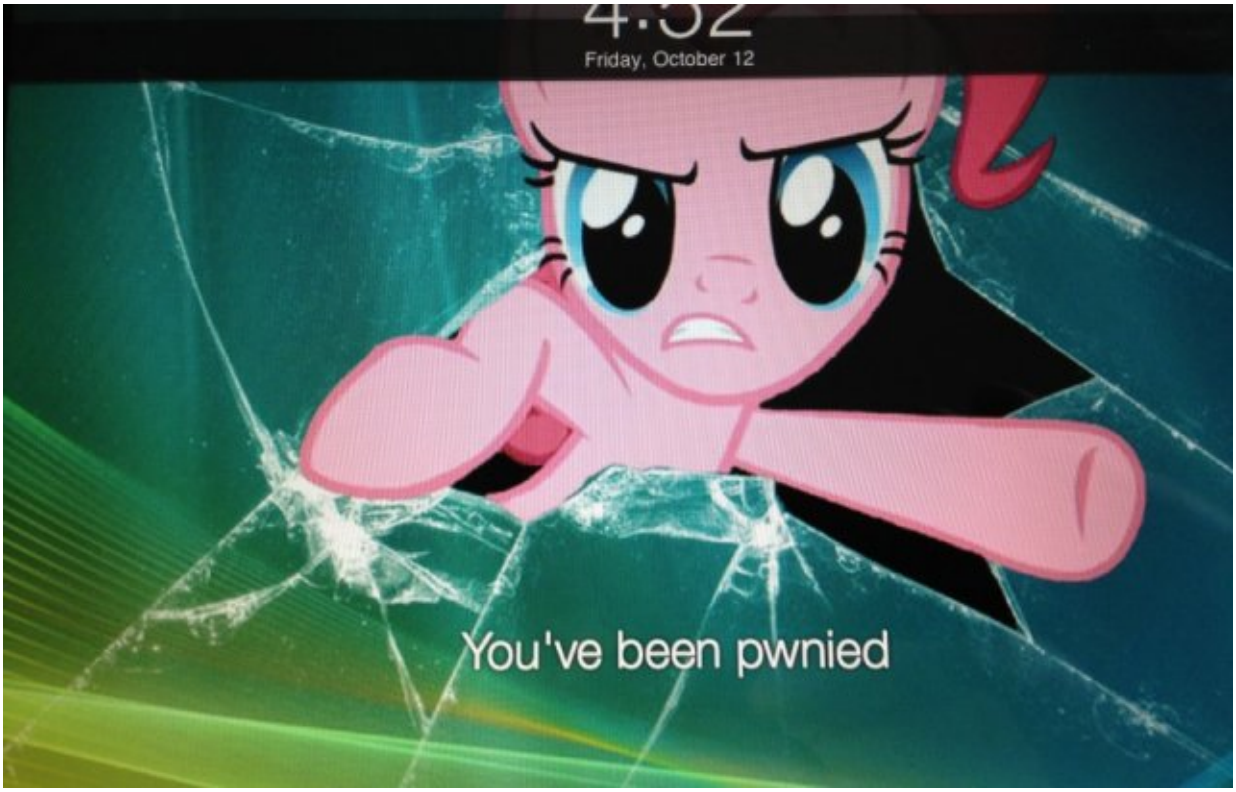
Hands-on: Securing iOS, pwning your kids with Apple Configurator 1.2

How I used Apple's mobile device config update for entertainment and vengeance.



My teenage son's iPad, after being put into "supervised mode" by Apple Configurator.

Apple recently released the latest version of Configurator [1], the company's management software for iOS devices, for download in the Mac App Store. Configurator version 1.2 is intended to give organizations a way to mass-configure iPads, iPhones, and even iPods with applications, settings, and security policies. It's also, as it turns out, the perfect tool to prank a teenage son, teaching him the hazards of leaving his iPad unattended and of interrupting conference calls with extended drum solos.

Configurator version 1.2 is enhanced to take advantage of the enterprise management features in iOS 6 [2]. It provides all the policy configuration muscle Apple gives to mobile device management tool developers with its management interfaces, in a free Mac OS X application. That includes the ability to lock down the lock screen, put a device into "app lock" mode, making it boot straight into an application, and blocking users' access to the rest of iOS's features. All those features let you turn a device into a secure wireless kiosk, a point-of sale system, or (as I did to my son's iPad) a dedicated My Little Pony Ruckus Reader [3] platform with an appropriately themed lock screen.

Of course, I backed all his stuff up first. I'm not that evil.

From iPad to iPwnie in three easy steps

There are two distinct levels of management control in iOS 6—supervised and unsupervised devices. Unsupervised device management is best for BYOD situations; it can be configured without being overly intrusive. Profiles set up this way can be overlaid on existing user settings, and can even be set to automatically expire after a specific period. Admins can give contractors access to resources for the length of a specific project without having to get a hold of their device to revoke it afterward, or give students access for the length of a specific class.

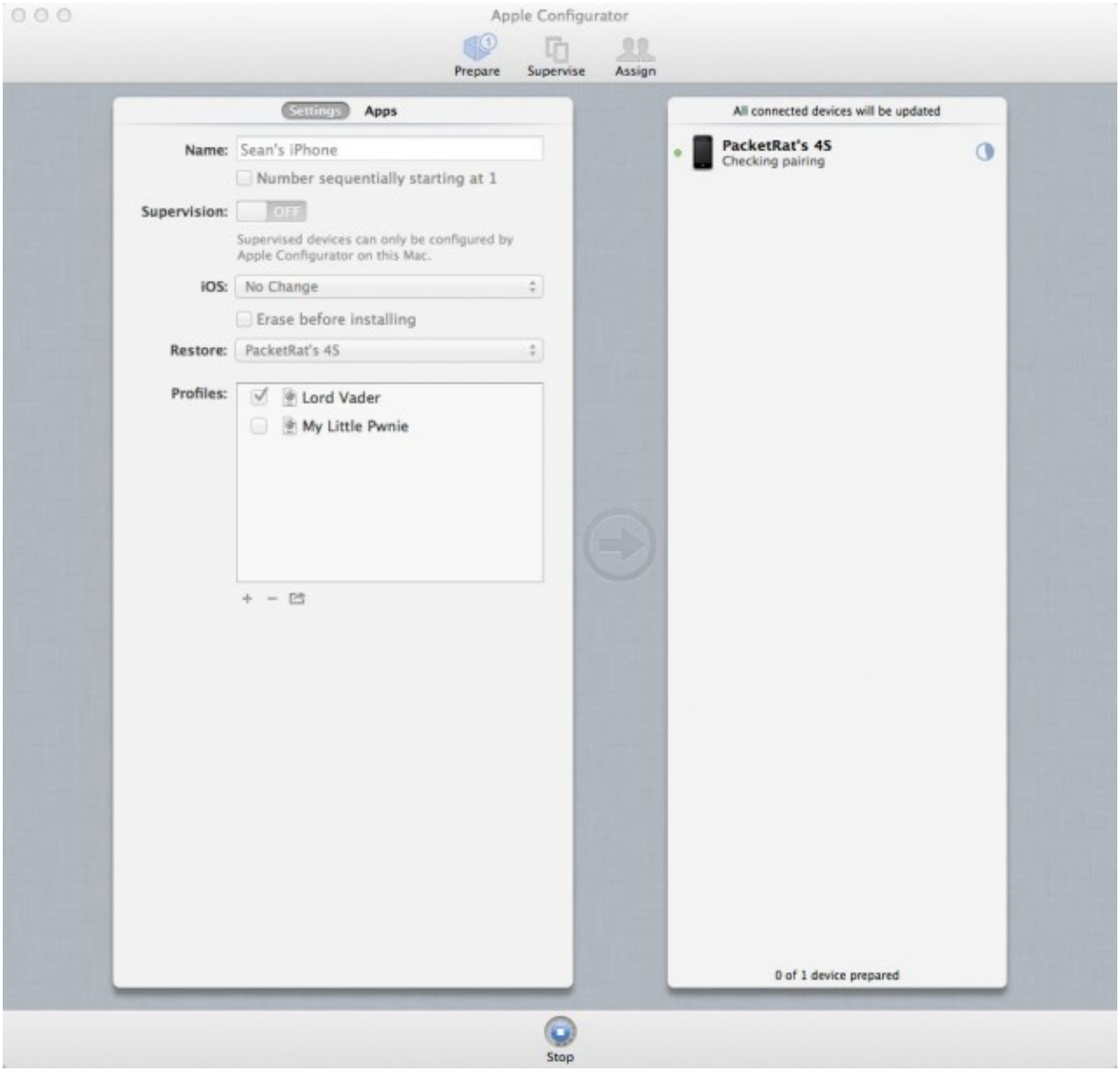
Supervised devices, on the other hand, require a re-install of iOS that throws additional management switches on and gives the administrator more control over configuration. Prior to iOS 6, supervised mode was only available for the iPad. Now, as we noted in our report on iOS 6's enterprise features, it's available for any iOS device.

Supervised mode can prevent the user from changing some or all of the device's configuration, selectively shut off features, prevent users from removing apps, and limit the types of content the device can download or use. It also allows administrators to "app lock" the device, so that it boots up directly into a specific application—with no way for the user to exit from it.

Supervised mode comes at an administrative price, however. While unsupervised profiles can be set up to allow users to enter their usernames and

passwords for features that require authentication, these need to be hard-coded in for devices put in supervised mode. Of course, the level of control from supervised mode is exactly what many companies want for their devices. Most devices that organizations will put in supervised mode will likely be used by multiple people, and won't need to have personalized e-mail or other settings.

Configurator's interface is broken into three views. The "Prepare" view is intended for initial provisioning of devices—setting them up with initial policies in either supervised or unsupervised mode and installing applications. You can also back up one device after it's been completely configured, and use the backup as an image to provision other devices.



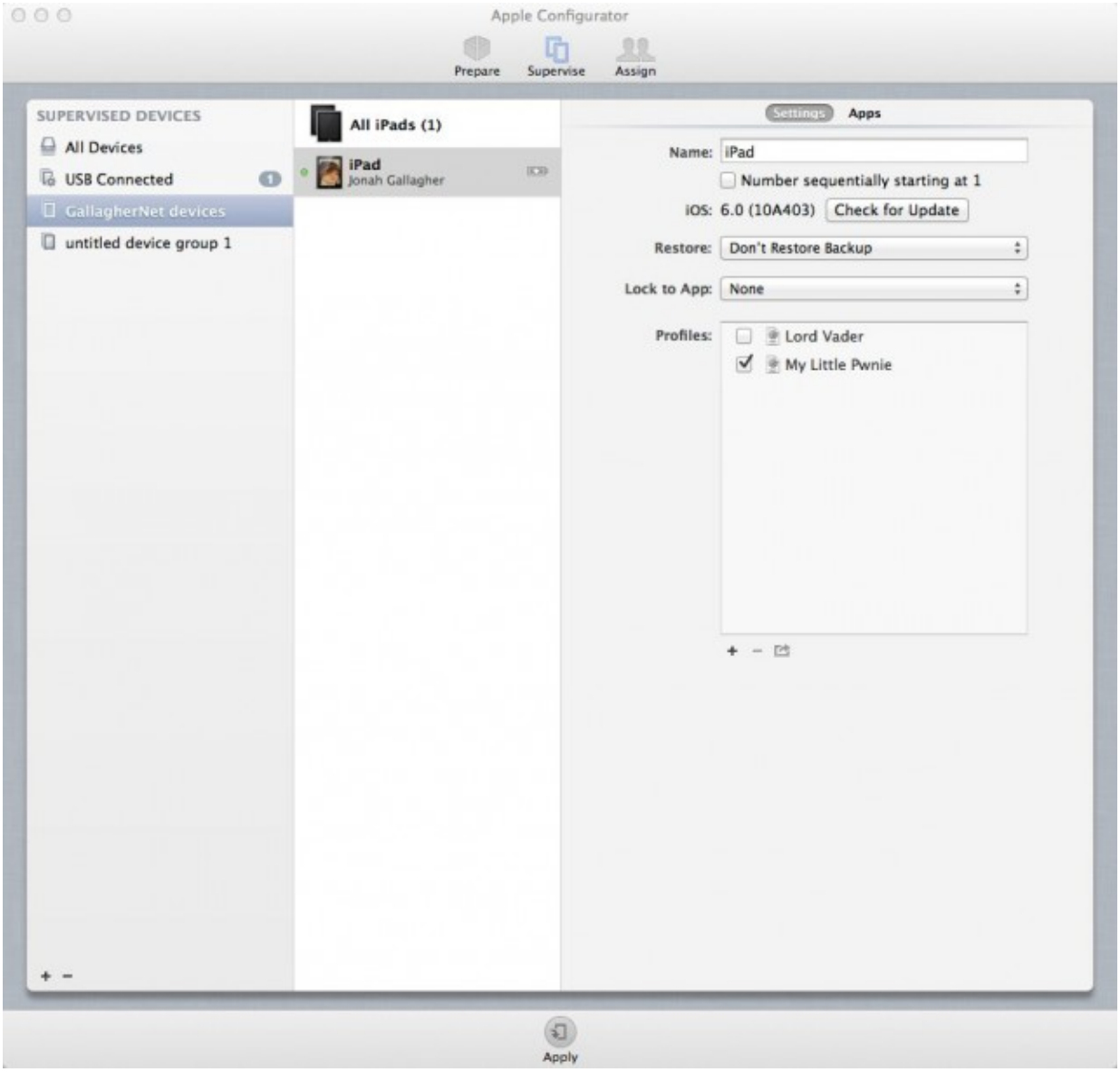
[4]

Enlarge [5] / Configurator in Prepare view, applying a policy profile to my iPhone

4S in unsupervised mode.

Sean Gallagher

The "Supervise" view is intended to manage supervised devices after they're configured. Admins can assign devices to groups so additional policies can be applied in batches. And this is where you can put devices into "app lock."



[6]

Enlarge [7] / Configurator's Supervise view, with my son's iPad connected and policy selected for application.

Sean Gallagher

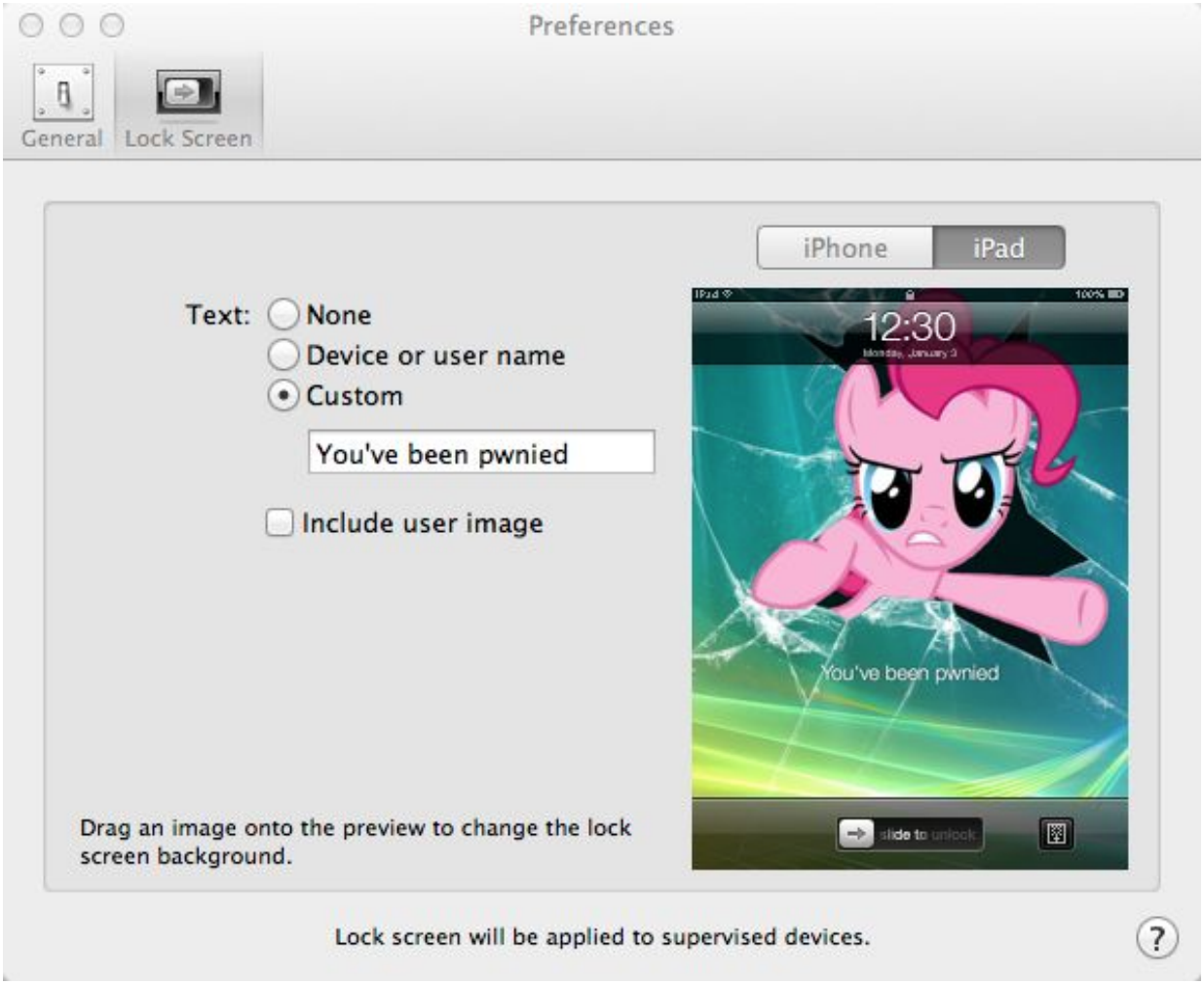
And finally, the "Assign" view is for checking out specific devices to users and managing their personalized application data. When you check in a device, it

backs up the user's data files to Configurator's library, so that they can be re-installed the next time the user is issued the device.

[8]

Enlarge [9] / Configurator's Assign view allows you to check devices in and out, deploy contents specific to users, and back it up for them between uses.

Some of the more general configuration settings for devices—such as lock screen graphics and customized text for supervised devices—are set up in Configurator's preferences menu.



The lock screen settings under Configurator's preferences menu allow you to set a standard lock screen for all supervised devices.

Both Prepare and Supervise allow you to create new policies or edit existing ones, and assign applications to be deployed. You can also import or export profile information (in an XML format with a .mobileconfig file extension) within both views. So one administrator can create a set of profiles to be distributed to anyone setting up iOS devices. They can also be imported and sent out to devices over-the-air by MDM tools via Apple's Push Notification Service, as described in Apple's MDM integration documentation (PDF here [10]). Sadly, there's no over-the-air update integration in Configurator itself, but I suppose some things can't be free.

While a tethered unsupervised device is being configured, it will pop up this window when it is passed profile data.

Sean Gallagher

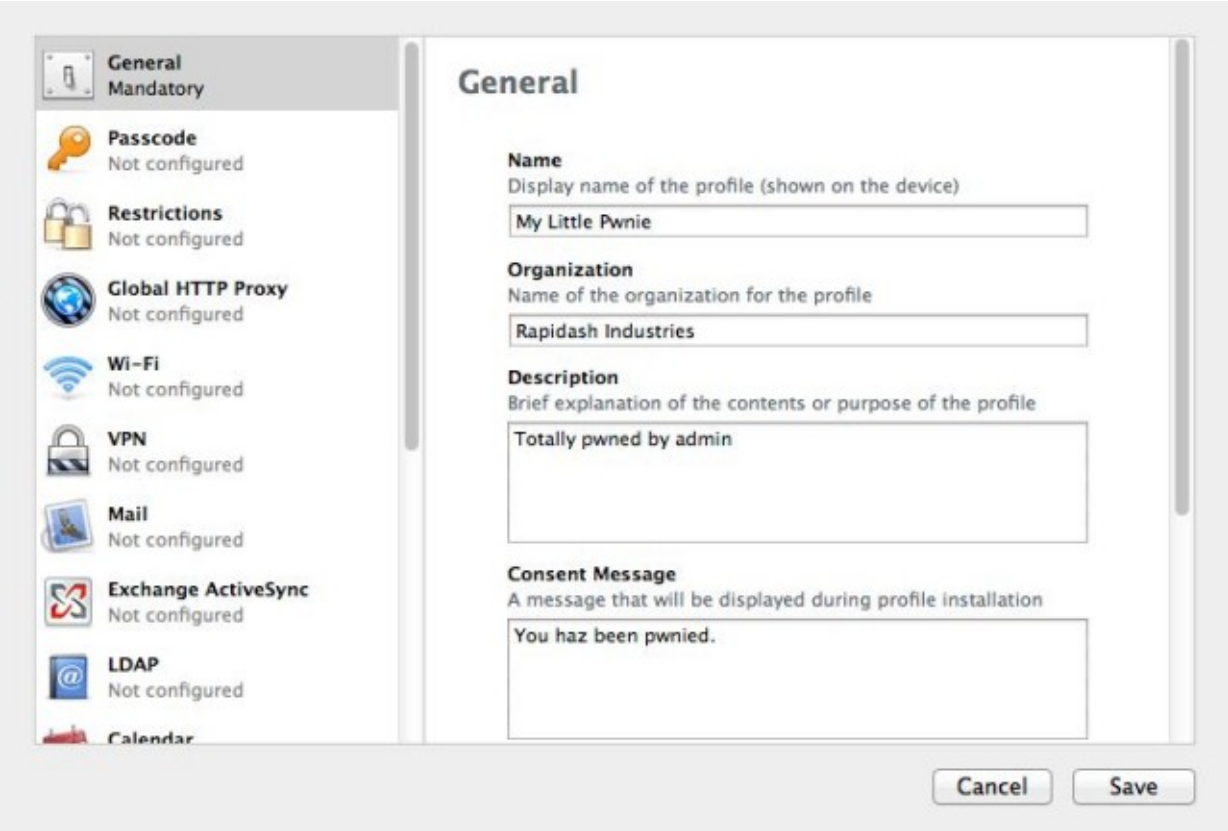
When you touch the "install" button on a profile pushed to an unsupervised device, it pops up a consent message. Since the profiles created by Configurator are unsigned, iOS warns that the profile is "unverified."

Sean Gallagher

A configuration profile sent to an unsupervised device can be uninstalled later by the user from within the iPhone's settings menu. Supervised devices can be prevented from changing or removing profiles.

Sean Gallagher

Configurator's profile editing interface creates a "package" for each component of the configuration an administrator sets. The first set of data for a profile is general information for the header of the profile, including its name, a description, and the consent message that it displays when sent to the device. Once you build profiles, you can deploy them to groups of devices—up to 30 at a time, hooked up by USB hubs. The profiles can be exported as well, and sent through MDM tools for remote policy changes.



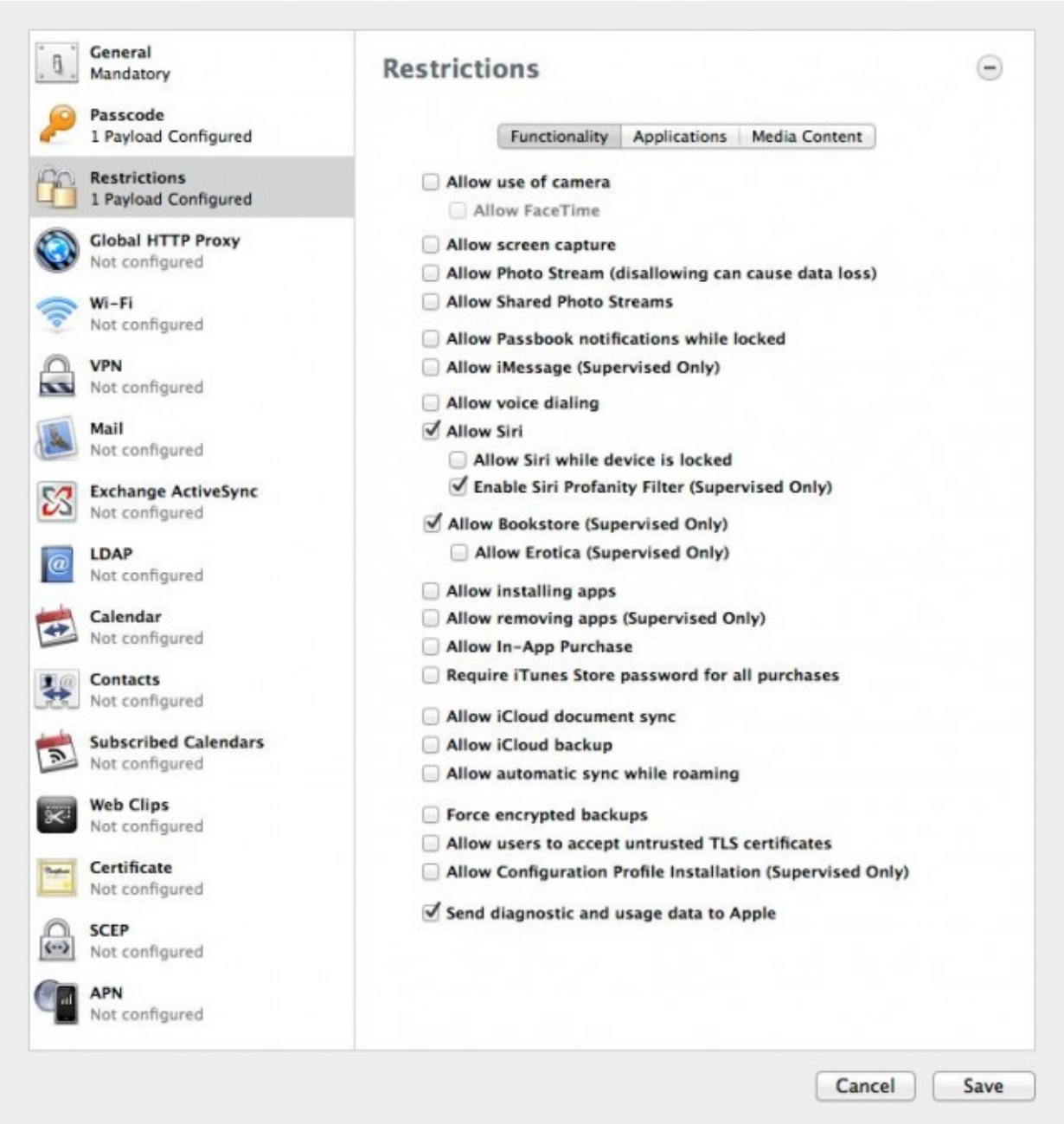
[11]

Enlarge [12] / Every profile needs a name. You can also give it a description and a consent notice, so that when it's exported to an MDM tool admins and users know what's lurking within the profile settings.

[13]

Enlarge [14] / The passcode policy section of the profile editor allows you to set the required length and complexity of user passcodes, as well as how aggressively the device locks itself—and how many wrong answers it allows before it self-destructs the data on the device.

Sean Gallagher



[15]

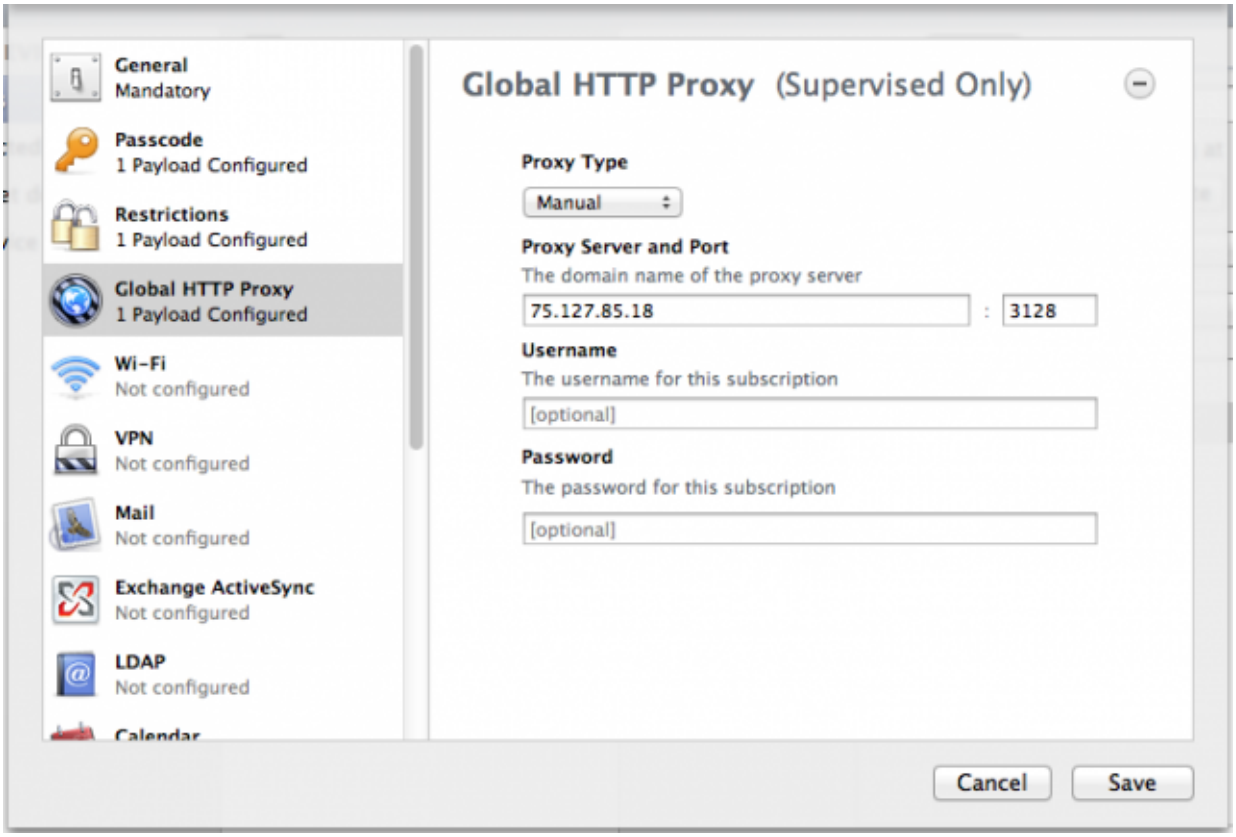
Enlarge [16] / Configurator exposes the "restrictions" settings for iOS policies as a set of check-boxes for iOS functionality, iOS built-in applications (YouTube, the iTunes Store, Game Center, and Safari), and media content (with "rating controls" to lock out anything unseemly).

Sean Gallagher

Configurator now allows administrators to enable and lock Siri's profanity filter, to prevent the app from being persuaded to parrot dirty words. Of course, you can always block Siri altogether. You can also now block (or allow) iOS's Game Center. Configurator policies can also block access to the iBooks bookstore in

supervised mode, or just block anything in the store labeled as "erotica." There are also some features that don't require "supervised mode" that have been added to the policy toolbox. FaceTime and iCloud features such as document sync and Photo Stream can be disabled by policies, for example. In Photo Stream, you can lock down the feature entirely, or just prevent users from pushing photos to shared Photo Streams.

Configurator 1.2 exposes all of the new supervised mode functionality, in addition to new feature and security settings that can be configured without having to get that medieval on the user. For example, Supervised mode isn't required for many of the other new policy controls in iOS 6. FaceTime and iCloud features such as document sync and Photo Stream can be disabled by policies, for example; in Photo Stream, you can lock down the feature entirely, or just prevent users from pushing photos to shared Photo Streams.



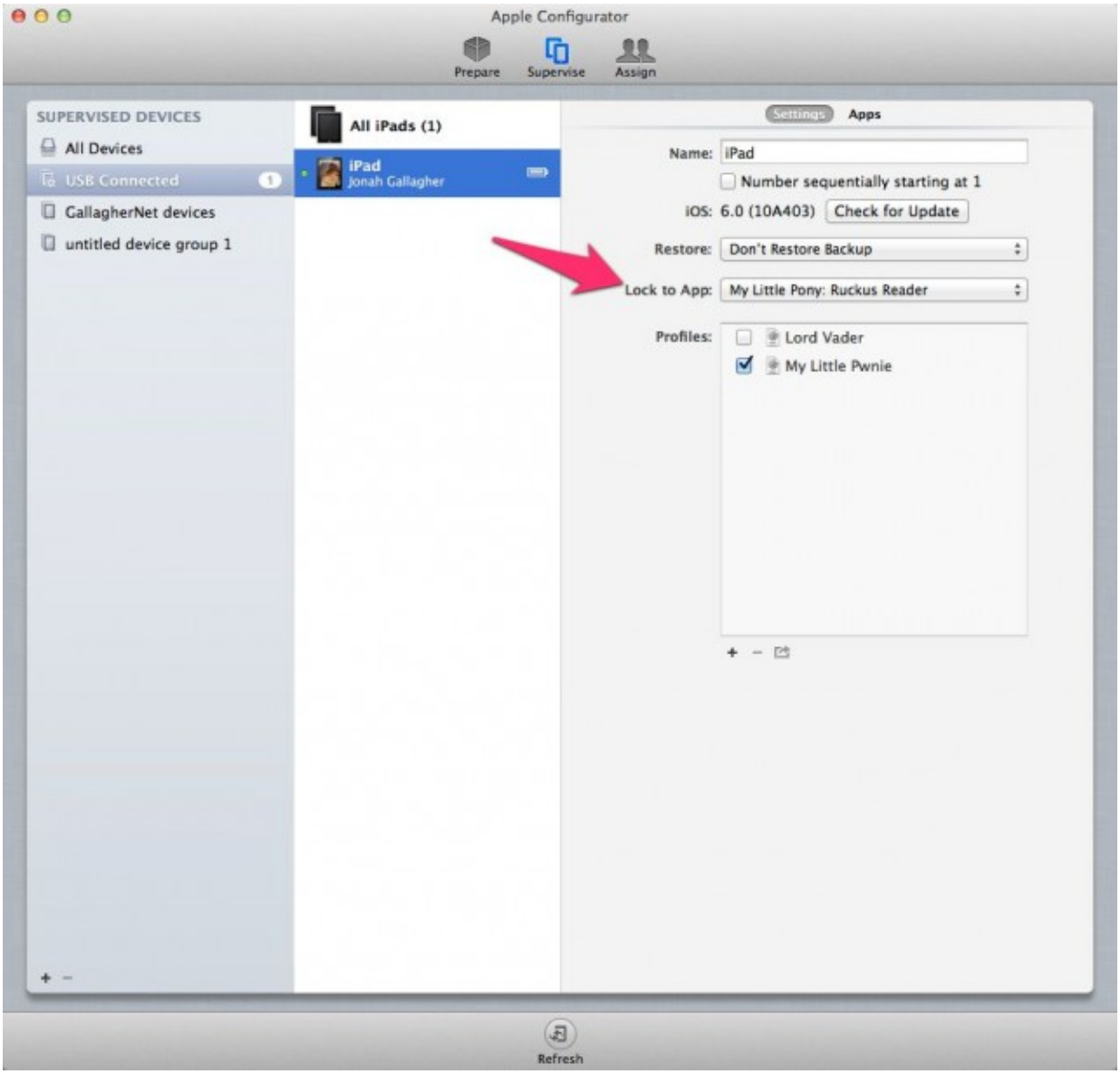
[17]

Enlarge [18] / Another new "supervised mode" capability exposed in Configurator 1.2 is forcing the use of a global proxy for iOS applications. Global proxies can be used to ensure that all of the IP traffic coming to and from an iOS device can be packet-filtered regardless of what network the user is connected through. Of course, you could use the settings to configure an anonymizing proxy for all

your iOS apps as well, but I suspect that's a side many organizations will consider secondary to data loss prevention or enforcing usage policies.

Sean Gallagher

The highest level of control achievable through supervised mode is "app lock" mode. This isn't set in the policy profile itself, but as a switch passed to iOS 6's "Guided Access" feature when docked. You can create a backup of an app-locked device to use as a template, but there's no way to remotely turn app lock on or off over-the-air—which might be a good thing, at least for my son.



[19]

Enlarge [20] / The "Lock to App" setting in the Supervise view allows you to pick the application the device is bound to from those installed on it. Once you've set this here, the only way to turn it off is to re-dock it with Configurator. Here, my

son's iPad is set for all ponies, all the time.

Sean Gallagher

Pwning complete?

Configurator would be even more useful if Apple provided a way for admins to connect it directly into Apple's Push Notification service to do over-the-air configuration. But then, that sort of Configurator would not be a free App Store download—it would require a back-end database of devices and other features that would essentially turn it into an MDM platform. Apple apparently isn't interested in doing that (or at least it hasn't hinted at it) much to the relief of MDM vendors who support iOS devices.

But while Configurator isn't a substitute for an MDM system in larger organizations, it does provide a way for administrators to quickly build policies to be used in MDM environments. Even without remote management, Configurator is probably all many small to mid-sized organizations will need to ensure that "bring your own" iOS devices are configured correctly for e-mail and basic security, or to manage a pool of company-owned devices being issued to employees or students for specific tasks.

At a minimum, Configurator is certainly enough for individuals who want an easier way to lock down their own devices and protect their mobile data. As for its value as family entertainment, the look on my son's face when he turned on his iPad was priceless.

1. https://itunes.apple.com/us/app/apple-configurator/id434433123?mt=12
2. http://arstechnica.com/apple/2012/09/locking-up-locking-down-hands-on-with-ios-6-enterprise-management/
3. https://itunes.apple.com/us/app/my-little-pony-ruckus-reader/id498464830?ls=1&mt=8
4. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator05.jpg
5. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator05.jpg
6. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator01.jpg
7. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator01.jpg

8. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator12.jpg
9. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator12.jpg
10. http://images.apple.com/iphone/business/docs/Mobile_Device_Management_9_2012.pdf
11. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator10.jpg
12. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator10.jpg
13. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator09.jpg
14. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator09.jpg
15. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator08.jpg
16. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator08.jpg
17. http://cdn.arstechnica.net/wp-content/uploads/2012/10/global-http.png
18. http://cdn.arstechnica.net/wp-content/uploads/2012/10/global-http.png
19. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator03.jpg
20. http://cdn.arstechnica.net/wp-content/uploads/2012/10/Configurator03.jpg