

Solution Guide Deploying Apple iOS in Education

MARCH 2013

This document covers strategies for deploying, monitoring, and supporting iOS devices in education environments.



IIIIIMeraki is nowCISCOpart of Cisco.

Table of Contents

Copyright © 2013 Cisco Systems, Inc. All rights reserved

Trademarks Meraki® is a registered trademark of Cisco Systems, Inc.

1 Executive Summary

Mobile devices are seeing remarkable adoption in education, and their use is poised to have a dramatic effect on students across grade and curriculum levels. iOS-powered devices from Apple, including the iPad and iPod, along with the ecosystem of educational content available through iTunes and the Apple App Store, are key learning platforms schools and educators are embracing.

To successfully deploy mobile devices like the iPad in a school setting, tech coordinators need deployment and device content strategies.

This document provides education-relevant deployment best practices for iOS devices using Meraki's mobile device management solution, Systems Manager, and Apple Configurator.

This document is not intended to cover or recommend any element of curriculum development.

2 Requirements

To deploy iOS devices using the instructions in this solution guide, you will need:

1 A Meraki dashboard account with a Systems Manager network

Note: Systems Manager is completely free! To begin, obtain a Meraki Dashboard account by visiting: www.meraki.com/form/systems-manager-signup

If you already have a Meraki dashboard account, log in to and select "Create a Systems Manager Network" from the dropdown menu

2 Mobile devices running iOS 6 or later

3 For supervised devices, a computer running:

- Apple OS X v10.8.2 or later
- Apple Configurator 1.2.1 or later
- Apple iTunes 10.6 or later

3 Meraki Systems Manager Overview

Meraki's Systems Manager is a cloud-based device management solution for iOS and Android devices, and it also provides desktop management for Windows and MAC OS X computers.

Systems Manager provides several features, including Over-the-air (OTA):

- Management of configuration profiles
- App delivery for iOS devices
- Real-time reporting and management of enrolled devices

Additionally, Systems Manager integrates with Apple Configurator to supervise iOS devices. Supervision provides additional control beyond that of configuration profiles.

									1	my profile	sign out
meraki	Network:	Merak	i Corp - Systems Manager	Tag: All	\$			O Searc	ch dashboard		
Monitor	Client	list	Jan 22 19:41 PST to .	Jan 23 19:41 PST							
Overview	Tag 👻	Locat	tion - Move - Comr	mand 👻 Search	Ψ.	435 clients				Download a	as CSV
Clients		Status *	Name	User	Model	OS	Last connected	Connectivity	Disk % used	Tags	+
Remote desktop Security	. 1		stevebyatt10000@gmail.com	stevebyatt10000@gmail.com	Samsung Galaxy S III	Android 4.1.2	now		- 24	6 recently- added	
Software	2		zmbush	Zachary	iMac	Mac OS X 10.7.5	now		= 11	% no-track	
Command line	3		sbiswasimac	Sanjit	iMac	Mac OS X 10.7.5	now		1 34	% <u>HQ</u>	
	4	×.	raultmanmbp	Rhett	iMac	Mac OS X 10.7.5	now		29	% one	
Mobile	5		macbookproimage	guirimte.habtemariam	MacBook Pro	Mac OS X 10.7.3	now		= 12	V6	
Configure	6		jbicket's iMac	jbicket	iMac	Mac OS X 10.7.5	now		65	% <u>HQ</u>	
oomigure	. 7		dodecaphonic	bewest	iMac	Mac OS X 10.6.8	now		31	% devel	
Organization	8		TJMICHIEMBP	тJ	MacBook Pro	Mac OS X 10.7.5	now		38	% <u>HQ</u>	
Help	9	¢.	Sean's Meraki MacBook Pro	seanbutler	MacBook Pro	Mac OS X 10.7.4	now		6	% <u>HQ</u>	



Start Preparing Devices

4 Apple Configurator

Apple Configurator is a free Apple utility that configures and enables advanced settings options via a method known as Supervision. This utility requires devices be physically connected via USB to a Mac running OS X; up to 30 connected devices at a time are supported. A typical deployment of Apple Configurator in a school environment uses mobile carts.

Apple Configurator supports three simple workflows:

Prepare: for updating iOS devices to the latest version of iOS, enrolling devices in Systems Manager, or restoring device backups.

Supervise: once a supervised device is enrolled in Systems Manager, advanced settings can be configured.

Assign: for assigning devices to individual users; individual users can be specified manually or via a directory service.

5 Volume Purchase Program (VPP)

Apple's Volume Purchase Program allows educational institutions to purchase iOS apps and books in volume and distribute them to persons associated with the institution including students, faculty, and other employees in accordance with the App store terms and conditions.

Apps can be reassigned to other students or installed on another iOS device in the future, but this requires upfront planning and selecting the appropriate deployment method. On the other hand, books must be redeemed by a student using his or her personal Apple ID and cannot be reassigned to another student once redeemed.

Content purchased via VPP is downloaded using redemption codes provided by Apple. There is one code per app or book purchased.

4

6 WiFi Planning

When deploying iOS devices, careful consideration of WiFi infrastructure in light of coverage area, device density, security, and OTA encryption requirements is paramount.

A best practice when using Apple Configurator is to provide two separate SSIDs in conjunction with Systems Manager. A basic SSID is used for initial device staging, and a secure SSID connects devices to a school's WiFi network:

1 A staging SSID (SSID-open) for initial device provisioning that is open for Internet access but restricted otherwise

Note: Coverage for this open SSID need not be pervasive; making it available only where iOS device provisioning occurs is sufficient.

2 A preferred, pervasive, and secure SSID (SSID-secure) by which devices access the school's WiFi network and resources; Systems Manager is used to push this SSID's configuration settings to iOS devices

The deployment scenarios in this paper assume the use of two separate SSIDs as described above.

7 iOS Deployment Models

Picking the right iOS deployment model is critical to eliminating management and support issues that can arise once devices are in use by students and instructors.

1 App Ownership

Which Apple ID (institutional or personal) will be used to redeem app codes purchased by the school in volume?

2 Device Personalization

Are users allowed to personalize content and settings on the device?

These questions guide the selection of a deployment model, the use of Meraki's Systems Manager, and the necessity of using Apple Configurator for initial setup and ongoing maintenance.

Table 1: Guide to selecting a suitable deployment model

	Personal Ownership	Institutional Ownership	Layered Ownership
Owner of Apps	Student	School	Both student and school
	Apps redeemed with personal iTunes ID	Apps redeemed with ID associated with school	Use school iTunes ID for purchased apps; personal ID after initial setup
Device Personalization	Yes	No	Yes
Usage Model	Single User	Multiple Users - Temporary Device Usage	Extended Single User - Future Reassignment
User's Age	13 years & Above	All Ages	13 years & Above
Initial Setup	Systems Manager	Apple Configurator*	Apple Configurator*
		Systems Manager	Systems Manager
Maintenance	Systems Manager	Apple Configurator	Systems Manager
Reporting	Systems Manager	Systems Manager	Systems Manager

*Use Apple Configurator to initially supervise devices and deploy institutional apps

7.1 Prerequisites for Preparing Systems Manager for iOS Devices



To start using Meraki Systems Manager with Apple iOS devices, you need to upload an SSL certificate obtained for free from Apple to the Meraki dashboard. This certificate is unique to your organization's Systems Manager account and very easy to install by following these steps:

- 1 Log in to the Meraki dashboard and select your Systems Manager network.
- 2 Select the 'Organization' tab and go to the 'Settings' page.
- 3 Follow the instructions under the 'iOS mobile device management' section by downloading the certificate signing request (CSR) from this page to generate a signed certificate from Apple.
- 4 Visit identity.apple.com/pushcert and sign in with a verified Apple ID and follow the instructions.

Once you upload the signed certificate from Apple into the Meraki dashboard, you are ready to get started securely enrolling Apple iOS devices.

Warning: There might be intermittent issues getting some versions of Internet Explorer (IE) to work properly with the Apple Push Notification Certificate (APNS). Try another browser if you have issues getting the APNS properly uploaded and accepted to the Meraki dashboard.

	Step 1: Enter your Network ID
	Register
On-device setup	
To enroll	
	1. From the device, open: <u>m.meraki.com</u>
	2. Enter your Network ID: 007-978-7409
	3. Press register
	4. In the profile that appears, press 'install', then 'install' again to confirm
To un-enroll	 In the profile that appears, press install, then install again to confirm
To un-enroll	1. On the device, open 'Settings'
To un-enroll	 On the device, open 'Settings' Select 'General'
To un-enroll	 On the device, open 'Settings' Select 'General' Select 'Profiles'
To un-enroll	 On the device, open 'Settings' Select 'General'
To un-enroll	 On the device, open 'Settings' Select 'General' Select 'Profiles'

Configuration \times	Manual ‡
SSID	School–District–SSID
	Auto join Automatically join the target network Hidden network Enable if the target network is not open or broadcasting
Proxy setup	None ‡
Security	WPA/WPA2 Enterprise 💲
Enterprise Settings	Protocols Authentication Trust
	Accepted EAP Types Authentication protocols supported on target network TLS LEAP EAP-FAST TTLS PEAP EAP-SIM

Enable passcode policy enforcement	Require passcode Require that the user set a passcode to secure the device
Passcode strength	✓ Allow simple value Permit the use of repeating, ascending, and descending character sequences
	✓ Require alphanumeric value Require passodes to contain at least one letter
Minimum passcode length	Smallest number of passcode characters allowed
Minimum number of complex characters	\$ Smallest number of non-alphanumeric characters allowed
Maximum passcode age	
Auto-Lock	Days after which passcode must be changed (1-730 days, or none) Never : Maximum allowed auto-lock value. Supported values: 2/5/10/15/never for iPads, 1-5/never for iPhones
Passcode history	
Grace period for device lock	Number of unique passcodes before reuse (1-50, or none) None +) Amount of time the device can be locked without prompting for the passcode on unlock

7.2 Personal Ownership

The personal ownership model allows students to use devices and apps in a manner typical of a consumer experience. In this deployment model, only the student's personal iTunes account is used for configuration and app installation. This means all redeemed apps are retained by the student. Apps purchased by the school but redeemed with the student's personal iTunes account cannot be reclaimed by the school.

- Begin with new or unconfigured devices. Perform initial setup using the built-in Apple setup assistant. Skip the process of providing an iTunes ID.
- 2 Connect the devices to an open wireless SSID (SSIDopen) and go to http://m.meraki.com.
- In Meraki Systems Manager, enroll the devices under the Mobile > Deployment page. Use the provided network ID to complete enrollment.
 - 4 To simplify management and to deploy apps to groups of devices, tag them in Systems Manager.
 - 5 Define a Systems Manager profile to deploy secure WiFi settings (SSID-secure) and a passcode policy on the device.
 - 6 Deploy devices to end users who then complete their set up using their personal iTunes ID.

The use of Apple Configurator in this deployment model is optional, but can be leveraged to enforce device restrictions unavailable with 3rd party mobile device management solutions.

dd a n	ew App: Mat	h Board		Coun	try: United States × Search Cancel		
ad Ap	ps						
	Title	Vendor	Version	Category	Description	Price	
	MathBoard	PalaSoftware Inc.	2.0.2	Education	MathBoard is an excellent math learning app for your iPad, iPhone or iPod touch. • One of the top educational apps worldwide. • Featured in Apple iPad	\$4.99	Ad
+ - × ÷	Conundra Math: a brain tr	Sarah Pierce	1.1	Games	★ Great exercise for your brain! ★ Conundra Math is a simple number game that is easy to learn, but hard to put down. Combine a series of numbers us	Free	Ad
	aMathing Numbers: a brain	Fourfig Applications S.L.	1.5	Games	Optimized for iPhone 5 screen! Keep your brain in shape using new technologies. This addictive arithmetic game will improve your mental abilities whi	\$0.99	Ad
3 4	A Montessori Approach to 	Rantek Inc.	1.7	Education	*** Join us on Facebook: www.facebook.com/mobilemontessori *** *****Used in schools and by parents all over the world! ***** See it used in a Montes	\$2.99	Ad
× 2 + +2	Math Fact Master - Additi	TicTapTech, LLC	4.2	Education	OVER 100,000 DOWNLOADS! Consistently ranks as a top 10 Education app in the App Store! Quotes from recent reviews:	\$0.99	Ad

Once the devices are enrolled in Systems Manager, apps from the app store as well as additional configuration profiles can be remotely pushed to them. Tags can group devices to receive specific apps.

MathBoard X + MathBoard	nd ×
Vendor:	PalaSoftware Inc.
Description:	MathBoard is an excellent math learning app for your iPad, iPhone or iPod touch. • One of the top educational apps worldwide. • Featured in Apple iPad TV ads "Learn" and "iPad its Delicious". • Appeared on the TODAY Show. WHAT THE EXPERTS SAY: "This is the best integer practice app or program I have
	View in the iTunes web catalog
Scope:	Install on devices with ANY tag \$
Redemption codes:	
	One code per line. Purchase codes from the Apple Volume Purchase Program
	Remove with MDM Remove this app when the management profile is removed
	Prevent backup

Systems Manager integrates with Apple's Volume Purchase Program (VPP), allowing redemption of purchased apps via redemption codes.

8



7.3 Institutional Ownership

In this model, the installation of the Meraki management profile, new apps, and any app updates are done by connecting each iOS device (via USB) to the computer running Apple Configurator that was originally used to stage the device. Because Systems Manager integrates with Apple Configurator, you can automatically enroll devices via management profiles.

Systems Manager provides asset tracking, hardware and software inventory management, reporting, and remote troubleshooting for enrolled devices.

A mobile cart is commonly used in this deployment model. A Mac running OS X, connected to the school's network and running Apple Configurator, is needed. Additionally, it must have iTunes installed, using the school's iTunes account.



Warning: When you supervise a device, Apple Configurator performs a software restore.

ne Apple Configurator. Be	g the management profile on a large number of devices is low is a link to the management profile for your port the profile into the Apple Configurator to enroll devices.
lanagement profile	meraki_sm_mdm.mobileconfig
	Preferences
eral Lock Screen	ce is connected:
Automatically refre	sh
When a supervised device	ce is refreshed: profiles Configurator did not install

- Log in to your Meraki dashboard, select your Systems Manager network, and access the Mobile > Deployment page; download the Meraki management profile file, xxxx.mobileconfig, to your Mac's hard drive.
- 2 Download institutional apps from iTunes.

3 On your Mac, open the Apple Configurator > Preferences pane; in the General tab, check both boxes to automatically refresh and remove any nonsanctioned apps or profiles.

- 4 Use the Lock Screen tab to set additional preferences.
- 5 In the Apple Configurator Prepare pane, select the Settings tab; import the Meraki management profile file, xxxx.mobilconfig.

NOTE: Ensure the Meraki management profile is unchecked. The management profile cannot be installed at this stage since the device does not have network connectivity.

6 In the Apple Configurator Prepare pane, select the Apps tab; import any paid apps, and include VPP codes.

000		rippie ee	onfigurator		
			i 1	2	
		Prepare Supe	ervise Ass	ign	
		Setting	Apps		
	Name:	Meraki K-12	1		
		✓ Number se	quentially s	tarting at 1	_
	Supervision:	ON			
		Supervised devid Apple Configura	es can only b tor on this Ma	e configured by Ic.	
	iOS:	Latest			•
		C Erase befor	e installing		•
	Restore:	Don't Restore	Backup		•
	Profiles:	Mera	ki Managen	nent	
			pare	_	
200		Pre Apple Co	nfigurator	_	
000		Pre Apple Co	nfigurator		
Supervised d	A	Apple Co	nfigurator	Settings Apps	
_	4	Apple Co Prepare Supe	nfigurator Nise Assign Name:	Meraki K-12 1	/starting at 1
SUPERVISED D	4	Apple Co Prepare Supe II i Pads (1)	nfigurator rvise Assign Name: IOS:	Meraki K-12 1 Number sequentially 6.1 (10B141) Check f	
SUPERVISED D	4	Apple Co Prepare Supe II i Pads (1)	nfigurator rvise Assign Name: iOS: Restore:	Meraki K-12 1 Number sequentially 6.1 (10B141) Check f Don't Restore Backup	for Update
SUPERVISED D	4	Apple Co Prepare Supe II i Pads (1)	nfigurator rvise 233 rvise 245 Assign Name: IOS: Restore: Lock to App:	Meraki K-12 1 Number sequentially 6.1 (10B141) Check f Don't Restore Backup None	ior Update
SUPERVISED D	4	Apple Co Prepare Supe II i Pads (1)	nfigurator rvise 233 rvise 245 Assign Name: IOS: Restore: Lock to App:	Meraki K-12 1 Number sequentially 6.1 (10B141) Check f Don't Restore Backup	ior Update
SUPERVISED D	4	Apple Co Prepare Supe II i Pads (1)	nfigurator rvise 233 rvise 245 Assign Name: IOS: Restore: Lock to App:	Meraki K-12 1 Number sequentially 6.1 (108141) Check 1 Don't Restore Backup None	ior Update
SUPERVISED D	4	Apple Co Prepare Supe II i Pads (1)	nfigurator rvise 233 rvise 245 Assign Name: IOS: Restore: Lock to App:	Meraki K-12 1 Number sequentially 6.1 (10B141) Check f Don't Restore Backup None	ior Update
SUPERVISED D	4	Apple Co Prepare Supe II i Pads (1)	nfigurator rvise 233 rvise 245 Assign Name: IOS: Restore: Lock to App:	Meraki K-12 1 Number sequentially 6.1 (108141) Check 1 Don't Restore Backup None	ior Update

At this stage, you are ready to create a master backup iOS device, which will be used as the template for additional devices.

7.3.1 Creating and enrolling your master backup device

 Select a new or unconfigured iOS device and connect it to the Mac running Apple Configurator.

- 2 In the Apple Configurator Prepare pane, turn on Supervision and click "prepare."
- On the newly prepared iOS device, complete initial setup using the built-in Apple setup assistant. Skip the process of providing an iTunes ID. Connect the device to an open SSID (SSID-open).
 - 4 Customize the device as needed including setting up your wallpaper, rearranging app icons, setting bookmarks, etc.
- 5 Once device customization is complete, go to the Apple Configurator supervise pane; check the Meraki management profile and select 'Apply'/'Refresh.'

Important: The iOS device requires network connectivity (SSID-open) in order to complete the installation of the Meraki management profile.

- 6 Your iOS device is now supervised and enrolled in your Systems Manager network; you now have a master/template iOS device.
- 7 Backup this device with Apple Configurator before applying any Systems Manager policies, and name the backup; now you are ready to prepare the remaining devices.
- 8 Disconnect the prepared master/template iOS device.

7.3.2 Enrolling remaining iOS devices

- 1 Connect new, unsupervised iOS devices (up to 30 at once).
- 2 In the Apple Configurator Prepare pane, set the devices to restore automatically from the backup created; name the devices and check the option to number them sequentially.
- 3 Make sure the Meraki management profile is now checked in the Apple Configurator Prepare pane.
- 4 Connect additional devices as needed, and click "prepare."
- 5 Go to the Apple Configurator supervise pane, click 'apply'/refresh' to ensure all devices are supervised.
- 6 Complete what is left of the iOS setup assistant to ready the iOS device for use.

At this stage all devices will be prepared, supervised, and enrolled into your Systems Manager network. Devices can now be tagged, and management profiles can now be pushed to the devices via the previously configured open SSID.

The secure wireless SSID (SSID-secure) should be selected as the preferred connection as part of the devices' Systems Manager configuration.

Configure the following items and set the following best practice restrictions in Systems Manager:

- · Configure secure WiFi SSID
- Configure a Global HTTP Proxy
- Disable Installing apps
- Disable iTunes Store
- Disable iBookstore
- Disable iCloud Backup
- Disable Game Center
- Disable iMessage

000	Preferences	
General Lock Screen		
When a supervised devic ☑ Automatically refree		
When a supervised devic	e is refreshed:	
Remove apps and p	rofiles Configurator did not install	
Play sound on completio	n: None ‡	
Reset all dialog warnings	Reset Warnings	?

7.4 Layered Ownership

Use the layered ownership model to allow students to personalize a device while still allowing a school to retain ownership of paid apps. This model uses a slight variation on the institutional ownership model's setup and configuration, as discussed above.

To configure devices in a layered ownership model, follow all the steps above for deploying the institutional ownership model, with one exception:

On your Mac, open the Apple Configurator > Preferences pane; in the General tab, check the box to automatically refresh devices; **de-select the check box to remove apps not installed by Apple Configurator.**

Once the layered ownership model's configuration steps are complete, the iOS devices should be given to students to complete the iOS setup assistant, including inputting a personal Apple iTunes ID.

To install new, institution-owned apps (or updates to them) with this model, you will need to reconnect the iOS devices to the same Apple Configurator computer used for initial setup. Personal apps, however, can be downloaded by the user; free apps can be delivered via Systems Manager iOS app store integration.

8 Privacy

When managing and monitoring mobile devices, choices must be made regarding user privacy when implementing capabilities such as location tracking. Systems Manager allows you to disable these types of features, which can be especially useful if devices are taken home by students or faculty for personal use.

From within Systems Manager, selecting Mobile > Settings > Privacy provides the option to disable location tracking.

Restrictions	Passcode	WiFi	VPN	Web Clips	Credentials	Backpack	Privacy
Enable priva	acy settings available privacy se	ettings					
Location Setting	js		v location v SSID tra				

9 Apple ID Management

An Apple ID is an e-mail address that serves as a user's credentials for everything done with Apple, including buying and downloading apps from the App store, accessing content on iTunes, backing up content to iCloud etc.

One of the common areas of questions around deploying Apple iOS devices in education is how to handle Apple IDs and which specific one to use for deploying Apps.

- What Apple ID should be used to deploy apps? Should a school use a student Apple ID or an institution/district Apple ID?
- How many Apple IDs should an institution create?

While the question about student versus institutional ID can be easily resolved based on the ownership model used, dealing with an organization level ID design can range from a single Apple ID for the entire district to multiple IDs for individual schools or departments within a district. The choice one makes here usually depends on the administrative model and internal processes of a given school district.

While every environment is different, a single Apple ID per school district typically provides the most flexibility for App reuse and reassignment across the school district. A single Apple ID, however, introduces other questions around password management for the Apple ID across potentially multiple administrators. Multiple Apple IDs tend to be appropriate for large school districts with several campuses and a distributed administrative team.

The table below captures the pros and cons of how educational institutions can think about Apple ID management and select the option that fits best in their environment for VPP apps.

Table 2: Apple ID management options for VPP apps.

Apple ID Option	Pros	Cons
Personal Apple ID	Low administrative overhead - users deploy all apps	Lack of app reuse across users; users retain apps
Single Apple ID per Institution	Institution retains apps for reuse	Administrative overhead
Multiple Apple IDs per Institution	School retains apps Facilitates distributed administration	Requires supervision to transfer apps to other Apple IDs Some administrative overhead

10 Supervision Caveats

Supervision allows an organization to control additional aspects of the device beyond configuration profiles and restrictions.

In addition, if you wish to reclaim apps deployed via VPP codes, the iOS device is required to have been supervised prior to initial app deployment.

Supervised devices must be re-connected to Apple Configurator for app updates and, with the Institutional deployment model, to remove any unsanctioned apps on the device.

Things to consider with respect to Supervision:

- Supervision requires devices running iOS 5 or later.
- A device can be supervised if it is unconfigured or has been factory reset; supervising a previously configured device will erase all apps and content on the device.
- Supervised devices are tied to the MAC OS devices running Apple Configurator that the device was supervised with; a supervised device can only sync with iTunes running on that same MAC OS device.
 - iOS specific restrictions Device functionality Allow installing apps Allow screen capture Allow voice dialing Allow FaceTime Allow automatic sync when roaming Allow Siri Allow Passbook notifications while locked Allow in-app purchases Force user to enter iTunes Store password for all purchases Allow multiplayer gaming Allow adding Game Center friends Allow use of YouTube Applications le access to applications on the Allow use of iTunes Store Allow use of Safari Enable autofill Force fraud warning Enable javascript Block popups iCloud Allow backup access to iCloud services Allow document sync Allow photo stream Content ratings Allow eveltable events and and and a sets Control

l access to apps and media	Allow exp	non music and pour	Jasis
gs region ne region for the ratings	United States	*	
ed content ratings	Movies:	PG-13	\$
	TV Shows:	TV-PG	\$
	Apps:	Allow All Apps	\$

• Reconnecting a supervised device to Apple Configurator will reconfigure the device back to a desired configuration.

- Additional restrictions are available to supervised devices running iOS 6 or later (these settings can be controlled using Meraki Systems Manager):
 - Global Network Proxy: Routes all web traffic through a proxy server for content filtering.
 - Allow iMessage: Disabling this feature prevents students from iMessaging each other.
 - Allow Removing Apps: Disabling this feature prevents students from removing apps on the home screen.
 - Allow Game Center: Disabling this feature removes the Game Center icon from the home screen.
 - Allow iBookstore / Allow iBookstore Erotica: Disabling these options completely prevents access to iBookstore or to adult content, respectively.
 - Single App Mode: Locks users to a single app, even after the device is powered down and rebooted.

11 Setting Restrictions

A number of restrictions can be applied on any device, regardless of whether the device is supervised or not. While every school environment has its own set of policies, it is useful to think about what an institution is looking to accomplish with iOS devices, and set practical restrictions as necessary.

For instance, the restriction to disallow installation of apps make sense in an ownership model where additional device customizations is not desirable. When devices are shared among students, enabling syncing with iCloud might not be the right approach, as iCloud accounts might be associated with individuals and students are unlikely to always be assigned the same device in a share model.

On the other hand, there might be very good reason to set restrictions around age appropriate content, if iTunes is available for students to use.

As a best practice rule of thumb, an institution is well served by thinking through its use case and deployment model and having the relevant parties, which might include educators and parents, weigh in on what specific restrictions to enable.

Rating Sets the Allower

12 Meraki Systems Manager Deployment: Profiles & Tags

Once a deployment model — be it personal, institutional, or layered — is chosen, most large-scale deployments need to apply different settings, apps, or data to specific groups of devices. Common examples include grouping for separate student and instructor devices, grouping by specific educational course, and grouping by grade level.

Systems Manager makes it easy to create groups of devices that can receive different policies controlling settings, app management, security restrictions, and device settings. Simply create configuration profiles and assign these to groups of devices based on device tags. Once groups have been created, adding hundreds or thousands of devices to the same group definition is as easy as tagging those devices. For instance, imagine an iPad deployment needing three groups to segment devices: two separate grade level groups for student devices and one group for faculty devices. In Systems Manager, all you need to do is create three tags — for example "5th-grade," "6thgrade," and "instructors." Next, associate these tags with specific profiles that can be created in the Mobile > Profiles page in Systems Manager. Any profile-specific policies would now apply to the tagged devices. For example, perhaps a profile created for students would include the the 6th-grade and 5th-grade tags, applying those profile settings to the student devices.

Instructor Profile WiFi settings, security restrictions



Instructor iPads Teaching apps

Student Profile WiFi settings, security restrictions





13 Reclaiming apps — Institutional & Layered Model Only

Apps purchased via Apple VPP codes can be removed from one device and assigned to another device; however, this can only be done on devices supervised with the Apple Configurator utility.

There are two options when it comes to removing paid apps and reassigning them to another device.

- Use Apple Configurator to remove an app from a supervised device; this allows the redemption code to be used by any iOS device configured using the same Mac computer running Apple Configurator. The redemption code is only available to this particular computer — not any other also running Apple Configurator.
- Use Apple Configurator to un-supervise the device; all apps are removed and the redemption codes used will become available for reassignment on any device.

14 Real-Time Monitoring

Beyond mobile device management and app delivery, Systems Manager also provides real-time monitoring and troubleshooting capabilities.

Schools can collect real-time statistics and data on installed apps, perform inventory and asset management for hardware and installed software, and use integrated Live Tools to remotely troubleshoot the devices and perform operations such as clearing passcodes or locking/erasing a device.

Troubleshooting capabilities give a real-time view of what specific restrictions and settings are applied on a particular device. A list of pending updates for a device, together with an event and activity log provide deep visibility required to effectively troubleshoot an iOS device environment.

15 Administering a Systems Manager Network

The Meraki Dashboard provides an organizational hierarchy that allows for different administrative rights and grouping of managed devices. Within a school district or organization, multiple Systems Manager networks can be created with different administrators managing and with visibility to only their specifically assigned network.

You can create additional Systems Manager networks under the organizational overview page.

Administrators of a Systems Manager network can also be granted one of two permissions; read/write or administrator privileges. Adding new administrators and permission changes can be made under the Organization -> Settings page.

meraki	Network: East Schools	\$	Tag: All	4
Monitor	Very Large School District networks >	No n	ew clients this	week
Overview	East Schools			
Clients	3 clients active in the last week.			
Remote desktop	Questions? Check out the FAQ.			
Security	Try the <u>SM iOS app</u> , now in beta!			
Software				

Name	Very Large School District				
Administration					
Organization admins	User		Account status	Privileges	Actions
These users have administrator access to all of your networks in Dashboard.	Lisa Brown (lisa.brown@bigschools.net)		Active	Full	
	Bob Admin (bob.admin@bigschools.net)		Active	Full \$	Log out
You can add per-network administrators on the "Network-	Jack Theit (jackit@bigschools.net)		Active	Read-only \$	Log out
wide settings" page under the Configure tab.	Add an existing user	or	Create new user		

16 Meraki Networking Portfolio

Systems Manager complements Meraki's networking product portfolio and utilizes the Dashboard like all of our other products for end-to-end visibility and control.

MR Cloud-Managed Access Points

- Industry leading cloud-managed wireless access points that include functionality like L7 application visibility, traffic shaping, and stateful firewall.
- MR access points deployed alongside Systems Manager include automatic WiFi setting sync options that make wireless configuration management a breeze.



to mercat

meran

MX Cloud-Managed Security Appliances

- Cloud-managed security appliance that includes a next-generation firewall, Auto VPN, content filtering, IDS/IPS and WAN Optimization.
- MX security appliance provides content filtering for CIPA compliance, as well as client VPN settings sync for mobile devices enrolled in Systems Manager.

MS Cloud-Managed Switches

- Industry first cloud-managed access switch with L7 application visibility and virtual stacking.
- MS switch deployed alongside Systems Manager, like the MR or MX solutions, provides an integrated network view and client drill-downs from the Meraki dashboard.

17 Conclusion

Meraki's complete portfolio of cloud-managed products, including Systems Manager, are ideal for school environments, businesses, and organizations where mobile devices and applications are the new norm, and where network deployments with management simplicity and ease of use are key requirements.

With support for iOS, Android, Mac OS, and Windows devices, Meraki Systems Manager provides an intuitive, easy to use device management solution with little to no training required. Systems Manager is available to use 100% free of charge on any network. Meraki provides complimentary phone support for Meraki networking customers and free email support for all other users.

Try out Systems Manager Today. It's 100% Free.

References

Meraki Security & Cloud Architecture http://www.meraki.com/trust/

Meraki Systems Manager Sign Up http://www.meraki.com/form/systems-manager-signup

Meraki Systems Manager How to Videos http://www.meraki.com/blog/2012/08/how-to-get-the-most-from-meraki-systems-manager/

Meraki Systems Manager User Guide http://docs.meraki.com/sm

Meraki Systems Manager Datasheet http://meraki.com/lib/pdf/meraki_datasheet_sm.pdf

Apple iOS 6 Education Deployment Guide http://images.Apple.com/education/docs/ios_6_education_deployment_guide.pdf

Apple Volume Purchase Program Redemption Codes http://support.Apple.com/kb/HT5188?viewlocale=en_US&locale=en_US

iOS Apple Configurator http://images.Apple.com/au/iphone/business/docs/iOS_Apple_Configurator_Mar12.pdf

Systems Manager FAQ http://docs.meraki.com/display/SM/Systems+Manager+FAQ