

# iOS 5 in the Enterprise

A hands-on guide to managing iPhones and iPads



John Welch

# iOS 5 in the Enterprise

A hands-on guide to managing iPhones and iPads

**John Welch**



## **iOS 5 in the Enterprise: A hands-on guide to managing iPhones and iPads**

John Welch

### **Peachpit Press**

1249 Eighth Street  
Berkeley, CA 94710  
510/524-2178  
510/524-2221 (fax)

Find us on the Web at: [www.peachpit.com](http://www.peachpit.com)

To report errors, please send a note to [errata@peachpit.com](mailto:errata@peachpit.com)

Peachpit Press is a division of Pearson Education

Copyright © 2012 by John Welch

**Editor:** Nancy Peterson

**Production editor:** Myrna Vladic

**Development editors:** Bob Lindstrom and Robyn Thomas

**Copyeditor:** Darren Meiss

**Cover design:** Aren Howell Straiger

**Cover production:** Jaime Brenner

**Interior design:** Mimi Heft

**Compositor:** David Van Ness

**Indexer:** Joy Dean Lee

### **Notice of Rights**

All rights reserved. No part of this book may be reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher. For information on getting permission for reprints and excerpts, contact [permissions@peachpit.com](mailto:permissions@peachpit.com).

### **Notice of Liability**

The information in this book is distributed on an “As Is” basis, without warranty. While every precaution has been taken in the preparation of the book, neither the author nor Peachpit Press shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the computer software and hardware products described in it.

### **Trademarks**

iOS, iPhone, iPad, and iTunes are trademarks of Apple, Inc., registered in the United States and other countries. Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and Peachpit Press was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified throughout this book are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this book.

ISBN 13: 978-0-321-81199-8

ISBN 10: 0-321-81199-2

9 8 7 6 5 4 3 2 1

Printed and bound in the United States of America

*This book, like everything I do, is dedicated to the family I live with:  
my amazing, beautiful, talented wife Melissa, and my son Alex,  
who is about to go into the world as a grownup.*

*It's also dedicated to the family I don't live with who keep me sane:  
Mom, Dad, Gypsy, Nicci, Mo, Brad, Kelly, Mark, Virginia, Jenny,  
Michelle, Rachel, Ernie, Sami, Sly . . . you guys are all amazing,  
and I'm lucky to know any one of you, much less all of you.*

## ACKNOWLEDGEMENTS

---

The very concept that I did this even slightly alone is ridiculous. There are quite a few people without whom this book would not have happened, and I would be far, far crazier than I am:

To the best editing team ever, Nancy Peterson and Bob Lindstrom, who kept me focused, working and regularly laughing. (Seriously, Bob has some of the funniest editorial comments ever and they make a rather tedious task a lot more fun.) Nancy had the unenviable job of chief whip-cracker to someone who is really good at procrastination and she did it perfectly. Whatever shreds of a schedule we managed to keep were all due to her fantastical fanatical work. I am also deeply appreciative that they, (and Peachpit) not only allowed, but encouraged me to keep my “voice” throughout the book.

The Apple iOS team, without whom I’d have nothing to write about.

Sal and the AppleScript team, because any chance I have to thank one of the best groups at Apple, or anywhere, I will.

The folks at the/zimmerman/agency, in particular my boss, Mike, along with Curtis & Carrie: you’ve created the environment that let me experiment and learn how to do things with iOS that gave me the ability to write this book based on the real world experiences I’ve gained with Z. Thank you all for that and for not letting the agency become just another place to work. Everyone at Z, you guys are the best.

Zach, Chip, Lance, and all the folks at JAMF software who answered questions and provided extensions to demo keys and were absolutely invaluable as a resource, you guys have earned every dime you’ve made or ever shall make.

Jessica, the most awesome, wonderful, amazing former editor ever, who gave me my start in getting paid to write . . . see what you started? Oh, and I have a lovely yard full of love bugs should you ever visit :-P

---

Kathy Moran, Paul Kent, Ron Moreau, Arek, Kevin, Ben, and all the other folks who work their keisters off to put Macworld Expo and MacIT together—thanks for letting me play too; you’re all wonderful.

My brothers in arms, Peter and Darby . . . guys, WHAT is going on, and how much fun is this? Every Tuesday for over two years, I get some of my sanity back.

Jason, Phil, Chris, the Dans, and all the folks at Macworld: I know how much of a pain my name on the site can be for you. But thank you for putting it there anyway. It’s still awesome every time I see it.

Dave Hamilton, ChuckL, JeffG, Dori, Tom, and all the other Expo peeps . . . every year I get a big funky reunion with my favorite people. Y’all are why I still get excited about expo.

The Group which must not be named shall nonetheless be thanked. Thank you to all the people on the Internet and elsewhere who have gone through the pain of learning how to manage iOS stuff and took the time to share their experiences. It’s folks like you that make the Internet worthwhile, far more than any NMD collective ever will.

Finally, to the baddest, funniest, coolest group of ladies I know: The Tallahassee RollerGirls. Derby. Rocks.

This book took, one way or another, my entire life to write and this is a TINY fraction of those who helped.

*This page intentionally left blank*

# CONTENTS

Acknowledgements .....	iv
Introduction .....	xiii
Welcome to iOS 5 in the Enterprise .....	xvi

## PART I iTunes and iPhone Configuration Utility

<b>CHAPTER 1</b>	<b>WHEN iTunes IS ENOUGH .....</b>	<b>2</b>
	Limitations of iTunes .....	4
	Managing with iTunes .....	5
	Using Device Settings .....	11
	Wrapping Up .....	12
<b>CHAPTER 2</b>	<b>THE iPhone CONFIGURATION UTILITY .....</b>	<b>14</b>
	OS X 10.7 Server Profile Manager and iPCU .....	16
	Getting the iPCU .....	16
	Understanding iPhone Configuration Utility Basics .....	17
	<i>Viewing Devices</i> .....	17
	<i>Using Applications and Provisioning Profiles</i> .....	18
	<i>Setting Up Configuration Profiles</i> .....	19
	<i>Applying Profiles with a Connected Device</i> .....	19
	Wrapping Up .....	19
<b>CHAPTER 3</b>	<b>APPS AND PROVISIONING .....</b>	<b>20</b>
	Using Provisioning Profiles .....	22
	<i>Understanding the Provisioning Portal</i> .....	22
	<i>Learning More About Profiles and Devices</i> .....	23
	Performing	
	Larger Scale Distribution .....	24
	<i>Uploading Multiple Devices</i> .....	24
	<i>Applying Distribution Profiles</i> .....	26
	Using Applications .....	27
	<i>Installing and Uninstalling Apps and Profiles</i> .....	27
	Wrapping Up .....	29



<b>CHAPTER 4</b>	<b>CREATING CONFIGURATION PROFILES</b>	<b>30</b>
	Using General Settings	32
	Setting a Passcode	35
	Choosing Restrictions	36
	Configuring Wi-Fi	37
	Setting Up VPN	38
	Setting Up Email	39
	Using Exchange ActiveSync	41
	Enabling LDAP	43
	Setting the Date with CalDAV	46
	Getting in Touch with CardDAV	47
	Keeping up with Subscribed Calendars	48
	Using Web Clips	49
	Setting Credentials	50
	About SCEP	50
	Using Mobile Device Management	51
	Managing Advanced Settings	51
	Wrapping Up	51
<b>CHAPTER 5</b>	<b>UNDERSTANDING CONFIGURATION PROFILE STRUCTURE</b>	<b>52</b>
	Starting with the Basics	54
	Editing Individual Payload Sections	57
	Why Do I Care?	61
	What about OS X Server 10.7?	61
	Changes in iOS 5	62
	Signing and Encrypting Profiles	63
	Wrapping Up	63
<b>CHAPTER 6</b>	<b>SCRIPTING THE IPHONE CONFIGURATION UTILITY</b>	<b>64</b>
	Learning AppleScript Basics	66
	<i>The AppleScript Language</i>	66
	<i>The Dictionary</i>	67
	<i>Scripting the iPhone Configuration Utility</i>	67
	Wrapping Up	78

	<b>PART II OVER-THE-AIR SETUP</b>	
<b>CHAPTER 7</b>	<b>ADDING PROFILES TO DEVICES</b>	<b>80</b>
	Using a Tethered Profile Installation	82
	Installing with Email	84
	<i>Using the iPhone Configuration Utility</i>	84
	<i>Using OS X Server 10.7</i>	84
	Wrapping Up	87
<b>CHAPTER 8</b>	<b>USING SIMPLE OVER-THE-AIR PROFILE DISTRIBUTION</b>	<b>88</b>
	Start with a Web Server	90
	<i>Using Amazon's S3 Service</i>	91
	Setting Up the OTA Web Server	92
	Using the OTA System	94
	Distributing Applications OTA	96
	Wrapping Up	97
<b>CHAPTER 9</b>	<b>SCEP: A BACKGROUND</b>	<b>98</b>
	Enter SCEP	100
	Configuring iOS Devices via SCEP	102
	<i>Authentication</i>	102
	<i>Certificate Enrollment</i>	103
	<i>Device Configuration and Encrypted Profiles</i>	107
	Wrapping Up	108
<b>CHAPTER 10</b>	<b>IMPLEMENTING SCEP ON OS X SERVER</b>	<b>110</b>
	Setting up SCEP on OS X Server	112
	<i>Implementing SCEP on OS X 10.6 Server</i>	112
	<i>Setting up SCEP with Casper</i>	114
	Implementing SCEP on OS X Server 10.7	119
	<i>Setting up Profile Manager</i>	124
	Wrapping Up	125

<b>CHAPTER 11</b>	<b>IMPLEMENTING SCEP ON WINDOWS SERVER 2008</b>	<b>126</b>
	Configuring the Server	128
	<i>Setting Up the Roles</i>	128
	Installing Absolute Manage	131
	Wrapping Up	134
<b>CHAPTER 12</b>	<b>IMPLEMENTING SCEP ON A CISCO DEVICE</b>	<b>136</b>
	Taking the Initial Steps	139
	The AnyConnect SCEP Settings	140
	Configuring the ASA	142
	Testing It All	143
	Wrapping Up	143

---

## PART III MOBILE DEVICE MANAGEMENT

<b>CHAPTER 13</b>	<b>PERFORMING MOBILE DEVICE MANAGEMENT</b>	<b>146</b>
	The Problem with Configuration Profiles	148
	Grokking the Mobile Device Management Concept	149
	Wrapping Up	153
<b>CHAPTER 14</b>	<b>MOBILE DEVICE MANAGEMENT FEATURES</b>	<b>154</b>
	Flexibility and Power	156
	Managing Passcodes	157
	<i>Setting Passcodes</i>	157
	Managing CardDAV Settings	164
	<i>Installing the CardDAV Profile</i>	164
	<i>Removing the CardDAV Profile</i>	165
	Gathering Device Inventory/Information	166
	Wrapping Up	166

<b>CHAPTER 15</b>	<b>SETTING UP A MOBILE DEVICE MANAGEMENT SERVER</b>	<b>168</b>
	Do You Really Need to Run Your Own Server?	170
	How Big Should Your Server Be?	171
	Firewall Planning	172
	Getting a Push Notification Certificate	173
	Using OS X Server 10.7	175
	Installing Casper on OS X 10.6 Server	176
	Configuring Casper for Mobile Device Management	180
	<i>Configuring LDAP</i>	180
	<i>Configuring Email Settings</i>	182
	<i>Uploading the Push Notification Certificate</i>	183
	<i>Setting Up the SCEP Server</i>	184
	<i>Setting Up the Initial Enrollment Profile</i>	186
	Wrapping Up	187
<b>CHAPTER 16</b>	<b>LIMITATIONS OF MOBILE DEVICE MANAGEMENT</b>	<b>188</b>
	Understanding Infrastructure Complexity	190
	Locking Mobile Device Management Profiles	192
	Wrapping Up	193

## PART IV BASIC WIRELESS APPLICATION DISTRIBUTION

<b>CHAPTER 17</b>	<b>BASIC WIRELESS APPLICATION DISTRIBUTION BACKGROUND AND SETUP</b>	<b>196</b>
	Background and Requirements for Wireless App Distribution	198
	App Distribution Server Requirements	200
	Preparing the App	201
	Accessing the App Distribution Web Page	205
	Installing the App	206
	Wrapping Up	206

<b>CHAPTER 18</b>	<b>WIRELESS DISTRIBUTION USING MOBILE DEVICE MANAGEMENT</b>	<b>208</b>
	App Installation and Management, Casper-Style	210
	<i>Performing the Initial Setup</i>	210
	<i>Installing the App</i>	212
	<i>Updating an App</i>	214
	<i>Deleting an App</i>	214
	<i>Managing App Store Apps</i>	216
	App Installation and Management, OS X Server 10.7-Style	219
	<i>Performing the Initial Setup</i>	219
	<i>Distributing Enterprise Apps via OS X Server 10.7</i>	219
	<i>Distributing App Store Apps via OS X Server 10.7</i>	220
	Wrapping Up	221
<b>CHAPTER 19</b>	<b>ISSUES WITH WIRELESS APP DISTRIBUTION</b>	<b>222</b>
	Considering Infrastructure	224
	Adding Issues for Developers	225
	Addressing App Management	226
	Wrapping Up	227
	Index	228

## INTRODUCTION

Those of you who have to deal with more than a handful of iPhones, iPads, or iPod Touches already know why you manage iOS devices. For everyone else, “manage” is not a short way to say “impose draconian control.” Managing devices on your network, including iOS devices, not only makes your life easier, but should also make life easier for your users.

That’s my core philosophy with regard to device management. In the end, device management *has* to make life easier for the user.

A happy side benefit to this is that when done right, it makes *your* life easier, too. When a user can personally take an iPhone from activation to full network integration in two to three steps and about five minutes, it frees you and that user to actually *do stuff with the gear*.

### WHY MANAGE iOS DEVICES?

I think we should all be clear on what is meant by that phrase because this book is pretty much built around it. While “managing iOS devices” can suggest all sorts of draconian imagery, the reality is a bit more mundane.

When you run a business or an IT department, you have to care about your company’s “stuff.” If you have a small number of people, it’s pretty easy to adopt a “live and let live” policy, so your management tasks may start and end with “Here’s the address for the email server we use. Have a nice day.”

But as your company grows, or if you have data that you need to control securely, then you need ensure that your data is set up and managed in a consistent, sane manner. Consider a small doctor’s office. Even with just two or three employees, that office has to take data security *very* seriously or many, many regulatory and legal entities may come down on it like a ton of bricks.

So that’s what management is about. You’re ensuring that your iOS devices are set up in a way that is consistent and sane for your needs, whatever those needs may be. Some of you may never need to care about disabling cameras, for example, while others may need to lock down those snapshot lenses as tightly as possible. That’s what this book is about: Helping you meet your iOS device needs whatever they may be.

---

## WHO NEEDS THIS BOOK?

The short answer is “anyone who wants to better manage their iOS devices.”

(By the way, throughout the book, I’ll use “iOS devices” to refer to the entire family of Apple products that run on iOS. If I’m talking about a specific product, such as an iPad, then I’ll do so. Trust me, referring to “iOS devices” beats the pants off of “iPhone, iPad, and/or iPod Touch.” It’s also gobs easier to type.)

The longer answer is about the same as the short answer with more details. No one profile perfectly covers everyone using iOS devices. *Everyone* is learning how to deal with Apple’s portable devices, from five- or ten-person SOHO shops to Big Enterprise. This book is simply a collection of information to help you out, regardless of your level of iOS usage.

## WHAT THIS BOOK IS

This book is, as true as I can make it, a reference source. It is designed to be of use to people across their ranges of need—from someone who just wants a guide to use iTunes and a USB cable to someone who needs to set up SCEP and MDM and talk to their back-end directory servers.

As much as is practically possible, this book tries to help all of you. I hope it does so in a way that will be of use past the current version of the iOS (which is v5.x at the time of this writing). That means I’m going to cover a lot of principles; the general application of said principles; and use specific, focused examples to illustrate an application when it makes sense, or when I’ve found an app that’s particularly neat or cool. (Yes, neat/cool counts in IT. You’d be amazed.)

---

## WHAT THIS BOOK IS NOT

If you're looking for a cookbook of how-tos, I will tell you now, this is not the book for you. While such books have their place, I think that place is the Internet, where information updates can be done more quickly. I'm not just being smarmy here. Some of the words you're reading were written six or more months ago. As a result, any how-to or step-by-step example included here will be similarly old. (What, you think editing my verbosity happens in a fortnight?) Do you really want to use a step-by-step setup that may be older than the iOS version you're trying to use it on? No.

In a sense, overly detailed step-by-step how-to books are handing you a fish. Instead, I want to teach you how to fish. This book is here to help you learn about what's going on with iOS devices and how they work with regard to iOS management, so you can develop the exact way *you* wish to implement that management in *your* environment in a way that works for *you*.

## THANKS

Outside of the specific thank-yous that are in the various prefaces to this book, I want to give some thanks specifically to Apple, for the iOS, the devices, and the management APIs; Cisco, for SCEP; Microsoft, for giving Windows Server 2008 the ability to act as a SCEP server even though I doubt that iOS was the reason; JAMF, for giving people yet another reason to buy Casper (it really is an amazing product); and a host of people on the Internet who have contributed knowledge and help on this subject, in general and directly to me, because they felt that adding to the knowledge base is The Right Thing To Do. When I can nail the information down to one source, I'll make sure you get credit. This book is as much yours as mine.



## WELCOME TO iOS 5 IN THE ENTERPRISE

iOS is, of course, the operating system for Apple's iPad, iPhone, and iPod Touch. If you haven't heard of those devices, well, I'm not sure how you would not have heard of those and still be interested in this book. Anyway, iOS and the devices that run it are really awesome and cool; but when you have to manage all of them, some

### THE TOOLS

You'll need to be familiar with a small set of tools and concepts to get the most out of this book and managing your iOS devices.



#### iTunes

iTunes is one of Apple's two primary tools for managing iOS devices. In the consumer space, it is *the* primary tool, and every iOS device running iOS 4.x has to connect to iTunes via USB at least once. iTunes is a free download from Apple and runs on Windows or OS X.



#### iPhone Configuration Utility

The iPhone Configuration Utility (iPCU) is the other primary Apple-provided tool for managing iOS devices. It is designed for administrators who need to manage their devices beyond the capabilities of iTunes and the on-device options. The iPCU is a free download from Apple and runs on OS X or Windows.



#### AppleScript

The book talks about using AppleScript to automate tasks involving the iPCU and various XML-based configuration files. AppleScript is Apple's own scripting language that uses vaguely quasi-English syntax. It is included with OS X.

of that awesomeness may decrease. Fear not! This book is here to re-awesome-ize those devices, and help make you seem awesome as well. To help you in your awesome journey to Ultimate iOS Awesomeness, here are a few tidbits you'll want to know about upfront.

---



#### XCODE

Even if you aren't an iOS developer, if you plan to distribute in-house or "enterprise" apps, Xcode will be a necessary part of the process. Xcode is Apple's primary development environment and is included free on every new Mac and is also available from the Mac App Store for around \$5 U.S.



#### A WEB SERVER

When we start talking about managing iOS devices on a large scale, or wirelessly, you'll need a web server. The platform and brand really don't matter. In fact, you don't even have to own the web server yourself. But, you will need one.



#### OS X SERVER 10.7

With OS X Server 10.7, Lion, Apple finally added the tools needed to properly manage iOS devices via Apple operating systems. Even better (for me), they released Lion right as I was finishing the first edition of this book. Since a lot of people won't immediately update to 10.7, you'll be getting kind of a split worldview. Information on OS X Server 10.7 will appear next to info on 10.6.



#### iOS 5

iOS 5 adds a huge number of features for the person using the phone, but the changes from a management perspective are, thankfully, minor and mostly relate to app distribution. If there are sections of the book affected by major iOS 5-specific changes, those changes will appear alongside the iOS 4 info. If the changes are only cosmetic, then they won't. (If the function of the button changes, I'll note that. If the shape of the button changes—not so much.)

*This page intentionally left blank*

---

# 4

## CREATING **CONFIGURATION PROFILES**

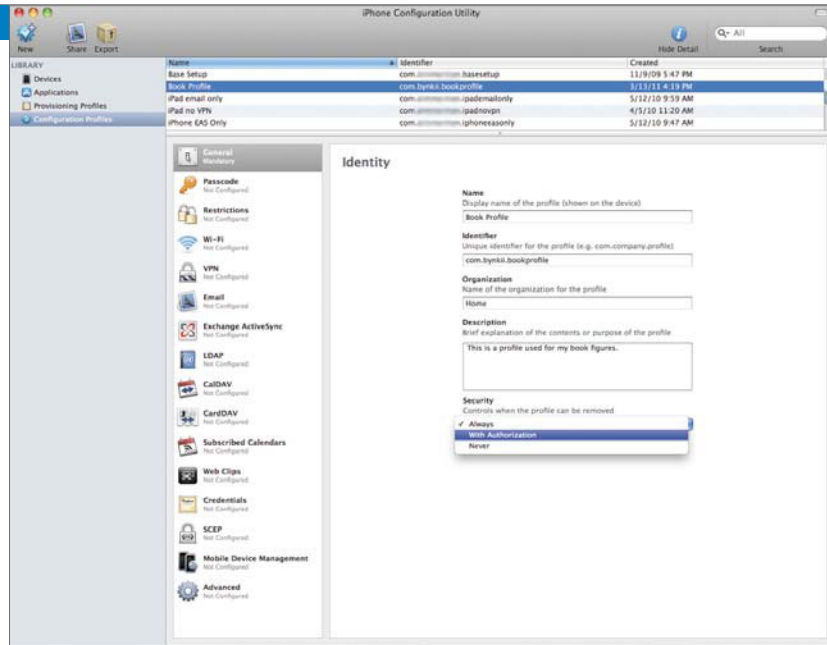
This is the “big” chapter for the iPhone Configuration Utility (iPCU), and for anyone who needs to perform extensive/advanced management of iOS devices. Configuration profiles are XML files that control the behavior of your iOS devices, restrict or allow specific features, and set up functions such as email and calendars. Once created, configuration profiles can be distributed via USB, email, or a web page.

You can also encrypt and sign a profile to restrict the devices it can be applied to, and password-protect it so that it cannot be removed short of wiping all the data on the device. Configuration profiles can be long and complicated, or kept simple and used only to point a device at a Mobile Device Management server that can push the desired settings to the devices.



## USING GENERAL SETTINGS

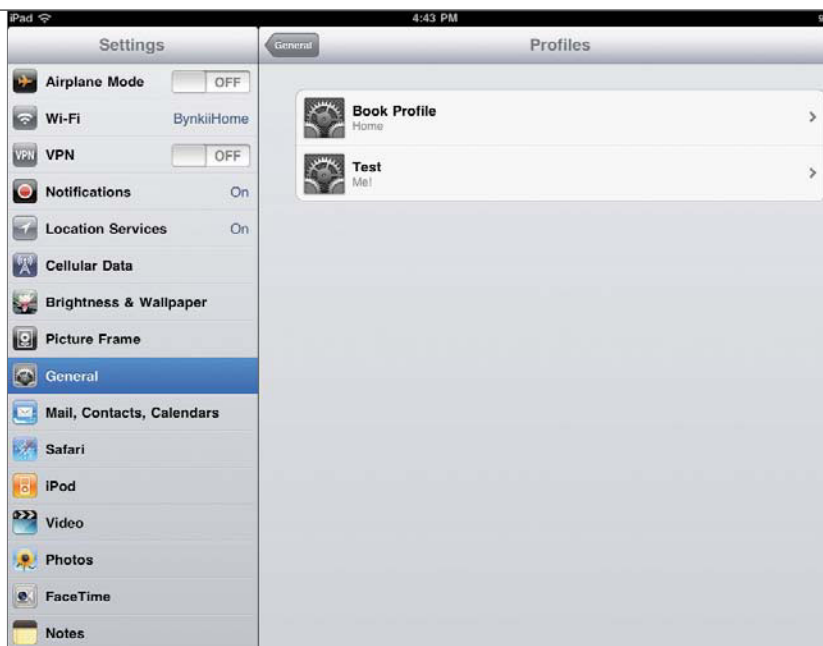
**FIGURE 4.1** General settings for identity security



When you're creating a configuration profile, the iPCU might have you thinking that the General settings are the only mandatory settings. That's not exactly correct. You need General plus at least one additional setting. This is logical because it doesn't make sense to have a configuration that has only the General section because the General section doesn't really *do* anything in terms of configuring your iOS device. It's just there to identify the profile.

But, if you aren't expecting that behavior, and you're testing a profile, it could be annoying when the device refuses to install a profile with only the General settings configured.

The General settings are concerned only with the profile identity security (Figure 4.1). As such, the number of settings here is pretty small. You can set the name of the profile, which is what users see when they go into the General settings on the device and select Profiles (Figure 4.2). That's not a misprint by the way; you can have multiple profiles on a single device. If you choose to have multiple profiles, however, please watch your settings. Choosing conflicting settings would be . . . bad.

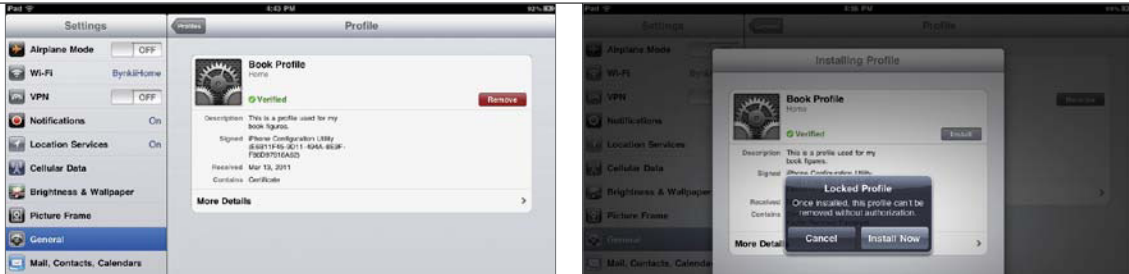


**FIGURE 4.2** General settings on an iOS device

Most of the settings here are descriptive, starting with a Name for the profile that the user will see on the device and a unique Identifier named similarly to plist files—for example, “com.bynkii.bookprofile”—that serves two important purposes: First, if no other profile on a device has that same identifier, the profile’s settings are added to the device. Second, if a profile on the device does have the same identifier, the settings in the new profile replace the previous profile’s settings.

This functionality can make it easy to update an existing profile. Rather than performing a full remove and replace, you can just edit an existing profile while retaining the same identifier, and re-install the profile on the device. The exception is when changing Exchange accounts. When changing an Exchange account, you must remove the profile with the Exchange info so that the Exchange data can be purged.

The Organization and Description fields are available for you to insert customized information that—like the Name field contents—are displayed on the device.



**FIGURE 4.3** (left) Click Remove to delete a profile from a device.

**FIGURE 4.4** (right) Warning displayed when installing an app that requires authorization

The Security setting controls the ability to remove the profile and has three settings: Always, With Authorization, and Never. Always is pretty self-explanatory: The profile can always be removed by clicking Remove in the profile's information section (**Figure 4.3**).

If you choose With Authorization, the profile can be removed only by entering a passcode that you set when you create the profile in the iPCU. You'll see a warning to that effect when you install a profile with this security setting (**Figure 4.4**).

If you choose the final option, Never, you're required to erase all the data from the device to remove the profile.

Realistically, don't choose Never unless you are in a high-security environment (and I mean "Lawrence Livermore National Laboratory where we perform nuclear weapons research," not just "I don't want people to know about our new website data" security); or unless you are not going to update that profile anytime soon. Choosing Never usually causes far more problems than it solves. Choosing With Authorization will cover you 99 percent of the time. If the device is a personal device that someone is using for work purposes, consider choosing Always, because it's kind of rude to lock someone out of her own phone.

## LION AND THE iPCU

If you're wondering how OS X Server 10.7 changes the iPhone Configuration Utility, the truth is, it doesn't. The iPCU still works the same way in OS X Server 10.7 and OS X 10.7 as it did in OS X Server 10.6 and OS X 10.6. OS X Server 10.7 does introduce some significant changes to managing iOS devices, but those primarily involve SCEP, Mobile Device Management, and Over The Air (OTA) management, and will be covered in detail in those chapters.



## SETTING A PASSCODE



**FIGURE 4.5** Passcode settings in iPCU

Next are the Passcode settings (**Figure 4.5**). These settings are simple enough, but you have a *lot* more granularity than you can access using only the device or iTunes.

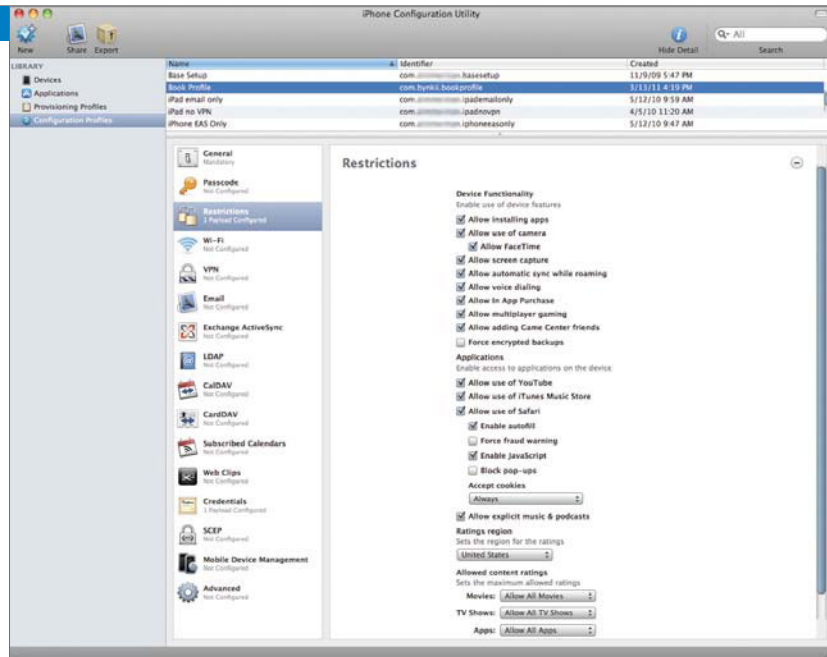
For example, if you don't want people to choose a passcode like "7777", simply deselect "Allow simple value." If you want to force the use of letters and numbers in a passcode, select "Require alphanumeric value." You can set the "Minimum passcode length" from 1 to 16 characters, set the "Minimum number of complex characters" (such as &, \$, or !) from 1 to 16, and choose "Maximum passcode age" up to 730 days. You can also restrict the number of unique passcodes that must be used before a passcode can be repeated, along with a few other passcode settings.

Really, none of the settings available differ much from password settings of any standard IT setup, save one: "Maximum number of failed attempts." This setting can be dangerous, because it lets you limit the number of times an incorrect passcode can be entered *before the device erases itself* (up to a maximum of 16 tries.) Yes, this restriction can be useful if your iOS devices carry critical confidential data; but, if this value is set too low, you can create a large user support headache for yourself.

This setting falls into a category I like to call "If you have to ask, the answer is No!" so, if you are currently asking yourself, "Should I use this?", then don't use it. If you actually need to use this setting, you'll know and you won't have to ask. Any setting that can cause a device to erase itself should be implemented with the greatest care and caution.

## CHOOSING RESTRICTIONS

**FIGURE 4.6** Restrictions settings



Restrictions is the most complex group of settings and the worst named. Restrictions. Really? This is the best Apple could come up with? Anyway, these settings enable and disable most of the basic hardware functionality on the device (**Figure 4.6**).

I'm not going to detail every one of these settings, as there's a ton of them and they're all pretty self-explanatory. However, a few are worth noting. For example, if you want to avoid the *hideous* roaming charges that both AT&T and Verizon love so well (in the U.S. at least), deselect "Allow automatic sync while roaming." A user can still check her communications automatically, and a device that's not being actively used won't rack up a few thousand dollars of data charges because that user gets a lot of email.

Selecting "Force encrypted backups" just makes sense, and causes almost no noticeable problems on the user's end. You may also want to deselect "Allow explicit music & podcasts" if the device is mostly used in a corporate setting. "Allow use of iTunes Music Store" applies only to the device. It's not going to stop people from using iTunes on their Mac or Windows computers.

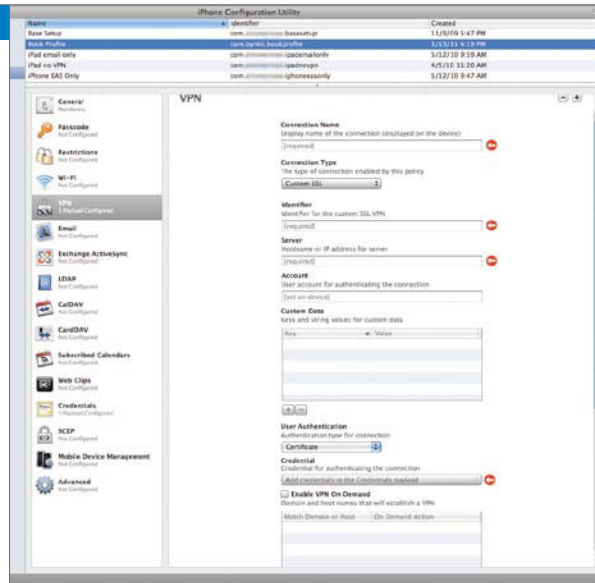
## CONFIGURING WI-FI

The Wi-Fi settings are short and to the point. You specify the SSID of the network, whether or not it's hidden, its security type, and the password (for personal networks). If you specify Enterprise in the “Security Type” pop-up menu, you reveal many more options, such as several Extensible Authentication Protocol (EAP) types; Authentication information; and Trust, which contains the certificates used to validate the authentication server for the network.

Notice that you can set up multiple networks here. So, if a user must travel between facilities—each with its own Wi-Fi network setup—you can populate his iOS device with the information for each network ahead of time, so his device just works. This also saves you from handing everyone the password to the wireless network, which is not only a good idea, but sometimes a regulatory requirement.

## SETTING UP VPN

**FIGURE 4.7** VPN settings are easy to configure incorrectly.



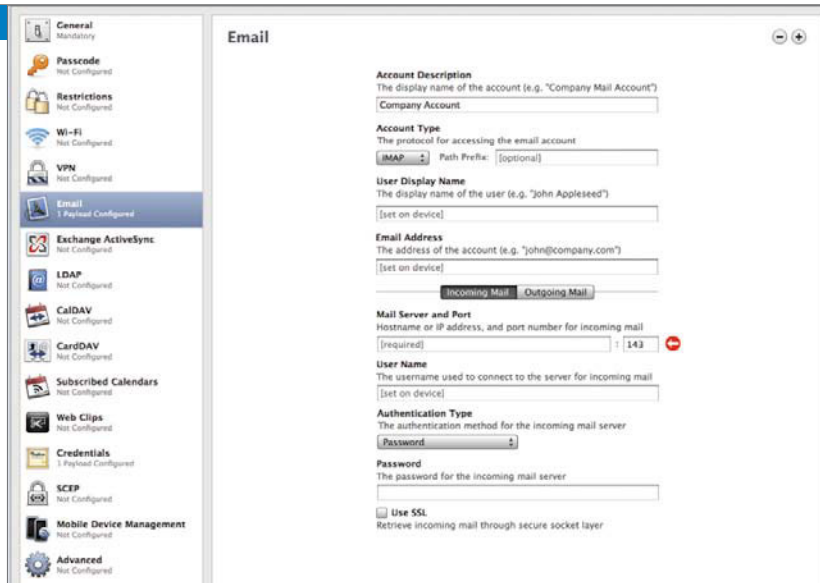
The VPN settings are the opposite of the Wi-Fi settings: They are not to the point, not terribly clear, and painfully easy to incorrectly configure so that your VPN will never work (**Figure 4.7**).

In addition, some of the VPN types listed in the iPCU—such as F5 SSL, Cisco AnyConnect, and Juniper SSL—require you to first install the appropriate apps from the Apple App Store. Not fun.

I'm not trying to downplay the importance of VPN or to avoid it; but there are six specified VPN connection types along with a “Custom SSL” setting, and at least 108 separate VPN settings; and, as with the Wi-Fi settings, you can configure *multiple* VPNs setups here. Furthermore, if you are dealing with “VPN on Demand” and some of the custom options, you'll be looking at *even more* settings.

Fully explaining all of that is literally a book unto itself and, in fact, many VPN books have been written. VPNs are still overly complex as the VPN settings show. If you are responsible for maintaining your VPN, I don't need to tell you what settings to use. If you are not the person maintaining your VPN, schedule some time to sit down with your VPN guru, the iPCU, and an iOS device to work out the best settings for your devices. Then use them. Take copious notes—you'll be glad you did.

## SETTING UP EMAIL



**FIGURE 4.8** POP/IMAP email account settings

These settings configure POP/IMAP email accounts for your devices (**Figure 4.8**).

One thing right away: Don't use POP. If someone is checking her email with an iOS device, it is fairly certain that it isn't the only way she checks email. You really, really want to use IMAP here. Yes, I know, POP has that "leave it on the server" option. That's nice but it's not IMAP, which is designed from the ground up to be used by multiple devices checking the same account. If you were entering the 24 hours of Le Mans, would you drive an Audi R15 TDI, or a '78 Pinto with a big spoiler and glasspacks? Right. Use IMAP.

By the same token, also use SSL. If you haven't enabled this on your server, now is a great time to do so. Open wireless networks are a gold mine for people doing illicit data mining, and SSL is an easily-implemented method to prevent them from mining you. So, use SSL. The only other thing I'd specifically recommend is using authenticated SMTP. It's a cheap way to stop unauthorized people from using your SMTP server, and iOS supports it.

As far as the other settings go, email settings are email settings are email settings. However, you will want to leave some settings blank for the user to fill in: the User Display Name, the User Name, and the Password. If you fill those out, you'll have to create a custom profile for everyone, or change the settings every time you install them on a device. You don't want to do that, do you? Of course not.

---

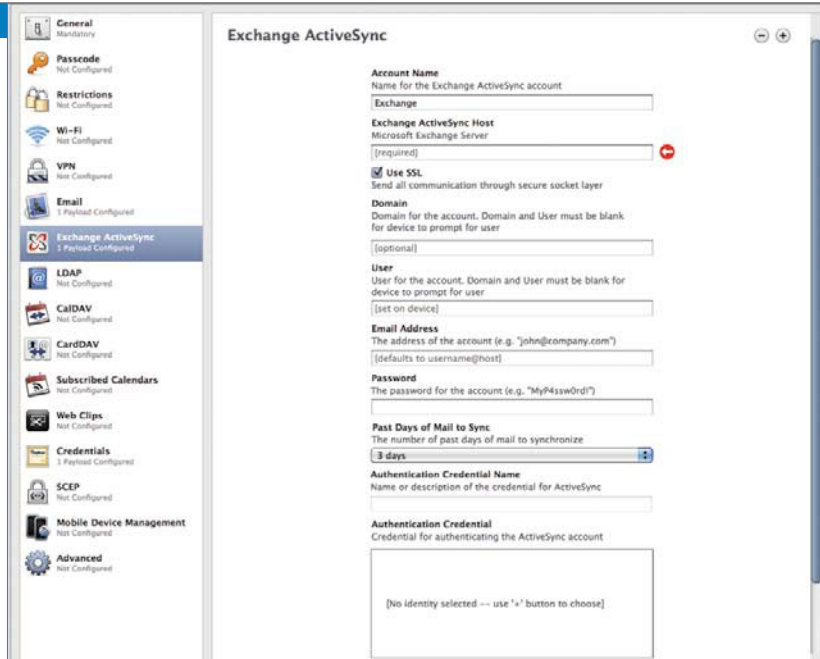
However, the downside of letting users enter that information is if you install a profile via USB, the user has to enter that information during that installation. So, when you're installing profiles to set up email or any other option that requires user input, you won't want to do so over USB. Luckily, as you'll see, you have other ways to distribute these profiles.

The only setting I want to talk about specifically is Path Prefix, because it is a setting you'll use with a rather popular email provider, namely Gmail.

When you set up a Gmail account on an iOS device, you're really setting up an IMAP account—and Google has an “interesting” take on IMAP. If you use the “standard” IMAP settings for Gmail, you'll realize that you have duplicates of every folder in your Gmail account. That's because if you look at your account from the folder root, you'll see you have a [Gmail] tree with all your Gmail “folders” and possibly an [IMAP] tree as well. By setting the Path Prefix to [Gmail], you avoid some of that duplication.

Boy, that's kind of a pain, isn't it? Wouldn't it be nice if you had an easier way to deal with Gmail that set up Google Calendars and Contacts at the same time? Well, you do. You can use Exchange ActiveSync instead of Email for this. Your setup is not only simpler, but you get all your calendaring and contacts, too. (Unfortunately, you still have the same ugly folders issue because Google's Exchange ActiveSync implementation is as “interesting” as their IMAP implementation, but at least you do less work for it.)

## USING EXCHANGE ACTIVESYNC



**FIGURE 4.9** Exchange ActiveSync settings

Microsoft Exchange is, for better or worse, the 800-pound gorilla of corporate email; and its mobile protocol, Exchange ActiveSync (EAS), is the way you connect mobile devices to Exchange. However, a while ago, Microsoft did something quite brilliant with EAS: they decoupled it from Exchange. So, it still has the name, but you can use it with servers that have nothing to do with Exchange, such as servers from Google, Kerio, Zimbra, Atmail, and others.

Exchange ActiveSync, name aside, is a boon to iOS devices and the like because—rather than configuring your email server *and* your calendar server *and* your contact server separately—you just set up EAS and you’re done. Exchange ActiveSync also allows handy things for IT folk such as the remote wipe of a device without signing up each and every device for “Find my iPad/iPhone.” In Exchange ActiveSync settings (**Figure 4.9**), you configure Exchange ActiveSync accounts on your iOS devices.

As with email, you’ll find the “normal” fields here, such as Account Name, the server name, Use SSL (YES), and so on. A few fields, however, may appear a bit odd to the uninitiated. First of these is the Domain field. If you are on a Windows

---

network using an Exchange Server, the domain is usually your Windows domain. If you're using a server such as Gmail, or Kerio Connect (that is, something other than an actual Microsoft Exchange server), you can leave this field blank.

The other strange fields are the authentication credential fields. These are used with certificates that validate the *server* to the *client*. This may seem odd, but it is a good way to avoid accidental connection to a rogue Exchange server that happens to have the same DNS address as the desired server. As with email settings, leave the User, Email, and Password fields blank unless you specifically want to fill them in for each user.



## ENABLING LDAP

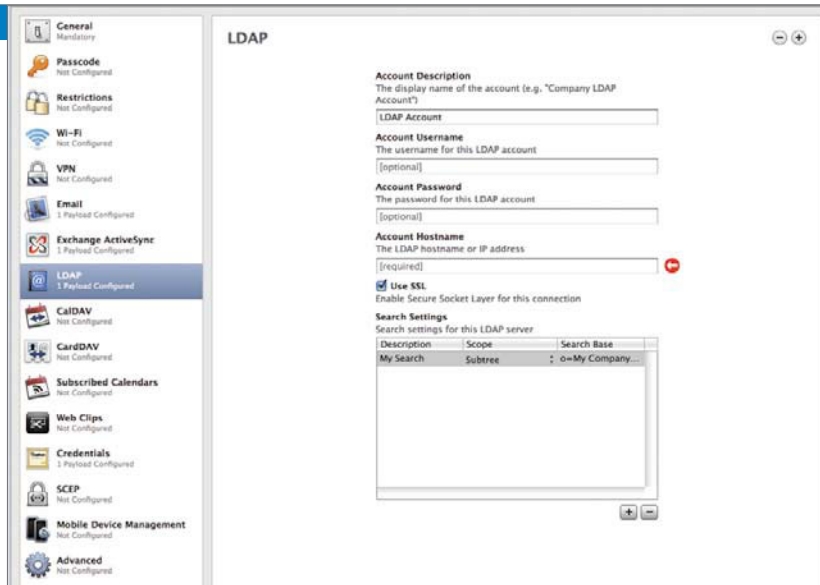


FIGURE 4.10 LDAP settings

Lightweight Directory Access Protocol (LDAP) started as a way to track email contact information and eventually morphed into the way companies manage all their computers and users. While Active Directory, Open Directory, and OpenLDAP are all based on LDAP, for the purposes of this book, LDAP is used only as a contact database.

Most of the settings here are pretty basic (**Figure 4.10**), with a couple of exceptions. The first exception is the “Account Username” field. Depending on your server type, your account name can look like:

- john
- john@company.com
- cn=john,cn=users,dc=example,dc=com

The last example is a full *distinguished name* and completely specifies the user, who in this case is *john*, in the *users* container in the domain *example.com*. It's simple, but only if you know how to read LDAP-ese. In that sense, LDAP is kind of like VPN. If you're running your LDAP server, you already know this; if you aren't, schedule some time with your directory administrator and have that person help you set up this information.

---

The second LDAP setting that might catch you off guard is the Search Settings field, which requires some basic knowledge of LDAP structure. LDAP is, in general, structured like a tree. At the root, you have the domain, so *company.com* would map to “dc=company,dc=com”. Everything expands out from there in a variety of containers (generally, although somewhat incorrectly, abbreviated as CN) and organizational units (OU).

When searching an LDAP directory, you obviously want to limit how much data has to be searched for the benefit of the search speed, and also to control the overall load on the system. A hundred devices searching thousands of entries are going to create a greater server load than if they’re searching a few hundred entries. So, you limit searches by the scope, or range, of the search and by the starting point. To set your search scope, you have three options:

- Base, which searches only the defined search base. If the data you want is one level below that base, the search won’t find it.
- One Level, which searches the base and the level immediately below it
- Subtree, which searches the base and everything below the base regardless of the number of levels.

The next step is to set up your Search Base or starting point. Since you’re really just using LDAP for email contact information, you’ll want to set up the container or OU for your users. If your LDAP directory is Apple’s Open Directory, typically the OU will be the users container, the Open Directory Master computer name, and the domain name. So:

```
cn=users,dc=odmasterserver,dc=domain,dc=com
```

would be a typical search base for a generic Open Directory setup. Other LDAP implementations would be different, but similar to this.

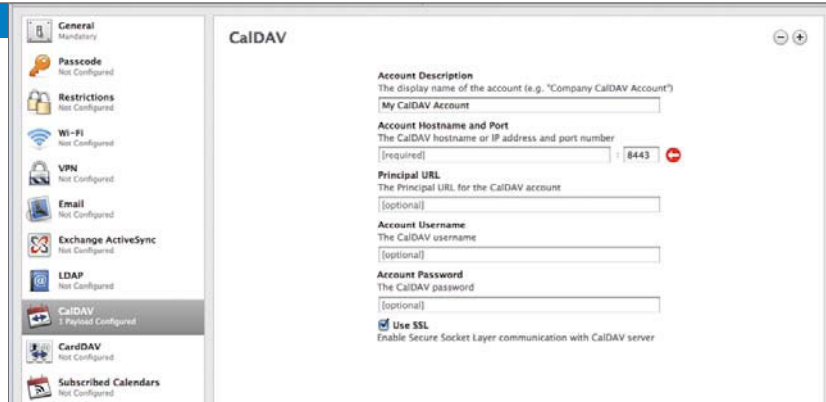
By restricting your starting point to just the users container, you can set the search scope to be “Subtree”, and not worry about every device iterating through every part of the LDAP directory just to find Bob’s email address. When LDAP is set up, both the Email and Contacts apps on the device will automatically use LDAP data for activities such as autofilling email addresses in messages.

### **BIG SCARY LDAP WARNING**

As I just said, LDAP isn’t only for email addresses. A modern LDAP implementation can, and often does, contain almost every bit of data about the people and computers in a company. It can also contain office lists, conference room lists, personal phone numbers and addresses, and all sorts of other information that you don’t want the world to be able to find. If you are going to set up LDAP on your iOS devices, it is *critical* that you do not allow anonymous access over unencrypted connections. You really, really, *really* want to require SSL, and use both usernames and passwords for everyone allowed to access your LDAP information from outside your company’s network. Plus, it’s a very good idea to also require it inside the company network. If everything is encrypted, someone who manages to get past your firewall still ends up with a whole lot of nothing for the effort.

## SETTING THE DATE WITH CALDAV

FIGURE 4.11 CalDAV settings



CalDAV is an open calendaring standard used by many companies, Apple and Google among them, to set up calendar servers. Unsurprisingly, iOS supports CalDAV. (A little background: CalDAV combines .ics calendaring files as the data format and WebDAV as the transport mechanism, hence: CalDAV.) The setup is simple with the only oddball bit being the Principal URL (**Figure 4.11**). That's the URL that contains the path to the CalDAV store on the server. This path can vary depending on the server and its implementation. For example, the Principal URL might look like `/caldav/users/domain.com/john/`.

As with Email and other “user input required” settings, leave the Account Username and Account Password fields blank to permit the user to enter that information. And always use SSL.

## GETTING IN TOUCH WITH CARDDAV

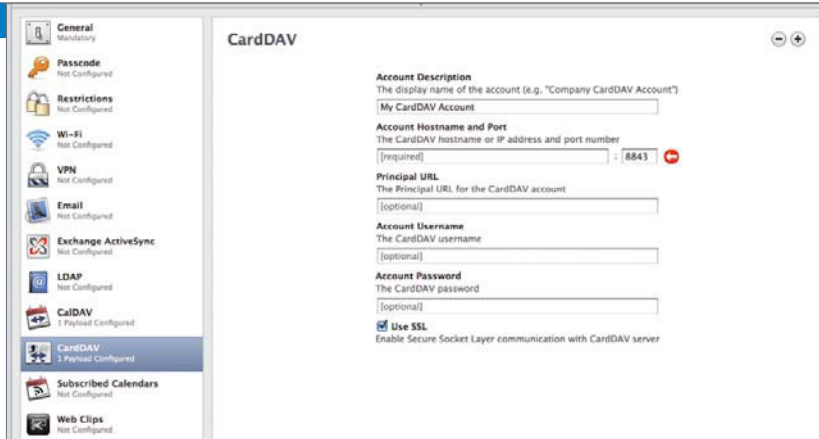
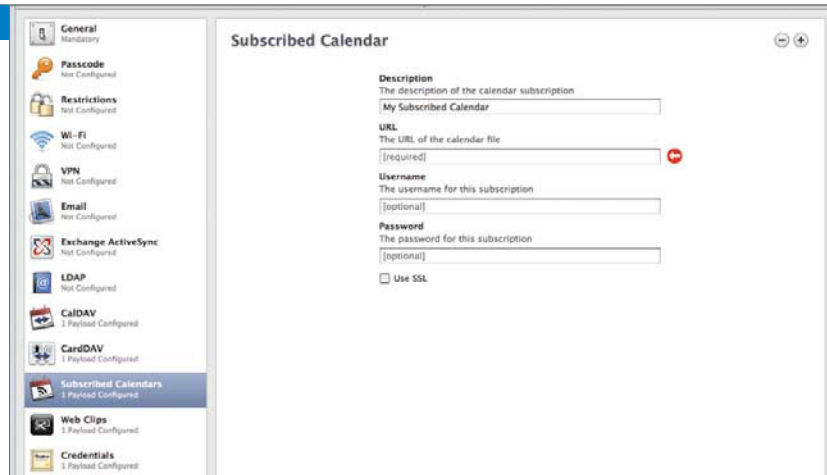


FIGURE 4.12 CardDAV settings

As you saw earlier, LDAP, while usable for email addresses and other contact info, is not always the best choice for many reasons, including that it's kind of a pain to set up. So, a few years back, Apple and several other entities took the CalDAV concept and applied it to contacts. What they came up with was using the vCard format as the data store and, again, WebDAV as the transport mechanism. The result? CardDAV. The setup is identical to CalDAV, including my standard warning to use SSL (Figure 4.12).

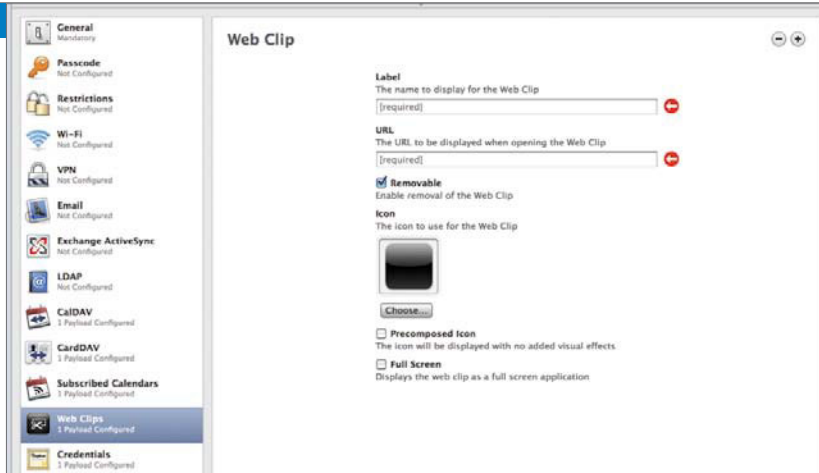
## KEEPING UP WITH SUBSCRIBED CALENDARS

**FIGURE 4.13** Enter username and password in the Subscribed Calendar settings.



These are publicly-accessible, read-only calendars based on the .ics file format that may be used for event lists, team schedules, and so on. Apple has a list of publicly accessible calendars at [www.apple.com/downloads/macosx/calendars/](http://www.apple.com/downloads/macosx/calendars/). If the calendar in question requires a username and password, those would be entered here (**Figure 4.13**), unless they need to be customized for each user, in which case you'd leave them blank. As always, use SSL if it's an option. (Though, sometimes, you just don't care. I doubt it's a problem if Little Bobby Haxxor sniffs the updates to my calendar of sunrise/sunset times in Helsinki.)

## USING WEB CLIPS

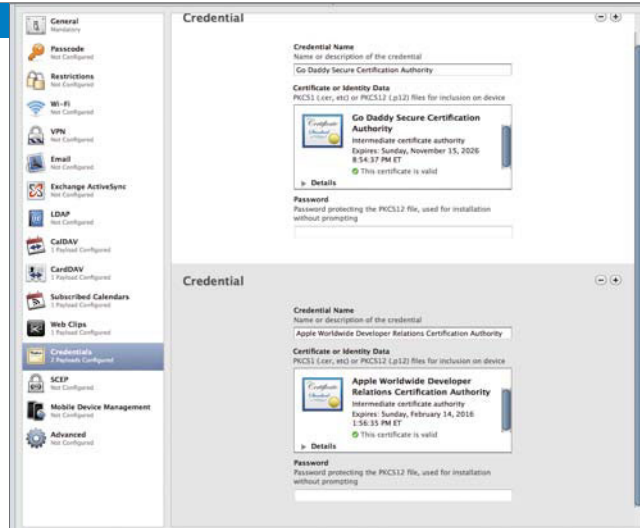


**FIGURE 4.14** Create web links for the iOS device.

At first glance, these settings can seem kind of useless. “What? Now we don’t want them typing in a browser?” But if you think about it, placing web links on an iOS device can be pretty useful for many companies. For example, do you have an internal Wiki or other informational web page? You can set those up here, and make them available on an iOS device without requiring the user to trawl through bookmarks. Do you have custom internal web applications for your users? Enter the info here (**Figure 4.14**), add a pretty icon, and select the “Full Screen” checkbox. When someone taps that link, it looks and behaves like an app, not a web page. Smaller companies may not have many uses for this feature, but for larger companies, these links can be quite handy.

## SETTING CREDENTIALS

**FIGURE 4.15** Credentials settings



Here and there I've talked about certificates and SSL. Well, if you have your own web or email servers and you're using SSL, you're going to have your own certificates for them. Or maybe you're using certs for Exchange or your VPN. If you want to install them on the iOS devices that need them, here's where you do it (**Figure 4.15**).

And it's pretty simple. When you click the Add (+) button in the main Credentials pane, you'll see a dialog that asks you to locate the cert file you want to use. Navigate to the file, click Open, and if it's a valid cert file, you're ready to go. As with Email, CalDAV, Exchange ActiveSync, and other settings, you can create multiple entries here. When you install this profile, the certificates are installed on the device, and ready for use.

## ABOUT SCEP

Simple Certificate Enrollment Protocol (SCEP) can securely add certificates to a device over the air (OTA). In this group of settings, you enter the information needed to use your device with a SCEP server. I'm not going to go into this in any detail here because several later chapters are devoted to SCEP and will provide all the detail you need.



## USING MOBILE DEVICE MANAGEMENT

Mobile Device Management (MDM) allows you to do everything you’ve done here in the iPCU, but wirelessly, securely, and with a lot less work on the part of the user. MDM works with Apple’s Push Notification Server (APNS) to wirelessly push configurations and configuration changes to iOS devices. As you’ll see later in the book, you can do some really cool stuff with MDM. Because Mobile Device Management will be explored in detail later, you can leave these settings alone for now; although if you examine them, you’ll begin to see what you can do with MDM, and how useful it can be.

## MANAGING ADVANCED SETTINGS

Remember back in the “Setting a Passcode” section that I said some things that fall into the “If I have to ask, the answer is probably No” category? The Advanced settings in the iPCU are the perfect example. Here you change your devices’ cellular connection settings. Apple says it in the iPCU settings themselves, and I’ll repeat it here: *These settings should only be managed by trained professionals*. If you mess these up, your users won’t have an iPhone or an iPad with 3G features any more. They have an iPod Touch. The iPod Touch is a neat bit of kit, but not if you need to make a call or use the cellular network to get work done. Unless you have a clear need to change these settings and know *exactly* what you are doing and *why* you are doing it, stay away from these settings like they were a swarm of rabid wolverines.

## WRAPPING UP

Woohoo! You made it through all the configuration profile settings! Congratulate yourself, you now have a solid bit of knowledge to help you manage and set up your iOS devices. Next, we’ll dive a little deeper and look at the structure of the configuration files you’ll be creating when you want to install these settings on devices without using a USB cable.

# INDEX

## A

- Absolute Manage, 114, 131–132
- Adaptive Security Appliances (ASA) devices, 139–142
- ADCS (Active Directory Certificate Services) role, 128–130, 132
- Advanced settings, Configuration Profiles, iPCU, 51
- Afaria, Sybase, 114
- airwatch, 114
- allowAssistant option, 62
- allowCloudBackup option, 62
- allowCloudDocumentSync option, 62
- allowPhotoStream option, 62
- allowUntrustedTLSPrompt option, 62
- Amazon's S3 service, 91
- AnyConnect VPN, 139–141
- Apple Push Notification Certificate documentation, 173
  - MDM (Mobile Device Management), 114
- Apple Push Notification Server, MDM (Mobile Device Management), 152
  - Configuration Profiles, iPCU, 51
- AppleScript
  - basics, 66
  - Cocoa APIs, 60
  - dictionaries, 67
    - caution, mixing commands from different dictionaries, 72
    - Scripting Additions, 72
    - Standard Additions, 67
    - Standard Additions: display dialog, 72
  - display dialog/dialog reply, 72–73
  - English-like, 66
  - repeat loops, 75
  - resources, 66–67
  - script editors, 67
  - scripting iPCU, 67–78
  - tell blocks, 66–77
  - theProfile, 68–77
    - CalDAV, 70–71, 74, 77
    - email, 70–71, 73, 77
    - restrictions, 69, 71, 73, 76–77
    - theEmailAddress, 75–76
    - theExportPath, 75–77
    - theFileName, 75–77
    - theFileReference, 74–75
    - theName, 75–76
    - theNameList, 75
    - theSourceFile, 74, 76
    - theUserName, 75–76
- AppleScript Editor, Mac OS X 10.6, 67
- AppleScript Users' email list, 66
- Apple Training Series: AppleScript 1-2-3*, 66
- applications
  - iTunes and iOS devices, 7
  - OTA (over-the-air) distribution, with MDM (Mobile Device Management)
    - Casper, deleting apps, 214
    - Casper, installing apps, 210–213
    - Casper, managing apps, 216–218, 226
    - Casper, updating apps, 214–215
    - OS X Server 10.7, installing and managing apps, 219–220
  - OTA (over-the-air) distribution, with web servers, 96
    - accessing server, 205
    - background, 198–199
    - installing apps, 206–207, 226
    - jailbroken distribution, 200
    - preparing apps, 201–204
    - registering devices, 198–200
    - requirements, 198–200
    - Wi-Fi *versus* cellular, 198
    - wired *versus* wireless distribution, 198–199
- Applications section, iPCU, 17–18
  - enterprise *versus* App Store, 18, 21, 198, 200
  - installing/uninstalling apps, 27–29
  - managing apps, 18
- App Store apps
  - versus* Enterprise apps, 18, 21, 198, 200
  - managing, 216–218
  - uninstalling, 29
- ASA (Adaptive Security Appliances) devices, 139–142
- authentication
  - Amazon's S3 service, 91
  - ASA (Adaptive Security Appliances) devices, 139–142
    - authenticated SMTP, 57
    - Cisco implementation, 139
    - EAP (Extensible Authentication Protocol), 37
    - HTTP MD5 Digest Authentication, 57
    - iPhone Business Resources page, 16
    - OTA (over-the-air) distribution, 93–94
    - provisioning profiles, 23
    - SCEP (Simple Certificate Enrollment Protocol), 102–103, 184
    - LDAP-based, 116
  - AutoJoin option, 62

## B – C

backups, Apple's iCloud service, 7, 62

Bucket Explorer website, 91

CA (Certificate authority), 63

    SCEP (Simple Certificate Enrollment Protocol)

        Casper, 114, 184

        OS X 10.6 Server, 112

CalDAV

    Configuration Profiles, iPCU, 46

    iTunes, 9

    theProfile, AppleScript, 70–71, 74, 77

calendars

    CalDAV

        Configuration Profiles, iPCU, 46

        iTunes, 9

        theProfile, AppleScript, 70–71, 74, 77

    Subscribed Calendars, Configuration Profiles, iPCU, 48

camera, disabling, 11

CardDAV

    Configuration Profiles, iPCU, 47

    iTunes, 9

    LDAP (Lightweight Directory Access Protocol), 9, 45

    MDM (Mobile Device Management), 164–165

Casper, JAMF Ssoftware

    MDM (Mobile Device Management), 116–117

        CardDAV, 164–165

        OTA (over-the-air) distribution of applications, 210–218

        passcodes, 158, 161

    SCEP (Simple Certificate Enrollment Protocol), 114–118

        Apple Push Notification Certificate, 114

Certificate Authority (CA), 63

    SCEP (Simple Certificate Enrollment Protocol)

        Casper, 114

        OS X 10.6 Server, 112

certificates

    Apple Push Notification Certificate, 114, 173

    Apple Push Notification Server, 51, 152

    CSRs (certificate signing requests), 103–106

    MDM (Mobile Device Management), 166–167

    NSData blob, 60

    SCEP (Simple Certificate Enrollment Protocol), 103–106

        Casper, 114–118

        Mac OS X Server 10.6, 112

        Mac OS X Server 10.7, 121–122, 124

    SMIMESigningCertificateUUID option, 62

    SSLs (Secure Sockets Layers), 103, 106

Cheeseman, Bill, 66

Cisco implementation

    IOS (Internet Operating System), 112, 137–138

    SCEP (Simple Certificate Enrollment Protocol)

        AnyConnect VPN, 139–141

        ASA (Adaptive Security Appliances) devices, 139–142

        documentation, 139, 143

        overview, 139

        testing, 143

Cocoa's NSData blob, 60

configuration profiles. *See also* Configuration Profiles, iPCU

    AppleScript, 66–78

        basics, 66

        dictionaries, 67, 72

        display dialog/dialog reply, 72–73

        English-like, 66

        repeat loops, 75

        resources, 66

        script editors, 67

        scripting iPCU, 67–78

        tell blocks, 66–77

        theProfile, 68–77

    disadvantages, 148

    distribution

        OTA (over-the-air) (*See also* SCEP)

        OTA (over-the-air), from web servers, 90, 91–95

        OTA (over-the-air), Windows Server 2008, 128–133

        tethered method, 82–83

    email, installing

        with iPCU, 84

        with OS X 10.7 Profile Manager, 84–87

    encryption, 57, 59

    managing, 18

    MDM (Mobile Device Management), 151–152

        advantages, 156

*versus* configuring without MDM, 162–163

        device inventory/information collection, 166–167

        locking profiles, 192

        passcodes, 157–163

    .mobileconfig file, 54

        <dict></dict> blocks, 55–56

        encrypting, 59, 63

        General settings, Configuration Profiles, iPCU, 55

        options new in iOS 5, 62

        PayloadRemovalDisallowed key, 55–56

        PayloadType key, 57

        PayloadUUID key, 55–57

        reasons to build/modify, 61

        signing, 63

- configuration profiles (*continued*)
  - SCEP (Simple Certificate Enrollment Protocol)
    - authentication, 102–103
    - certificate enrollment, 103–106
    - encryption, 107
- Configuration Profiles section, iPCU, 17–19. *See also* configuration profiles
  - Advanced settings, 51
  - CalDAV settings, 46
  - CardDAV settings, 47
  - Credentials settings, 50
  - EAS (Exchange ActiveSync) settings, 40–42, 62
  - Email settings, 39–40, 62
    - File menu, Share via Email, 84
    - IMAP *versus* POP.IMAP standards, 39
    - Path Prefix setting, 40
    - SMTP (Simple Mail Transfer Protocol), 39
    - SSLs (Secure Sockets Layers), 39
  - File, Share via Email, 84
  - General settings
    - authorization, 34
    - Exchange accounts, 33
    - identity security, 32
    - .mobileconfig file structure, 55
    - multiple profiles, 32
    - Organization and Description fields, 33
    - Profiles, Remove, 82
  - Install, 82–83
  - LDAP (Lightweight Directory Access Protocol) settings, 43–45
  - MDM (Mobile Device Management) settings, 51
  - Passcode settings, 35
  - profiles
    - locking, 192
    - managing, 18
  - Restrictions settings, 36, 62
  - SCEP (Simple Certificate Enrollment Protocol) settings, 50
  - Security settings, 34
  - Subscribed Calendar settings, 48
  - VPN settings, 38
  - Web Clips settings, 49
  - Wi-Fi settings, 37, 62
- contacts, CardDAV
  - Configuration Profiles, iPCU, 47
  - iTunes, 8–9
  - LDAP (Lightweight Directory Access Protocol), 9, 45
  - MDM (Mobile Device Management), 164–165
  - Credentials settings, Configuration Profiles, iPCU, 50
  - CSRs (certificate signing requests), 103–106

## D

- data storage on personal devices
  - encryption recommended, 5
  - security risks, 4
- .deviceids files, 24–25
- Devices section, iPCU, devices
  - registering, 22, 25
  - registration limitations, 25
  - uploading, 24–25
  - viewing, 17, 24
- Devices section (currently- connected devices), apps and profiles, installing/uninstalling, 27–29
- <dict></dict> blocks, 55–56
- dictionaries, AppleScript, 67
  - caution, mixing commands from different dictionaries, 72
  - Scripting Additions, 72
  - Standard Additions, 67, 72
  - display dialog, 72
- display dialog/dialog reply, AppleScript, 72–73
- documentation
  - Apple Push Notification Certificates, 173
  - AppleScript, 66
  - Apple's iPhone Support—Business Resources and Enterprise pages, 16
  - application distribution, 96, 199
  - Bucket Explorer, 91
  - Cisco and SCEP (Simple Certificate Enrollment Protocol), 130, 139, 143
  - Enterprise Deployment Guide, 55–56
  - JSS (JMAF software server), 176
  - Profile Manager, 16
  - provisioning profiles, 26
  - SCEP (Simple Certificate Enrollment Protocol), 102
    - Casper, 114
    - Cisco, 130, 139, 143
    - OS X.6 Server, 112–113
    - OTA (over-the-air) distribution, 101
  - security, 119
  - Windows Server 2008 and SCEP (Simple Certificate Enrollment Protocol), 128, 130

## E

- EAP (Extensible Authentication Protocol), 37
- EAS (Exchange ActiveSync)
  - Apple's iPhone Support—Business Resources page, 16
  - Configuration Profiles, iPCU, 40–42, 62

- email
  - AppleScript
    - theProfile, 70–71, 73, 77
    - theProfile, theEmailAddress, 75–76
  - AppleScript Users' email list, 66
  - configuration profiles, installing
    - with iPCU, 84
    - with OS X Server 10.7 Profile Manager, 84–87
  - Configuration Profiles, iPCU, 39–40, 62
    - File menu, Share via Email, 84
    - IMAP and POP standards, 39–40
    - LDAP (Lightweight Directory Access Protocol), 45
    - Path Prefix setting, 40
    - SMTP (Simple Mail Transfer Protocol), 39
    - SSLs (Secure Sockets Layers), 39
  - iTunes
    - IMAP and POP standards, 9–10
    - preventing account changes, 11
    - syncing with computers, 8–9
  - .mobileconfig file payloads, 57–58, 70–71, 73, 77
- encryption
  - anonymous access caution, 45
  - configuration profiles, 36, 57, 59, 63
  - CSRs (certificate signing requests), 103–106
  - data storage on mobile devices, 5
  - EncryptionType option, 62
  - MDM (Mobile Device Management), 150
  - public and private keys, 107
  - SMIMEEncryptionCertificateUUID option, 62
- Enterprise Deployment Guide, 55–56, 59
- Exchange ActiveSync (EAS)
  - Apple's iPhone Support—Business Resources page, 16
  - Configuration Profiles, iPCU, 40–42, 62
- Extensible Authentication Protocol (EAP), 37

## F – G

- forceITunesStorePasswordEntry option, 62
- Game Center features, disabling, 11
- General settings, Configuration Profiles, iPCU
  - authorization, 34
  - Exchange accounts, 33
  - identity security, 32
  - multiple profiles, 32
  - Organization and Description fields, 33
  - Security settings, 34
- Good, 114
- Google/Gmail
  - Apple's iPhone Support—Business Resources page, 16

- Configuration Profiles, iPCU
  - Calendar, 40
  - Contacts, 40
  - EAS (Exchange ActiveSync), 40–42, 62
  - Gmail, 40
  - Path Prefix setting, 40

## H

- help sources
  - Apple Push Notification Certificates, 173
  - AppleScript Editor, Mac OS X 10.6, 67
  - AppleScript Users' email list, 66
  - Apple's iPhone Support—Business Resources and Enterprise pages, 16
  - Apple Training Series: AppleScript 1-2-3*, 66
  - application distribution, 96, 199
  - Bucket Explorer, 91
  - Cisco and SCEP (Simple Certificate Enrollment Protocol), 130, 139, 143
  - Enterprise Deployment Guide, 55–56, 59
  - JSS (JMAF Software Server), 176
  - Profile Manager, 16
  - provisioning profiles, 26
  - SCEP (Simple Certificate Enrollment Protocol), 102
    - Casper, 114
    - Cisco, 130, 139, 143
    - OS X.6 Server, 112–113
    - OTA (over-the-air) distribution, 101
    - Windows Server 2008, 128, 130
  - security, 119
- HTTP MD5 Digest Authentication, 57

## I

- iCloud service, back ups, 7, 62
- IIS (Internet Information Services), 128–129, 131
- IMAP standards, *versus* POP standards
  - Configuration Profiles, iPCU, 39–40
  - iTunes, 9–10
- Internet Information Services (IIS), 128–129, 131
- IOS (Internet Operating System), Cisco, 137–138
- iOS 5
  - iTunes and iOS devices, 6
  - .mobileconfig file, new options, 62
  - OS X Server 10.7, 210
- iOS Developer Enterprise Program
  - device registration, 22, 198–200
  - MDM (Mobile Device Management), 190
- iOS Developer Program, 22

iOS management tools, OS X Server 10.7, 16

## iPad

- Advanced settings, Configuration Profiles, iPCU, 51
- profiles, installing/removing, 83
- setup documentation, 113

## iPCU (iPhone Configuration Utility)

- Apple's iPhone Support, Business Resources and Enterprise pages, 16

- Apple's iPhone Support, Enterprise page, 16

- Applications section, 17–18

  - apps, enterprise *versus* App Store, 18, 21, 198, 200

  - apps, installing/uninstalling, 27–29

  - apps, managing, 18

- Configuration Profiles section, 17–19 (*See also* configuration profiles)

  - Advanced settings, 51

  - CalDAV settings, 46

  - CardDAV settings, 47

  - Credentials settings, 50

  - EAS (Exchange ActiveSync) settings, 40–42, 62

  - Email settings, 39–40, 62

  - File, Share via Email, 84

  - General settings, 32–34, 82–83

  - Install, 82–83

  - LDAP (Lightweight Directory Access Protocol) settings, 43–45

  - locking profiles, 192

  - MDM (Mobile Device Management) settings, 51

  - .mobileconfig file structure, 55

  - Passcode settings, 35

  - Restrictions settings, 36, 62

  - SCEP (Simple Certificate Enrollment Protocol) settings, 50

  - Subscribed Calendar settings, 48

  - VPN settings, 38

  - Web Clips settings, 49

  - Wi-Fi settings, 37, 62

## Devices section

- devices, registering, 22, 25

- devices, registration limitations, 25

- devices, uploading, 24–25

- devices, viewing, 17, 24

- Devices section (currently- connected devices), apps and profiles, installing/uninstalling, 27–29

- dictionary, 67

- disadvantages, 148

- .mobileconfig files, 68–77

## OS X Server 10.7

- versus* OS X Server 10.6, 34

- Profile Manager warning, 16, 61

- platforms supported, 16

- Provisioning Profiles section, 17–18

  - distribution profiles, applying, 26

  - provisioning portal, 22–23

  - provisioning profiles, defined, 22

  - provisioning profiles, installing/uninstalling, 23–25, 27–29

- registering devices

  - iOS Developer Enterprise Program, 22, 25

  - iOS Developer Program, 22, 25

  - limitations, 25

- resources, 16

- Summary section, 17

## iPhone

- Advanced settings, Configuration Profiles, iPCU, 51

- Apple's iPhone Support, Business Resources and

  - Enterprise pages, 16

- manual device settings, 11

- Windows Server 2008 problem, 130

## iPhone Configuration Utility (iPCU)

- Apple's iPhone Support, Business Resources and

  - Enterprise pages, 16

- Apple's iPhone Support, Enterprise page, 16

- Applications section, 17–18

  - apps, enterprise *versus* App Store, 18, 21, 198, 200

  - apps, installing/uninstalling, 27–29

  - apps, managing, 18

- Configuration Profiles section, 17–19 (*See also* configuration profiles)

  - Advanced settings, 51

  - CalDAV settings, 46

  - CardDAV settings, 47

  - Credentials settings, 50

  - EAS (Exchange ActiveSync) settings, 40–42, 62

  - Email settings, 39–40, 62

  - File, Share via Email, 84

  - General settings, 32–34, 82–83

  - Install, 82–83

  - LDAP (Lightweight Directory Access Protocol) settings, 43–45

  - locking profiles, 192

  - MDM (Mobile Device Management) settings, 51

  - .mobileconfig file structure, 55

  - Passcode settings, 35

  - Restrictions settings, 36, 62

  - SCEP (Simple Certificate Enrollment Protocol) settings, 50

  - Subscribed Calendar settings, 48

  - VPN settings, 38

- Web Clips settings, 49
- Wi-Fi settings, 37, 62
- Devices section
  - devices, registering, 22, 25
  - devices, registration limitations, 25
  - devices, uploading, 24–25
  - devices, viewing, 17, 24
- Devices section (currently-connected devices),
  - apps and profiles, installing/uninstalling, 27–29
- dictionary, 67
- disadvantages, 148
- .mobileconfig files, 68–77
- OS X Server 10.7
  - versus* OS X Server 10.6, 34
  - Profile Manager warning, 16, 61
- platforms supported, 16
- Provisioning Profiles section, 17–18
  - distribution profiles, applying, 26
  - provisioning portal, 22–23
  - provisioning profiles, defined, 22
  - provisioning profiles, installing/uninstalling, 23–25, 27–29
- registering devices
  - iOS Developer Enterprise Program, 22, 25
  - iOS Developer Program, 22, 25
  - limitations, 25
- resources, 16
- Summary section, 17
- iPod Touch, Advanced settings, Configuration Profiles, iPCU, 51
- iTunes and iOS devices
  - applications, 7
  - backing up to Apple's iCloud service, 7
  - basic settings
    - iOS 4.x, 5
    - iOS 5, 6
  - data storage on personal devices, security risks, 4
  - email
    - IMAP *versus* POP/IMAP standards, 9–10
    - preventing account changes, 11
    - syncing with computers, 8–9
  - limitations, 4
  - manual settings, 11
  - OTA (over-the-air) configuration, 4, 6
  - parental controls, 10
  - restrictions, 11
  - SMB (small-to-medium business), 4
  - SOHO (small office/home office), 4
  - syncing with computers, 6–9
- iTunes Music Store, 36

## J

- jailbreaking iOS devices, 22, 200
- JAMF Software
  - Casper
    - MDM (Mobile Device Management), 116–117
    - CardDAV, 164–165
    - OTA (over-the-air) distribution of applications, 210–218
    - passcodes, 158, 161
  - SCEP (Simple Certificate Enrollment Protocol) setup, 113–118
  - Apple Push Notification Certificate, 114
- JSS (JAMF Software Server), 177–178, 184–185

## K

- Kerio Connect, EAS settings, 42
- Keychain application, 121
- keys/PKI (Public Key Infrastructure), 57, 63, 107, 121–123, 131
- Krebs, Brian, 119

## L

- LANRev. *See* Absolute Manage
- Late Night Software's Script Debugger, 67
- LDAP (Lightweight Directory Access Protocol)
  - CardDAV/LDAP, 9
  - Configuration Profiles, iPCU, 43–45
  - MDM (Mobile Device Management), 190
- Linux, documentation, Apple Push Notification Certificates, 173
- Lion OS. *See* OS X Server 10.7

## M

- MacScripter, 66
- MDM (Mobile Device Management)
  - Apple Push Notification Certificate, 152
  - CardDAV, 164–165
  - Casper, 116–117
    - CardDAV, 164–165
    - OTA (over-the-air) distribution, 210–218
    - passcodes, 158, 161
  - complexity, 190–191
  - configuration profiles, 151–152
    - advantages, 156
    - comparison without using MDM, 162–163
    - device inventory/information collection, 166–167
    - locking, 192
    - MDM advantages, 156
    - passcodes, 157–163

## MDM (Mobile Device Management) (*continued*)

- Configuration Profiles, iPCU, 51
  - enrollment, 150
  - iOS Developer Enterprise Program, 190
  - LDAP (Lightweight Directory Access Protocol), 190
  - OS X Server 10.7, 34, 119, 219–220
  - OTA (over-the-air) distribution
    - Casper, 210–218
    - infrastructure issues, 224
    - issues for developers, 225
    - OS X Server 10.7, 219–220
  - overview, 149
  - Windows Server 2008, 131–132
- Microsoft Windows/Windows Server
- Apple Push Notification Certificates, documentation, 173
  - Exchange Server, 42
  - iOS device management
    - Good, 114
    - Sybase's Afaria, 114
  - iPCU (iPhone Configuration Utility), tethered profile
    - installation, 82–83
  - Microsoft .NET Framework 3.5 SP1 and iPCU, 16
  - SCEP (Simple Certificate Enrollment Protocol), 112
    - Absolute Manage, 131–132
    - configuration profiles, 102, 128–133
    - documentation, 128, 130
    - IIS (Internet Information Services), 128–129, 131
    - MDM (Mobile Device Management) server, 131–132
    - NDES (National Device Enrollment Service), 129–130
    - Server Manager, 128
- .mobileconfig files, 54
- <dict></dict> blocks, 55–56
  - encrypting, 59, 63
  - General settings, Configuration Profiles, iPCU, 55
  - PayloadRemovalDisallowed, 55–56
  - PayloadType, 57
  - PayloadUUID, 55–57
  - reasons to build/modify, 61
  - scripting with AppleScript, 66–78
  - signing, 63
- Mobile Device Management (MDM)
- Apple Push Notification Server, 152
  - CardDAV, 164–165
  - Casper, 116–117
    - CardDAV, 164–165
    - OTA (over-the-air) distribution, 210–218
    - passcodes, 158, 161
  - complexity, 190–191

- configuration profiles, 151–152
    - advantages, 156
    - comparison without using MDM, 162–163
    - device inventory/information collection, 166–167
    - locking, 192
    - MDM advantages, 156
    - passcodes, 157–163
  - Configuration Profiles, iPCU, 51
  - enrollment, 150
  - iOS Developer Enterprise Program, 190
  - LDAP (Lightweight Directory Access Protocol), 190
  - OS X Server 10.7, 34, 119, 219–220
  - OTA (over-the-air) distribution
    - Casper, 210–218
    - OS X Server 10.7, 219–220
  - overview, 149
  - Windows Server 2008, 131–132
- .mobileprovision files, 23

## N – O

- NDES (National Device Enrollment Service), 129–130
- .NET Framework 3.5 SP1, Microsoft, and iPCU, 16
- NSData blob, 60
- Objective-C, .mobileconfig files, 60
- Open Directory, Apple
  - documentation, 113
  - LDAP settings, Configuration Profiles, iPCU, 44
  - OTA (over-the-air) distribution, 92–93
  - Profile Manager, OS X Server 10.7, 124
- OpenSCEP, 113
- OS X Server 10.6
  - versus* 10.7, 34
  - Apple Push Notification Certificates, documentation, 173
  - MDM (Mobile Device Management) and Casper,
    - passcodes, 161
  - OTA (over-the-air) distribution, 92
  - SCEP (Simple Certificate Enrollment Protocol) setup,
    - 112–113
- OS X Server 10.7
  - versus* 10.6, 34
  - Apple Push Notification Certificates, documentation, 173
  - iOS 5, 210
  - MDM (Mobile Device Management)
    - CardDAV, 164–165
    - device inventory/information collection, 166–167
  - OTA (over-the-air) distribution, 92, 219–220
  - Profile Manager, 16
    - installing configuration profiles by email, 84–87



- iPCU warning, 16, 61
- SCEP (Simple Certificate Enrollment Protocol) setup, 119–125
- OTA (over-the-air) distribution. *See also* SCEP
  - applications, 96
    - accessing app distribution web server, 205
    - background, 198–199
    - installing apps, 206–207, 226
    - jailbroken distribution, 22, 200
    - with MDM (Mobile Device Management), Casper, 210–218
    - with MDM (Mobile Device Management), OS X Server 10.7, 219–220
    - preparing apps, 201–204
    - registering devices, 198–200
    - requirements, 198–200
    - Wi-Fi *versus* cellular, 198
    - wired *versus* wireless distribution, 198–199
  - configuration profiles
    - from web servers, 90, 94–95
    - from web servers, Amazon's S3 service, 91
    - from web servers, server setup, 92–93
  - infrastructure issues, 224
  - issues for developers, 225
  - iTunes, iOS 5 *versus* iOS 4.x, 4, 6
  - OS X Server 10.7, 34, 219–220

## P – Q

- parental controls, iTunes, 10
- passcodes, Configuration Profiles, iPCU, settings, 35
- PayloadRemovalDisallowed key, 55–56
- PayloadType key, 57
- PayloadUUID key, 55–57
- PKI (Public Key Infrastructure)/keys, 57, 63, 107, 121–123, 131
- POP *versus* IMAP standards
  - Configuration Profiles, iPCU, 39–40
  - iTunes configuration, 9–10
- PreventAppSheet option, 62
- PreventMove option, 62
- private keys, 107
- Profile Manager, OS X Server 10.7
  - app distribution, 219–220
  - email installation, 84–87
  - iOS management tools, 16, 120
  - iPCU (iPhone Configuration Utility), Profile Manager warning, 16, 61
- Open Directory, 124–125

- OTA (over-the-air) distribution, 95
  - setup, 124–125
- Provisioning Profiles section, iPCU, 17–18
  - distribution profiles, applying, 26
  - provisioning portal, 22–23
  - provisioning profiles, 211
    - defined, 22
    - device registration, 199–200
    - installing/uninstalling, 23–25, 27–29
- ProxyType option, 62
- Public Key Infrastructure (PKI), 107
- public keys, 107
- Python and Cocoa APIs, 60

## R

- registration of devices
  - iOS Developer Enterprise Program, 22, 25, 198–199
  - iOS Developer Program, 22, 25
  - limitations, 25
- repeat loops, AppleScript, 75
- resources
  - Apple Push Notification Certificates, 173
  - AppleScript Editor, Mac OS X 10.6, 67
  - AppleScript Users' email list, 66
  - Apple's iPhone Support—Business Resources and Enterprise pages, 16
  - Apple Training Series: AppleScript 1-2-3*, 66
  - application distribution, 96, 199
  - Bucket Explorer, 91
  - Cisco and SCEP (Simple Certificate Enrollment Protocol), 130, 139, 143
  - Enterprise Deployment Guide, 55–56, 59
  - JSS (JMAF Software Server), 176
  - Profile Manager, 16
  - provisioning profiles, 26
  - SCEP (Simple Certificate Enrollment Protocol), 102
    - Casper, 114
    - Cisco, 130, 139, 143
    - OS X.6 Server, 112–113
    - OTA (over-the-air) distribution, 101
    - Windows Server 2008, 128, 130
  - security, 119
- restrictions
  - Configuration Profiles, iPCU, 36, 62
  - iTunes and iOS devices, 11
  - theProfile, AppleScript, 69, 71, 73, 76–77
- roaming charges, Configuration Profiles, iPCU, 36
- Ruby and Cocoa APIs, 60

## S

S3 service, Amazon, 91

SCEP (Simple Certificate Enrollment Protocol)

- background and basics, 100–101

- Casper, 114–118, 184–185

- Cisco implementation, 112

  - AnyConnect VPN, 139–141

  - ASA devices, 139–142

  - IOS (Internet Operating System) on iOS devices, 137–138

  - overview, 139

  - testing, 143

- configuration profiles

  - authentication, 102–103

  - certificate enrollment, 103–106

  - encryption, 107

- Configuration Profiles, iPCU, 50

- OpenSCEP implementation, 113

- OS X Server 10.6 implementation, 112–113

- OS X Server 10.7 implementation, 34, 119–125

- security difficulty, 138

- security risks, 4, 138

- Windows Server 2008, AD CS (Active Directory Certificate Services) role, 128–130, 132

- Windows Server 2008 implementation

  - Absolute Manage, 131–132

  - documentation, 128, 130

  - IIS (Internet Information Services), 128–129, 131

  - MDM (Mobile Device Management) server, 131–132

  - NDES (National Device Enrollment Service), 129–130

  - Server Manager, 128

Script Debugger, Late Night Software, 67

script editors, AppleScript, 67

Secure Sockets Layers (SSLs)

- CalDAV, 46

- CardDAV, 47

- caution, 119

- certificates, 103, 106

- credentials, 50

- CSRs, 103

- EAS, 41

- email, 39, 57

- security risks, 138

- Subscribed Calendars, 48

security

- Configuration Profiles section settings, iPCU, 34

- resources, 119

- risks data on personal devices, 4

- SCEP (Simple Certificate Enrollment Protocol), 4, 138

- SSLs (Secure Sockets Layers), 138

- Server Manager, Windows Server 2008, 128

- Simple Certificate Enrollment Protocol (SCEP)

  - background and basics, 100–101

  - Casper, 114–118, 184–185

  - Cisco implementation, 112

    - AnyConnect VPN, 139–141

    - ASA devices, 139–142

    - IOS (Internet Operating System) on iOS devices, 137–138

    - overview, 139

    - testing, 143

- configuration profiles

  - authentication, 102–103

  - certificate enrollment, 103–106

  - encryption, 107

- Configuration Profiles, iPCU, 50

- OpenSCEP implementation, 113

- OS X Server 10.6 implementation, 112–113

- OS X Server 10.7 implementation, 34, 119–125

- security difficulty, 138

- security risks, 4, 138

- Windows Server 2008, AD CS (Active Directory Certificate Services) role, 128–130, 132

- Windows Server 2008 implementation

  - Absolute Manage, 131–132

  - documentation, 128, 130

  - IIS (Internet Information Services), 128–129, 131

  - MDM (Mobile Device Management) server, 131–132

  - NDES (National Device Enrollment Service), 129–130

  - Server Manager, 128

- small office/home office (SOHO), 4

- SMB (small-to-medium business), 4

- SMIMEEnabled option, 62

- SMIMEEncryptionCertificateUUID option, 62

- SMIMESigningCertificateUUID option, 62

- SMTP (Simple Mail Transfer Protocol), 57

  - Configuration Profiles, iPCU, 39

- Soghoian, Sal, 66

- SOHO (small office/home office), 4

- SSLs (Secure Sockets Layers)

  - CalDAV, 46

  - CardDAV, 47

  - caution, 119

  - certificates, 103, 106

  - credentials, 50

  - CSRs, 103

  - EAS, 41

  - email, 39, 57

- security risks, 138
- Subscribed Calendars, 48
- Subscribed Calendar settings, Configuration Profiles, iPCU, 48
- Summary section, iPCU, 17
- Sybase's Afaria, 114
- syncing with iTunes, iOS devices and computers, 6–7
  - calendars, 8–9
  - contacts, 8–9
  - email, 8–9

## T – U

- tell blocks, AppleScript, 66–77
- tethered installation of configuration profiles, 82–83
- theProfile, AppleScript, 68–77
  - CalDAV, 70–71, 74, 77
  - email, 70–71, 73, 77
  - options
    - theEmailAddress, 75–76
    - theExportPath, 75–77
    - theFileName, 75–77
    - theFileReference, 74–75
    - theName, 75–76
    - theNameList, 75
    - theSourceFile, 74, 76
    - theUserName, 75–76
  - restrictions, 69, 71, 73, 76–77
- uuidgen utility, 55

## V

- Volume Purchase Plan (VPP) program, Apple, 216
- VPN (virtual private network)
  - Apple's iPhone Support—Business Resources page, 16
  - Configuration Profiles, iPCU, 38
- VPP (Volume Purchase Plan) program, Apple, 216

## W – Z

- Web Clips settings, Configuration Profiles, iPCU, 49
- Wi-Fi settings. *See also* wireless distribution
  - Apple's iPhone Support—Business Resources page, 16
  - Configuration Profiles, iPCU, 37, 62

- Windows/Windows Server
  - Apple Push Notification Certificates, documentation, 173
- iOS device management
  - Good, 114
  - Sybase's Afaria, 114
- iPCU (iPhone Configuration Utility)
  - Apple's iPhone Support—Business Resources and Enterprise pages, 16
  - tethered profile installation, 82–83
- SCEP (Simple Certificate Enrollment Protocol)
  - Absolute Manage, 131–132
  - ADCS (Active Directory Certificate Services) role, 128–130, 132
  - configuration profiles, 102, 128–133
  - documentation, 128, 130
  - IIS (Internet Information Services), 128–129, 131
  - MDM (Mobile Device Management) server, 131–132
  - NDES (National Device Enrollment Service), 129–130
  - Server Manager, 128
- wireless distribution. *See also* SCEP
  - applications, 96
    - accessing app distribution web server, 205
    - background, 198–199
    - installing apps, 206–207, 226
    - jailbroken distribution, 22, 200
    - with MDM (Mobile Device Management), Casper, 210–218
    - with MDM (Mobile Device Management), OS X Server 10.7, 219–220
    - preparing apps, 201–204
    - registering devices, 198–200
    - requirements, 198–200
    - Wi-Fi *versus* cellular, 198
    - wired *versus* wireless distribution, 198–199
  - configuration profiles
    - from web servers, 90, 94–95
    - from web servers, Amazon's S3 service, 91
    - from web servers, server setup, 92–93
  - infrastructure issues, 224
  - issues for developers, 225
  - iTunes, iOS 5 *versus* iOS 4.x, 4, 6
  - OS X Server 10.7, 34, 219–220