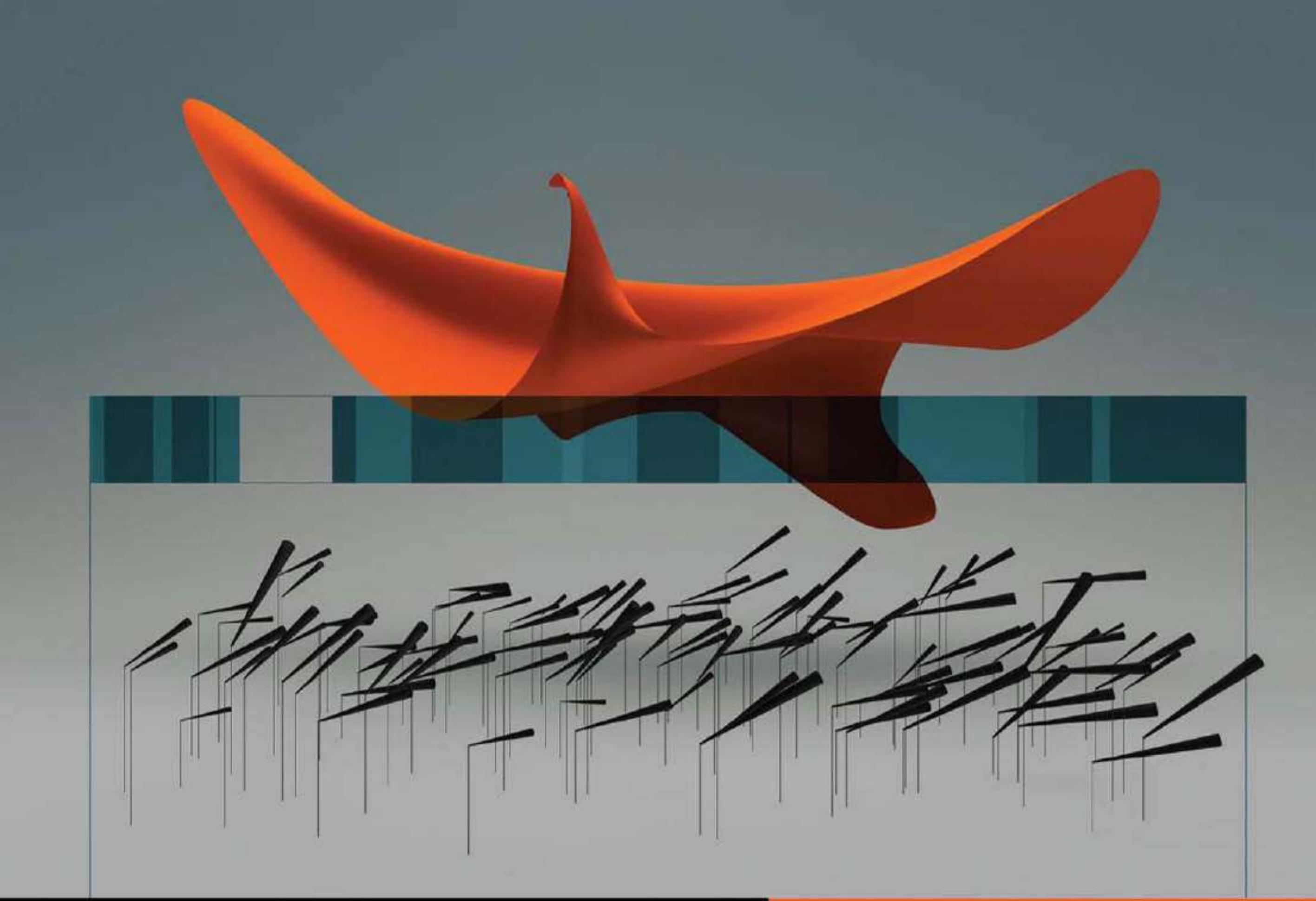


Apple Pro Training Series

OS X Lion Server Essentials

Using and Supporting OS X Lion Server

Arek Dreyer and Ben Greisler

Apple Certified

Certification exam preparation
for: Apple Certified Technical
Coordinator 10.7

Apple Pro Training Series

OS X Lion Server Essentials

Arek Dreyer and Ben Greisler

Apple Certified

Apple Pro Training Series: OS X Lion Server Essentials
Arek Dreyer and Ben Greisler
Copyright © 2012 by Peachpit Press

Published by Peachpit Press. For information on Peachpit Press books, contact:

Peachpit Press
1249 Eighth Street
Berkeley, CA 94710
(510) 524-2178
www.peachpit.com
To report errors, please send a note to errata@peachpit.com.
Peachpit Press is a division of Pearson Education.

Apple Series Editor: Lisa McClain
Production Coordinator: Kim Elmore, Happenstance Type-O-Rama
Technical Editor: Andrina Kelly
Apple Reviewer: John Signa
Apple Project Manager: Judy Lawrence
Copy Editor: Jessica Grogan
Proofreader: Jessica Grogan
Compositor: Chris Gillespie, Happenstance Type-O-Rama
Indexer: Jack Lewis
Cover Illustration: Kent Oberheu
Cover Production: Chris Gillespie, Happenstance Type-O-Rama

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.

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 authors 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

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 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: 978-0-321-77508-5   ISBN 10: 0-321-77508-2
9 8 7 6 5 4 3 2 1 Printed and bound in the United States of America

Acknowledgments

We extend a big thank you to all the people at Apple for getting Lion and Lion Server out the door, and of course to Steve Jobs, for inspiring us all.

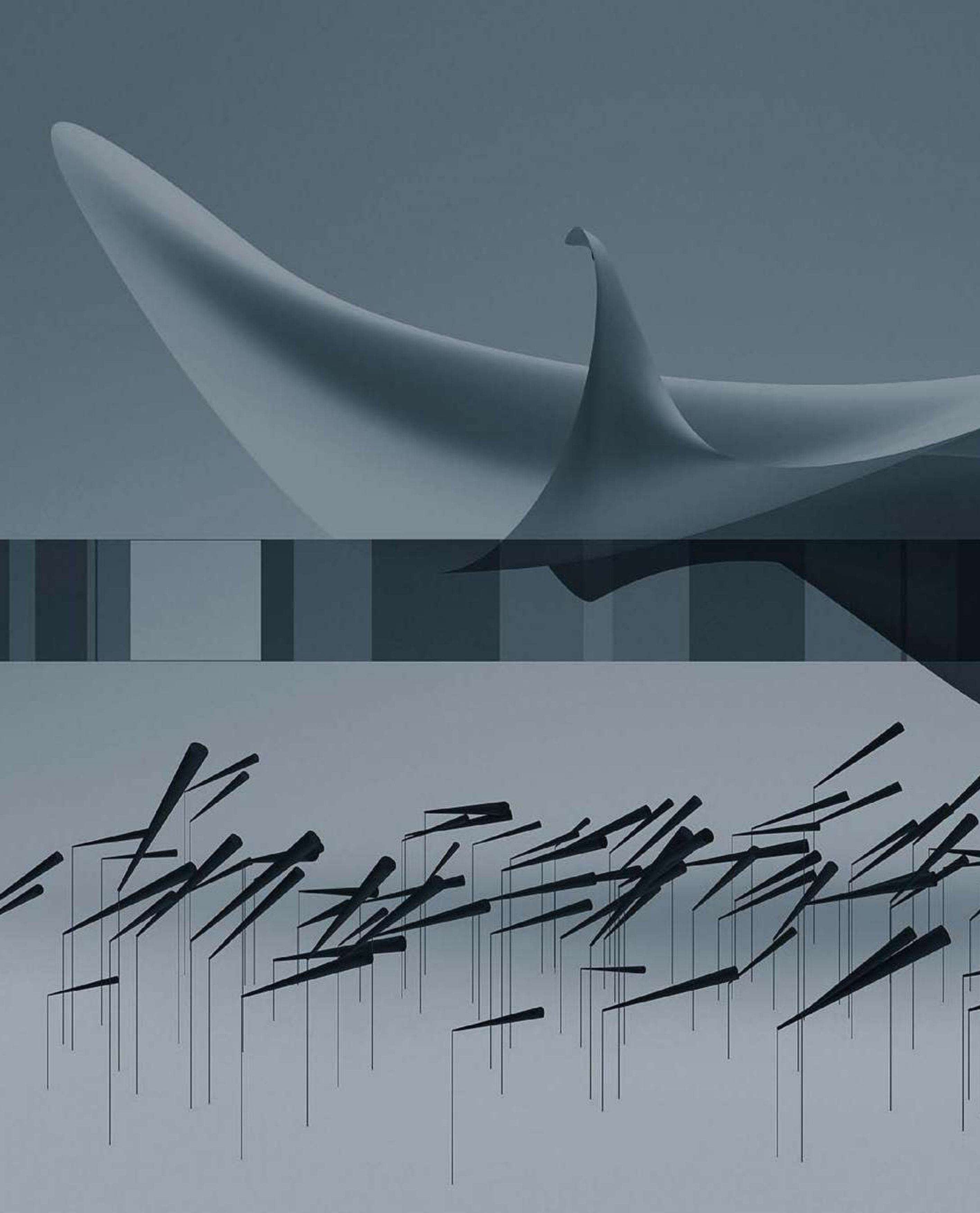
Thanks to the Mac sysadmin community for always striving to better serve your users.

Thanks to Lisa McClain for gently making sure these materials made it into your hands, and to Jessica Grogan and Kim Elmore for working their editorial and production magic.

Thank you, also, to the following people. Without your help, this book would be much less than what it is: David Colville, Gordon Davisson, John DeTroye, Andre LaBranche, Charles Edge, Matthias Fricke, Allen Hancock, Aaron Hix, Eric Hemmeter, Jason Johnson, Adam Karneboge, Andrina Kelly, Ian Kelly, Bob Kite, Judy Lawrence, Chad Lawson, Woody Lidstone, David Long, Tip Lovingood, Duane Maas, Andrew MacKenzie, Jussi-Pekka Mantere, Steve Markwith, Kim Mitchell, Nader Nafissi, Tim Perfitt, Mike Reed, Schoun Regan, Jeremy Robb, John Signa, Chris Silvertooth, David Starr, Kevin White, Simon Wheatley, and Josh Wisenbaker.

Arek Dreyer Thanks to my lovely wife, Heather Jagman, for her love and support.

Ben Greisler My love and appreciation to my wife, Ronit, and my children, Galee and Noam, for supporting me through this project.



Contents at a Glance

Getting Started xi

Chapter 1 Installing and Configuring OS X Lion Server 1

Chapter 2 Authenticating and Authorizing Accounts 85

Chapter 3 Using Open Directory 153

Chapter 4 Managing Accounts 249

Chapter 5 Implementing Deployment Solutions 281

Chapter 6 Providing File Services 315

Chapter 7 Managing Web Services 383

Chapter 8 Using Collaborative Services 405

Index 461

Table of Contents

Getting Started xi

Chapter 1 Installing and Configuring OS X Lion Server 1

Evaluating Lion Server Requirements. 2

Installing Lion Server 3

Configuring an Administrator Computer 15

Initial Lion Server Configuration 20

Using Tools for Monitoring 39

Configuring SSL Certificates 59

Troubleshooting 76

What You've Learned 78

References 80

Chapter Review 81

Chapter 2 Authenticating and Authorizing Accounts 85

Managing Access to Services 86

Creating and Administering User and Administrator Server Accounts 88

Controlling Access With Server Access Control Lists (SACLs) . .116

Configuring Virtual Private Network (VPN) Service 137

Troubleshooting 145

What You've Learned 148

References 149

Chapter Review 150

Chapter 3 Using Open Directory. 153

Introducing Directory Services Concepts. 154

What Is Open Directory? 154

Overview of Open Directory Service Components. 155

Preparing to Configure Open Directory Services 159
Configuring Open Directory Services. 165
Managing Network User Accounts 193
Configuring Authentication Methods on Lion Server 209
Archiving and Restoring Open Directory Data 221
Troubleshooting 233
Preparing DNS Records (Optional) 236
What You've Learned 243
References 244
Chapter Review 246

Chapter 4 Managing Accounts. 249
Introducing Account Management 250
Configuring Profile Manager 251
Managing User, Group, Device, and Device Group Accounts . . 269
Troubleshooting 277
What You've Learned 278
References 278
Chapter Review 279

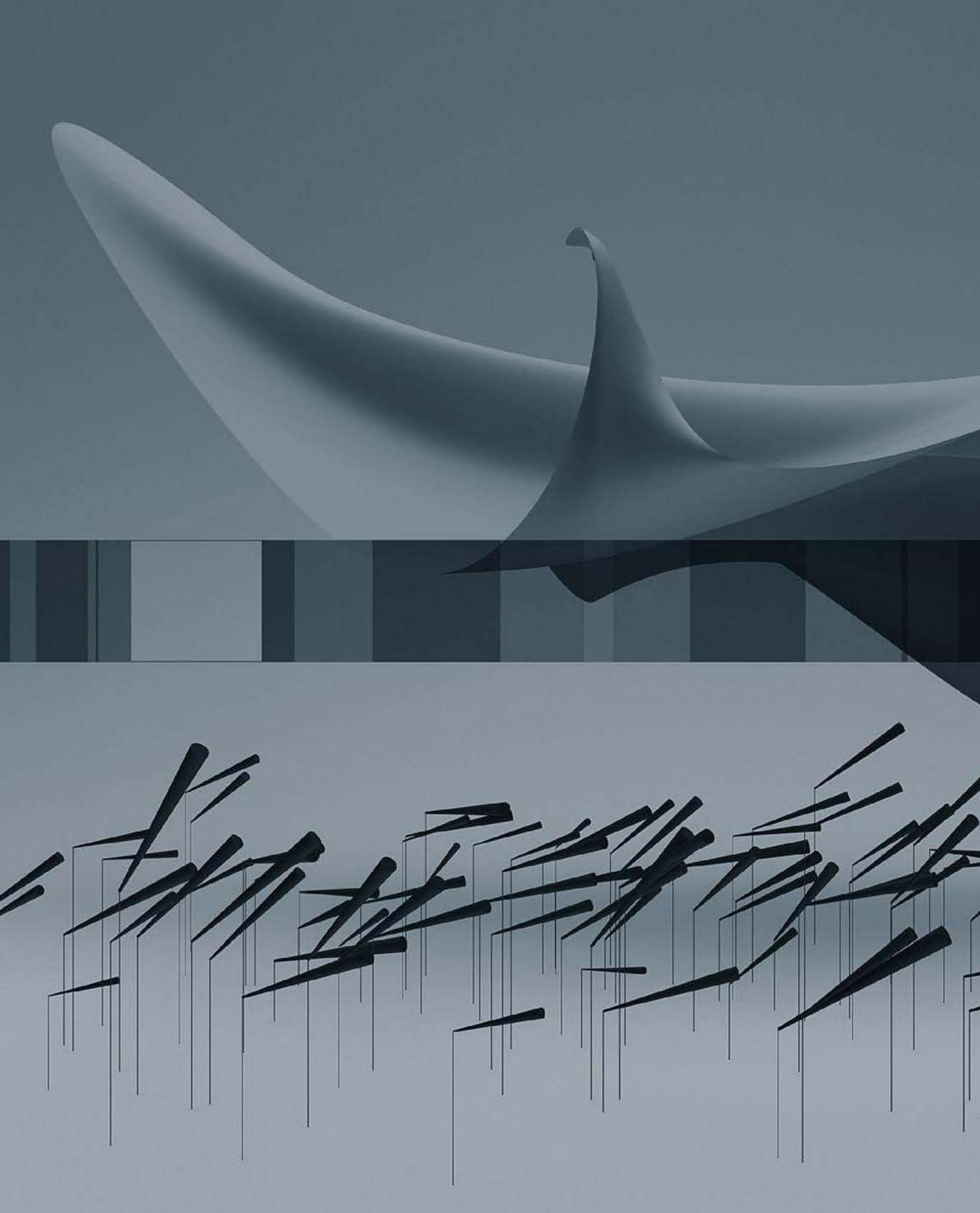
Chapter 5 Implementing Deployment Solutions 281
Deployment Issues 282
Managing Computers with NetBoot. 282
Creating NetBoot Images 290
Specifying a Default Image and Protocol 293
Understanding Shadow Files 294
Configuring a NetBoot Server 296
Configuring a NetBoot Client 299
Configuring NetBoot Images. 300
Configuring NetRestore Images 303
Filtering NetBoot Clients 303
Monitoring NetBoot Clients 305
Troubleshooting NetBoot. 307
Managing Software Updates 308
Troubleshooting Software Update Service 311
What You've Learned 312
References 312
Chapter Review 312

Chapter 6 Providing File Services 315
Addressing the Challenges of File Sharing 316
Creating Share Points 323
Understanding POSIX Ownership, POSIX Permissions, and ACLS. 333
Preparing for a Network Home Folder. 361
Offering Time Machine Services 366
Troubleshooting File Services 374
Cleaning up 376
What You've Learned 377
References 378
Chapter Review 379

Chapter 7 Managing Web Services 383
Understanding Basic Website Concepts 384
Managing Websites 386
Managing Website Access. 393
Securing Your Website 396
Monitoring Web Services 399
Troubleshooting 402
What You've Learned 402
References 403
Chapter Review 403

Chapter 8 Using Collaborative Services 405
Utilizing Administrative Tools. 406
Locating the Data Stores 406
Understanding and Managing a Wiki. 406
Using the iCal Service. 416
Managing the iChat Service 429
Understanding the Address Book Service. 439
Hosting Mail Services. 445
What You've Learned 457
References 458
Chapter Review 458

Index 461



Getting Started

This book is based on the same criteria used for Apple's official training course, Lion 201: OS X Server Essentials 10.7, which provides an in-depth exploration of Lion Server. This book serves as a self-paced tour of the breadth of functionality of Lion Server and the best methods for effectively supporting users of Lion Server systems.

The primary goal of this book is to prepare technical coordinators and entry-level system administrators for the tasks demanded of them by Lion Server; you will learn how to install and configure Lion Server to provide network-based services, such as configuration profile distribution and management, file sharing, authentication, and collaboration services. To become truly proficient, you'll need to learn the theory behind the tools you will use. For example, not only will you learn how to use the Server app—the tool for managing services and accounts—but you will also learn about the ideas behind profile management, how to think about access to and control of resources, and how to set up and distribute profiles to support your environment.

You will learn to develop processes to help you understand and work with the complexity of your system as it grows. Even a single Lion Server computer can grow into a very complicated system, and creating documentation and charts can help you develop processes so that additions and modifications can integrate harmoniously with your existing system.

This book assumes that you have some knowledge of OS X Lion, because Lion Server is built on top of Lion. Therefore, basic navigation, troubleshooting, and networking are all similar regardless of whether the operating system is Lion or Lion Server. This book concentrates on the features that are unique to Lion Server. When working through this book, a basic understanding and knowledge of Lion is preferred, including knowledge of how to troubleshoot the operating system. Refer to *Apple Pro Training Series: OS X Lion Support Essentials* from Peachpit Press if you need to develop a solid working knowledge of Lion.

Unless otherwise specified, all references to Lion and Lion Server refer to version 10.7.2, which was the most current version available at the time of writing. Due to subsequent upgrades, some screen shots, features, and procedures may be slightly different from those presented on these pages.

Learning Methodology

This book is based on lectures and exercises provided to students attending Lion 201: OS X Server Essentials 10.7, a three-day, hands-on course designed to give technical coordinators and entry-level system administrators the skills, tools, and knowledge to implement and maintain a network that uses Lion Server. For consistency, this book follows the basic structure of the course material, but you may complete it at your own pace.

The exercises contained within this book are designed to let you explore and learn the tools necessary to manage Lion Server. They move along in a predictable fashion, starting with the installation and setup of Lion Server and moving to more advanced topics such as performing multiprotocol file sharing, using access control lists, and permitting Lion Server to manage network accounts. If you already have a Lion Server set up, you can skip ahead to some of the later exercises in the book, provided you understand the change in IP addressing from the examples to your server and are not running your server as a production server.

This book serves as an introduction to Lion Server and is not meant to be a definitive reference. Because Lion and Lion Server contain several open source initiatives, it is impossible to include all the possibilities and permutations here. First-time users of Lion Server and users of other server operating systems who are migrating to Lion Server have the most to gain from this book; still, others who are upgrading from previous versions of Lion Server will also find this book a valuable resource.

Lion Server is by no means difficult to set up and configure, but how you use Lion Server should be planned out in advance. Accordingly, this book is divided into eight chapters:

- Chapter 1 covers planning, installation, and initial configuration of Lion Server. It contains an introduction to the various administration tools, and has a focus on SSL (Secure Socket Layer) certificates.
- Chapters 2 and 3 define authentication and authorization, various types of access control, and Open Directory and the vast functionality it can provide.
- Chapter 4 covers managing accounts with the new Profile Manager service.
- Chapter 5 introduces deployment services, including NetBoot and the System Image Utility.
- Chapter 6 introduces the concept of sharing files, associating share points with users and groups, and controlling access to files with Access Control Lists.
- Chapter 7 teaches you how to use the Server app to configure how your server offers web sites.
- Chapter 8 focuses on setting up collaboration services such as mail, web, wiki, calendaring, and instant messaging.

Chapter Structure

Each chapter begins by listing the learning goals for the chapter and providing an estimate of time needed to complete the chapter. The explanatory material is augmented with hands-on exercises essential to developing your skills. If you lack the equipment necessary to complete a given exercise, you are still encouraged to read the step-by-step instructions and examine the screen shots to understand the procedures demonstrated.

WARNING ► The initial exercise in this book requires you to reformat a volume on which you will install Lion Server. All data on this volume will be erased. Once past that point, the majority of the exercises in the book are designed to be nondestructive if followed correctly. However, some of the exercises are disruptive; for example, they may turn off or on certain network services. Other exercises, if performed incorrectly, could result in data loss or corruption to some basic services, possibly even erasing a disk or volume of a computer connected to the network on which Lion Server resides. Thus, it is recommended that you run through the exercises on a Lion Server computer that is not critical to your work or connected to a production network. This is also true of the Lion computer you will use in these exercises. Please back up all your data if you choose to use a production computer for either the Lion Server and/or the Lion computers. Instructions are given for restoring your services to their preset state, but reasonable caution is recommended. Apple, Inc. and Peachpit Press are not responsible for any data loss or any damage to equipment that occurs as a direct or indirect result of following the procedures described in this book.

You'll also find resources that provide ancillary information throughout the chapters. These resources are merely for your edification, and are not essential for the coursework or certification.

Each chapter closes with a list of relevant Apple Knowledge Base articles and recommended documents related to the topic of the chapter. Lion Server documentation (http://www.apple.com/macosx/server/resources/) and Knowledge Base articles (http://www.apple.com/support) are free resources that contain the very latest technical information on all of Apple's hardware and software products. We strongly encourage you to read the suggested documents and search the Knowledge Base for answers to any problems you encounter.

Finally, at the end of each chapter is a short chapter review that recaps the material you've learned. You can refer to various Apple resources, such as the Knowledge Base, and Lion Server documentation, as well as the chapters themselves, to help you answer these questions.

System Requirements

This book assumes a basic level of familiarity with Lion. All references to Lion and Lion Server refer to v10.7.2, unless otherwise stated.

Here's what you will need to complete the lessons in the book:

- Two Macintosh computers, one with Lion installed and one on which you will install Lion Server
- An Ethernet switch to keep the two computers connected via a small private local network
- Two Ethernet network cables for connecting both computers to the switch
- A router (preferably an AirPort base station) to connect the small private network to the Internet, so you can obtain Apple Push Notification service (APNs) certificates for the Profile Manager service
- Optionally, a wireless access point (preferably an AirPort base station) to provide wireless access for iOS devices to your private network
- Optionally, three additional Macintosh computers on which to install Lion Server and configure as: an Open Directory replica; a member server; and a bound server on which to import users.

Apple Certification

After reading this book, you may wish to take the OS X Server Essentials 10.7 Exam. Passing both this exam and the OS X Support Essentials 10.7 Exam earns Apple Certified Technical Coordinator 10.7 (ACTC) certification. This is the second level of Apple's certification program for Mac professionals, which includes:

- Apple Certified Support Professional 10.7 (ACSP)—Ideal for help desk personnel, service technicians, technical coordinators, and others who support OS X Lion customers over the phone or who perform Mac troubleshooting and support in schools and businesses. This certification verifies an understanding of Lion's core functionality and an ability to configure key services, perform basic troubleshooting, and assist end users with essential Mac capabilities. To receive this certification, you must pass the OS X Support Essentials 10.7 Exam. This book is designed to provide you with the knowledge and skills to pass that exam.

- Apple Certified Technical Coordinator 10.7 (ACTC)—This certification is intended for Lion technical coordinators and entry-level system administrators tasked with maintaining a modest network of computers using Lion Server. Since the ACTC certification addresses both the support of Mac clients and the core functionality and use of Lion Server, the learning curve is correspondingly longer and more intensive than that for the ACSP certification, which addresses solely Mac client support. This certification requires passing both the OS X Support Essentials 10.7 Exam and OS X Server Essentials 10.7 Exam.

  NOTE ▶ Although all of the questions in the OS X Server Essentials 10.7 Exam are based on material in this book, simply reading it will not adequately prepare you for the exam. Apple recommends that before taking the exam you spend time setting up, configuring, and troubleshooting Lion Server.

Apple hardware service technician certifications are ideal for people interested in becoming Macintosh repair technicians, but also worthwhile for help desk personnel at schools and businesses, and for Macintosh consultants and others needing an in-depth understanding of how Apple systems operate.

- Apple Certified Macintosh Technician (ACMT)—This certification verifies the ability to perform basic troubleshooting and repair of both desktop and portable Macintosh systems, such as iMac and MacBook Pro. ACMT certification requires passing the Apple Macintosh Service Exam and the Lion Troubleshooting Exam. To learn more about hardware certification, visit http://training.apple.com/certification/acmt.

About the Apple Training Series

Apple Pro Training Series: OS X Lion Server Essentials is part of the official training series for Apple products developed by experts in the field and certified by Apple. The chapters are designed to let you learn at your own pace. You can progress through the book from beginning to end, or dive right into the chapters that interest you most.

For those who prefer to learn in an instructor-led setting, training courses are offered at Apple Authorized Training Centers worldwide. These courses are taught by Apple Certified Trainers, and they balance concepts and lectures with hands-on labs and exercises. Apple Authorized Training Centers have been carefully selected and have met Apple's highest standards in all areas, including facilities, instructors, course delivery, and infrastructure. The goal of the program is to offer Apple customers, from beginners to the most seasoned professionals, the highest-quality training experience.

To find an Authorized Training Center near you, please visit http://training.apple.com.

4

Time

This chapter takes approximately three hours to complete.

Goals

Configure Profile Manager

Construct management profiles

Deliver profiles

Install and delete profiles

Manage users, groups of users, devices, and groups of devices using profiles

Chapter 4

Managing Accounts

If you run an organization with several hundred users or even just a handful, how can you make sure you can manage their experience with OS X and iOS? In previous chapters you learned management techniques involving the user name, password, and home folder. There are many other aspects to user account management, and it is important to understand how these various aspects interact with each other.

OS X Lion Server provides a service called Profile Manager that allows you, as the administrator, to assign certain behaviors to the client devices such as computers and mobile devices.

Introducing Account Management

Account management was controlled by Workgroup Manager in Mac OS X 10.6 and earlier, but Lion introduces the concept of profiles that contain configurations and settings. By assigning profiles to users, user groups, devices, or groups of devices you can achieve control over your systems.

With effective account management, you can achieve a range of results, including the following:

- Providing users with a consistent, controlled interface
- Controlling settings on mobile devices and computers
- Restricting certain resources for specific groups or individuals
- Securing computer use in key areas such as administrative offices, classrooms, or open labs
- Customizing the user experience
- Customizing Dock settings

Profile Manager

Profile Manager is an account management tool that allows the development and distribution of configurations and settings to control the experience on Lion computers and iOS devices. The configurations and settings are contained in XML based text files called profiles. Profile Manager has three parts:

1. Profile Manager web tool
2. User Portal web site
3. Mobile Device Management Server

Profile Manager Web App

The web tool allows easy access to the Profile Manager functionality from any browser that can connect to the Lion Server with the Profile Manager service turned on. An administrator can utilize the web interface to create profiles for use on client machines. It is also used to create and manage device accounts and device group accounts. Users and Groups are created in the Server app, but are displayed in the Profile Manager web app. The Profile Manager is reached at https://*server.domain.com*/profilemanager/.

User Portal

The User Portal is a simple way for users to enroll devices, obtain profiles, and wipe or lock their devices. The User Portal is accessed via a web browser and lists the user's enrolled devices and available profiles. It is reached at https://*server.domain.com*/mydevices/.

Device Management

You can configure and enable the Mobile Device Management (MDM) functionality to allow you to create profiles for devices. When you or your users enroll Lion computers and iOS 4 or later devices, this allows over the air (OTA) management of devices including remote wipe and lock.

Levels of Management

Using Profile Manager you can apply profiles at various levels including:

- Individual Users
- Groups of Users
- Devices
- Device Groups

Not all management levels make sense for all purposes, so when setting policy you have to decide what is appropriate. For example, you might want to define printers by device groups, because a typical situation has a group of computers located geographically close to a specific printer. You may want to set VPN access via a group of users such as remote salespeople. And individuals might have specific application access rights granted to them.

Each level can have a default group of settings and then custom settings. Mixing and layering profiles with conflicting settings is not recommended.

Configuring Profile Manager

To allow assigning profiles, the Profile Manager service must be enabled. Using profiles is significantly different than managing clients in earlier versions of OS X Server. Note that the older method of using Workgroup Manager is still valid in Lion Server, but this book doesn't approach it. For information on OS X Managed Client , see Chapter 9, "Managing Accounts," in the book *Apple Training Series: Mac OS X Server Essentials v10.6*.

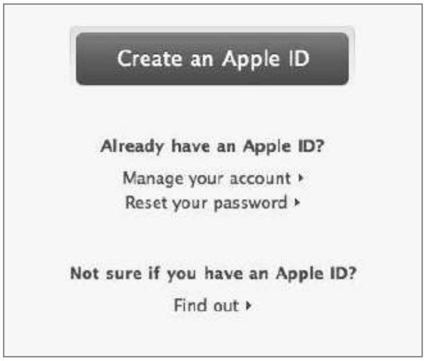
Terminology

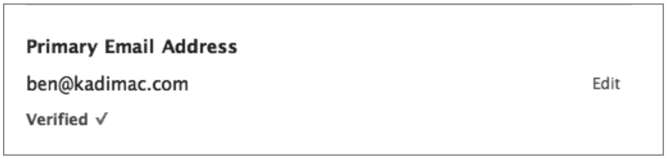
In the context of device management, a Profile is basically a collection of settings. Configuration profiles define settings such as Wi-Fi settings, email accounts, calendar accounts, and security policies. Enrollment profiles allow the server to manage your device. A payload is what's inside a profile.

Preparations for Profile Manager

Prior to configuring Profile Manager, you'll need to set up a few items to make the process more streamlined.

- Configure your server to manage network users and groups. This is also referred to as creating an Open Directory Master.
- Obtain and install an SSL certificate. It is recommended to use one signed by a trusted certificate authority. You could use the certificate that was automatically generated when you configured your server to manage network accounts, but you first need to configure devices to trust that certificate. If you instead use your self-signed certificate, you won't be able to enroll iOS devices.
- Obtain an Apple ID for use when you request a push certificate from Apple through the http://appleid.apple.com website. Prior to using this ID, make sure you log in at that site under "Manage My Account" and verify the address. Otherwise, it is possible that you won't have success requesting the push certificate.




Primary Email Address

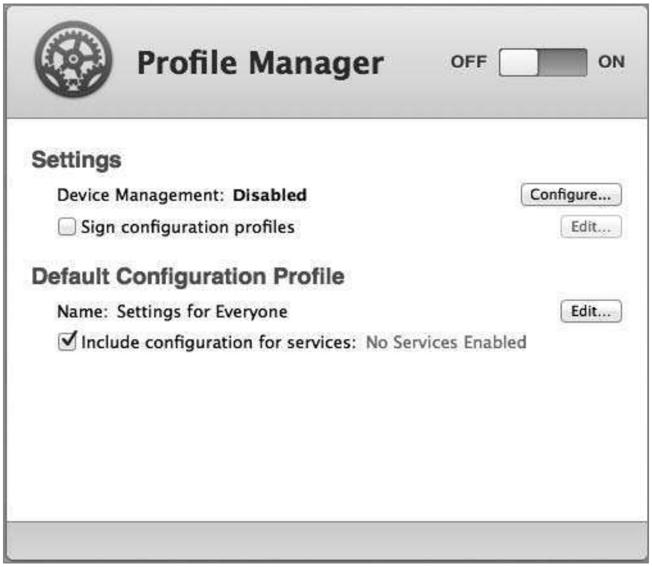
ben@kadimac.com

Verified ✓

Enabling Profile Manager

In this section, you'll go through the steps to enable Profile Manager including the signing of a configuration profile.

1 Open Server app and select Profile Manager in the Server app sidebar.



Settings

Device Management: **Disabled** Configure...

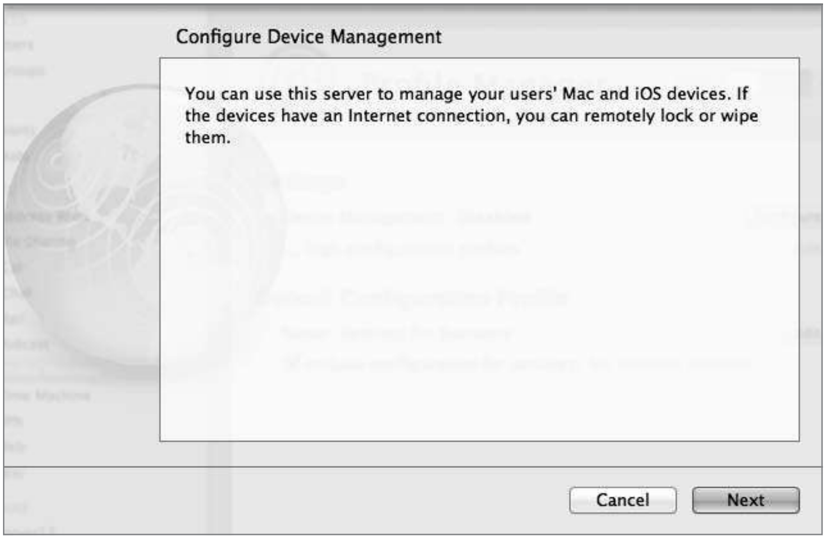
□ Sign configuration profiles Edit...

Default Configuration Profile

Name: Settings for Everyone Edit...

☑ Include configuration for services: No Services Enabled

2 Click Configure, next to Device Management.

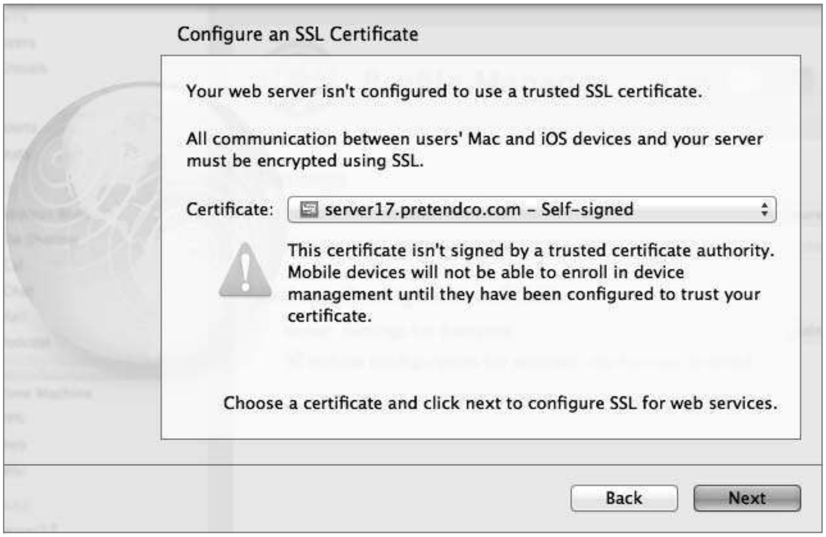


Configure Device Management

You can use this server to manage your users' Mac and iOS devices. If the devices have an Internet connection, you can remotely lock or wipe them.

3 The service will gather some data and give a description of its capabilities. Click Next.

4 Choose your certificate. If you use your self-signed certificate, you will not be able to enroll any iOS devices.



Configure an SSL Certificate

Your web server isn't configured to use a trusted SSL certificate.

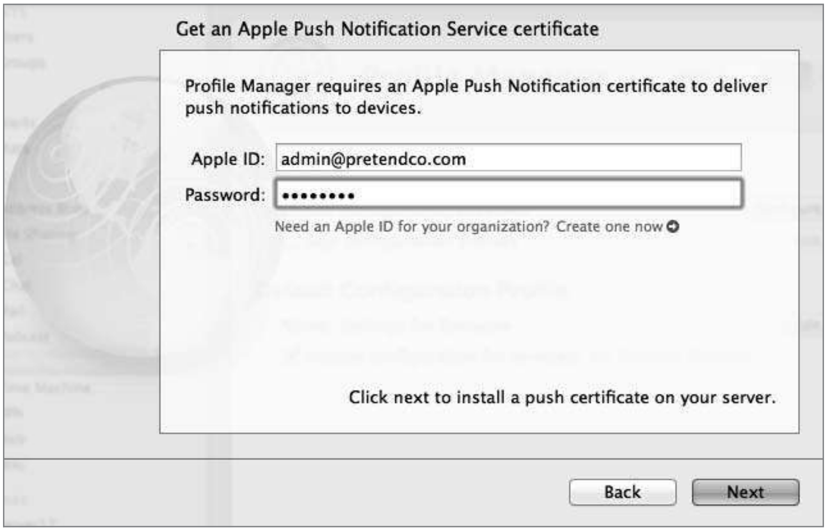
All communication between users' Mac and iOS devices and your server must be encrypted using SSL.

Certificate: server17.pretendco.com – Self-signed

This certificate isn't signed by a trusted certificate authority. Mobile devices will not be able to enroll in device management until they have been configured to trust your certificate.

Choose a certificate and click next to configure SSL for web services.

5 Request an Apple Push Notification certificate using an Apple ID. If you do not have one, there's a link to obtain one under the credential fields. Make sure to verify the address at the http://appleid.apple.com site. Click Next.



Get an Apple Push Notification Service certificate

Profile Manager requires an Apple Push Notification certificate to deliver push notifications to devices.

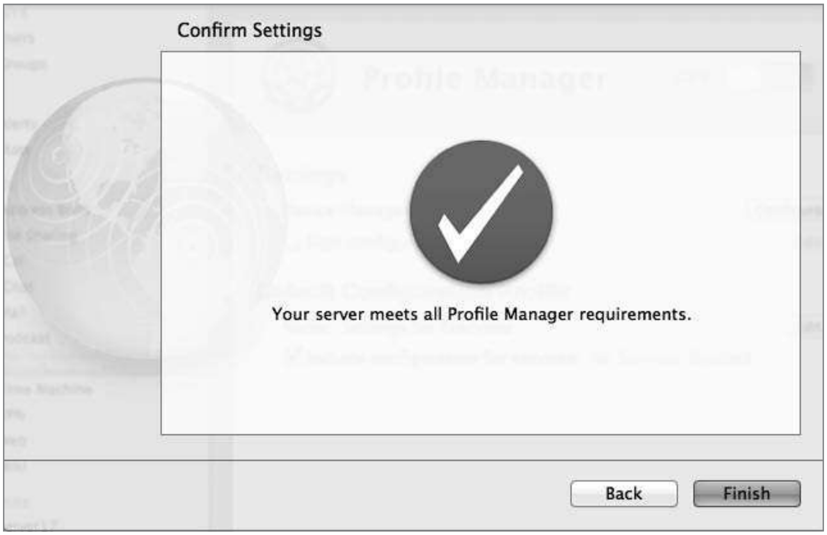
Apple ID: admin@pretendco.com

Password: ••••••••

Need an Apple ID for your organization? Create one now

Click next to install a push certificate on your server.

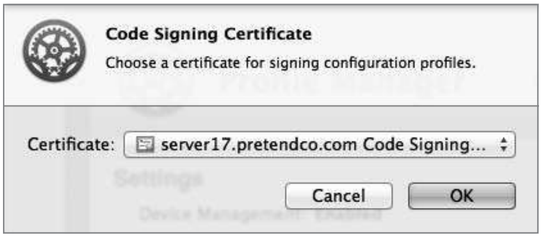
6 A green circle will indicate that you succeeded. Click Finish.



Confirm Settings

Your server meets all Profile Manager requirements.

7 Select the checkbox labeled "Sign configuration profiles," then choose the Code Signing certificate that was created when you created your network accounts.



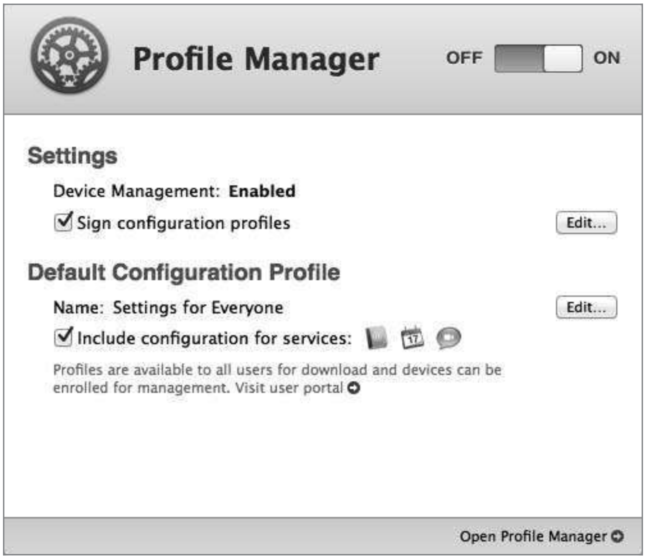
Code Signing Certificate

Choose a certificate for signing configuration profiles.

Certificate: server17.pretendco.com Code Signing...

By signing the profiles with a certificate, you provide a way to validate that the profiles came from where they are supposed to be from.

8 If you don't have any services running, use this time to configure and activate a few services, then click the On/Off switch to turn on Profile Manager.



Settings

Device Management: **Enabled**

☑ Sign configuration profiles

Default Configuration Profile

Name: Settings for Everyone

☑ Include configuration for services:

Profiles are available to all users for download and devices can be enrolled for management. Visit user portal

User Profile Portal

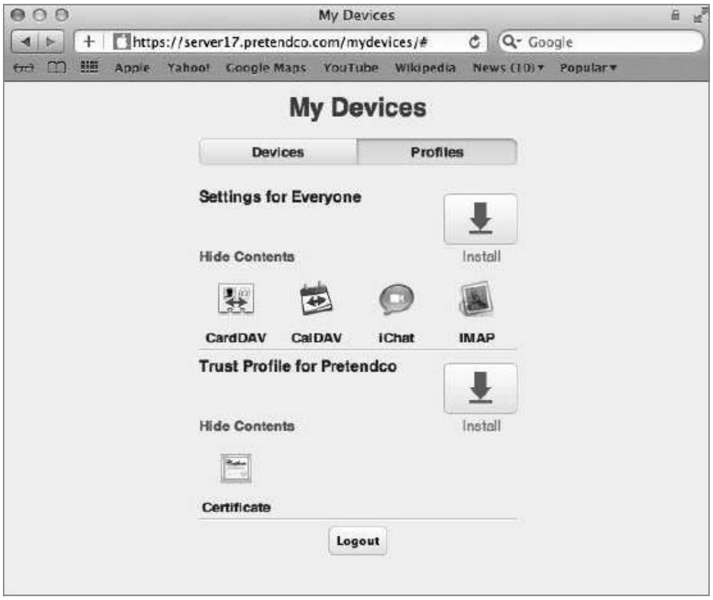
The User Profile Portal provides simple access for users to log in, apply profiles, and manage their devices. The portal is accessed via a web browser; by simply publishing the website, users anywhere in the world can enroll their devices–whether they be computers, iPhones or other iOS based mobile devices. It is through the portal that a user can lock or wipe their enrolled devices.

> **NOTE ►** The example below is for OS X, but the iOS version is conceptually and visually similar.

1 Navigate to the site https://server17.pretendco.com/mydevices.

2 Through a series of redirects the user will be prompted for her credentials to log in.

3 The user is given tabs for Devices and Profiles. Devices is where the user can enroll the device. Profiles is where the various profiles made available to her will be displayed.


My Devices
https://server17.pretendco.com/mydevices/#
Google
Apple Yahoo! Google Maps YouTube Wikipedia News (10) Popular

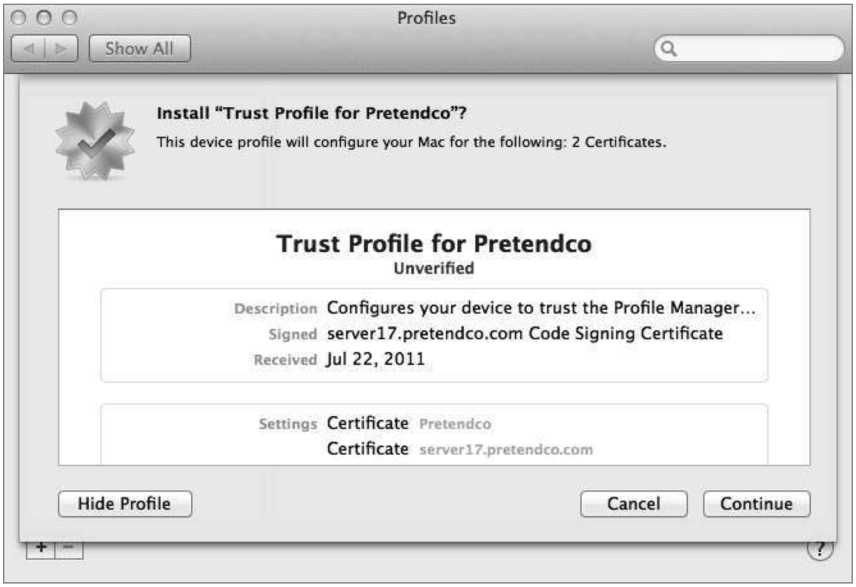
My Devices

Settings for Everyone

Trust Profile for Pretendco

4 Click the Install Trust Profile. The profile will be downloaded, and the Profiles preferences will appear.

5 Click the Show Profile button to view the contents of the profile, then click Continue.



Install "Trust Profile for Pretendco"?

This device profile will configure your Mac for the following: 2 Certificates.

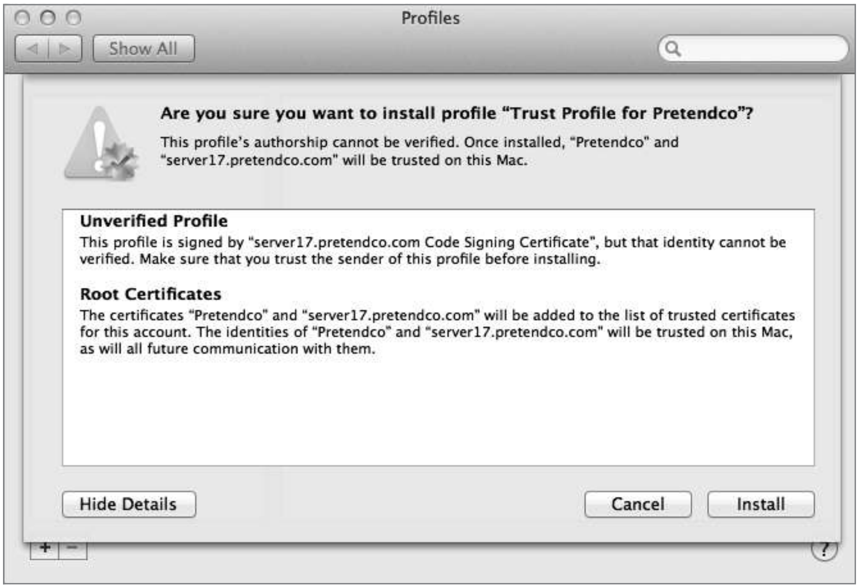
Trust Profile for Pretendco

Unverified

Description Configures your device to trust the Profile Manager…
Signed server17.pretendco.com Code Signing Certificate
Received Jul 22, 2011

Settings Certificate Pretendco
Certificate server17.pretendco.com

6 In the next window click Show Details to view more information regarding the certificates involved, and then click Install. Enter an administrator's credentials when prompted.



Are you sure you want to install profile "Trust Profile for Pretendco"?

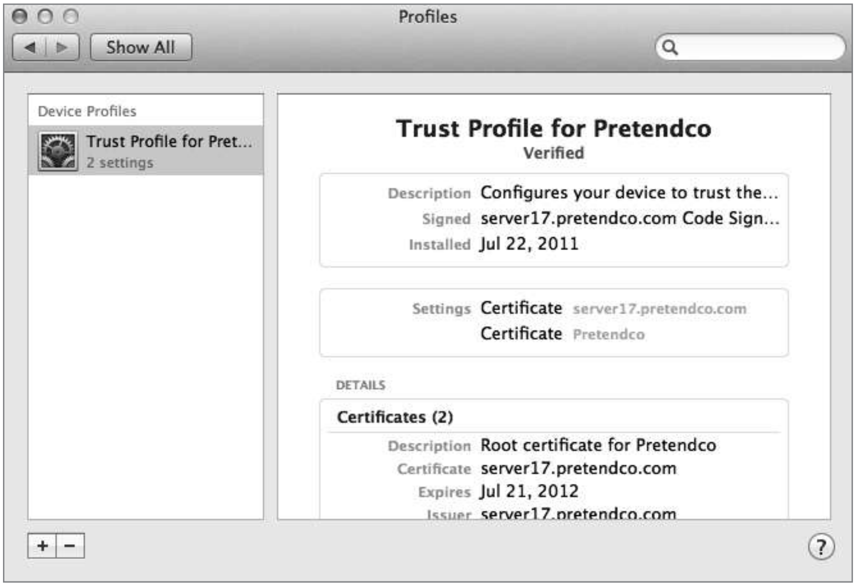
This profile's authorship cannot be verified. Once installed, "Pretendco" and "server17.pretendco.com" will be trusted on this Mac.

Unverified Profile

This profile is signed by "server17.pretendco.com Code Signing Certificate", but that identity cannot be verified. Make sure that you trust the sender of this profile before installing.

Root Certificates

The certificates "Pretendco" and "server17.pretendco.com" will be added to the list of trusted certificates for this account. The identities of "Pretendco" and "server17.pretendco.com" will be trusted on this Mac, as will all future communication with them.



Trust Profile for Pret...
2 settings

Trust Profile for Pretendco
Verified

Description Configures your device to trust the...
Signed server17.pretendco.com Code Sign...
Installed Jul 22, 2011

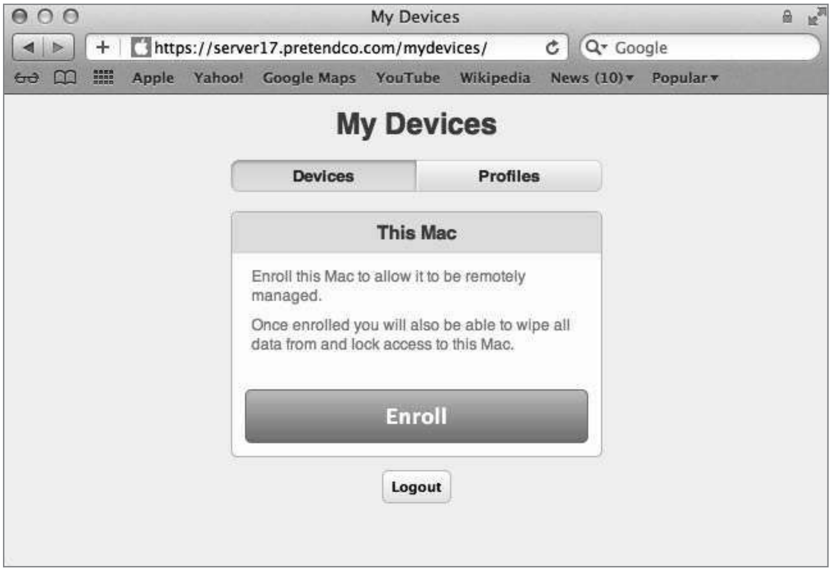
Settings Certificate server17.pretendco.com
Certificate Pretendco

DETAILS

Certificates (2)

Description Root certificate for Pretendco
Certificate server17.pretendco.com
Expires Jul 21, 2012
Issuer server17.pretendco.com

7 Navigate to the Devices tab and click Enroll. You will be brought back to the Profile preferences and asked if you want to enroll. View the profile and then click Install.

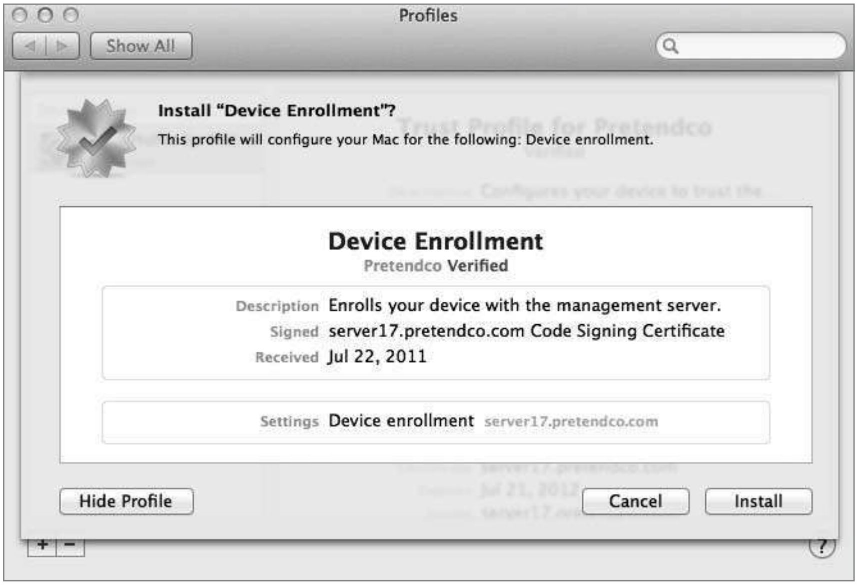


My Devices

This Mac

Enroll this Mac to allow it to be remotely managed.

Once enrolled you will also be able to wipe all data from and lock access to this Mac.



Install “Device Enrollment”?

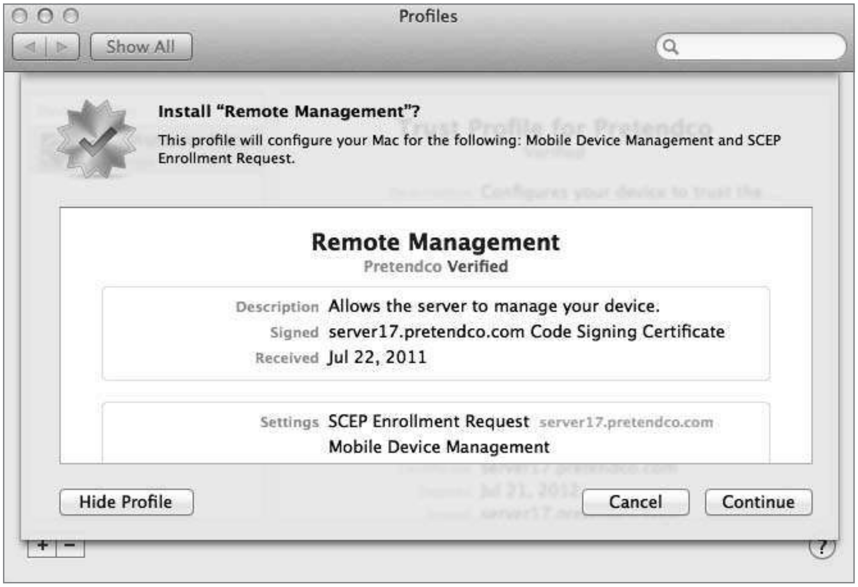
This profile will configure your Mac for the following: Device enrollment.

Device Enrollment

Pretendco Verified

Description	Enrolls your device with the management server.
Signed	server17.pretendco.com Code Signing Certificate
Received	Jul 22, 2011
Settings	Device enrollment server17.pretendco.com

8 In the next screen, you will be asked to install Remote Management which allows the server to manage that machine. View the profile and click Continue. Enter an administrator’s credentials when prompted.



Install “Remote Management”?

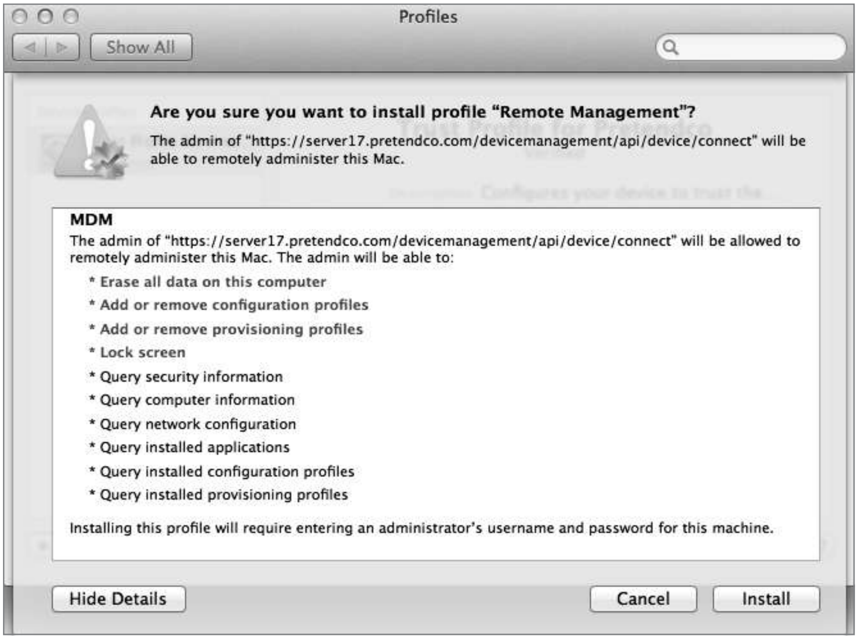
This profile will configure your Mac for the following: Mobile Device Management and SCEP Enrollment Request.

Remote Management

Pretendco **Verified**

Description Allows the server to manage your device.
Signed server17.pretendco.com Code Signing Certificate
Received Jul 22, 2011

Settings SCEP Enrollment Request server17.pretendco.com
Mobile Device Management



Are you sure you want to install profile “Remote Management”?

The admin of “https://server17.pretendco.com/devicemanagement/api/device/connect” will be able to remotely administer this Mac.

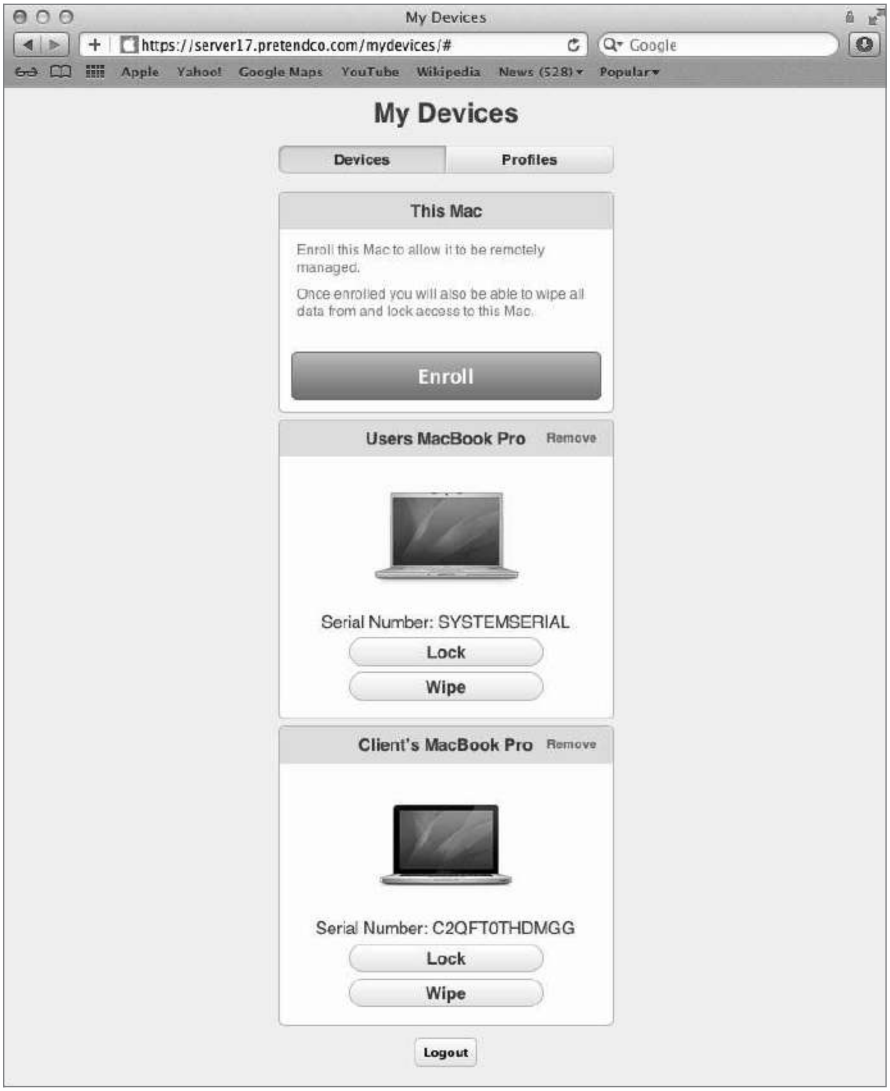
MDM

The admin of “https://server17.pretendco.com/devicemanagement/api/device/connect” will be allowed to remotely administer this Mac. The admin will be able to:

- Erase all data on this computer
- Add or remove configuration profiles
- Add or remove provisioning profiles
- Lock screen
- Query security information
- Query computer information
- Query network configuration
- Query installed applications
- Query installed configuration profiles
- Query installed provisioning profiles

Installing this profile will require entering an administrator’s username and password for this machine.

9 Now that the profile has been installed on the computer, refresh the view in the browser and notice that the computer is now listed under the Devices tab with choices to Lock or Wipe the computer. This allows the user to utilize any modern web browser to control those aspects of the computer remotely, if the machine were to get lost or stolen.



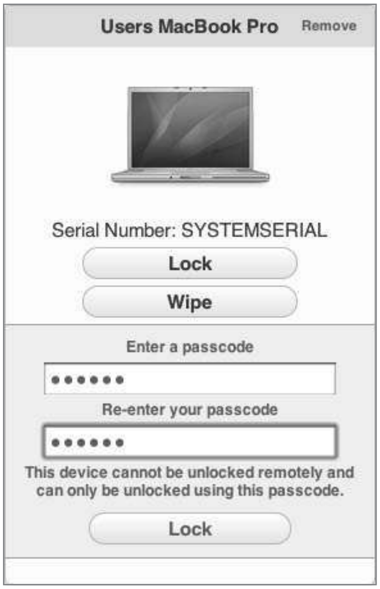
Enroll this Mac to allow it to be remotely managed.

Once enrolled you will also be able to wipe all data from and lock access to this Mac.

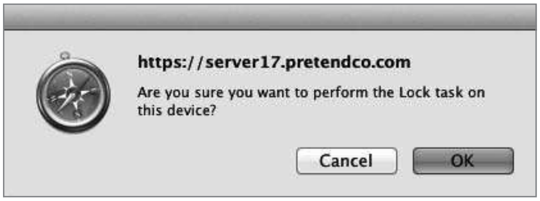
Serial Number: SYSTEMSERIAL

Serial Number: C2QFT0THDMGG

10 To lock the remote device, navigate to the site https://server17.pretendco.com/mydevices on a different computer and log in. Choose your test computer and lock it by clicking the Lock button and entering a 6 digit passcode. Click the Lock button again, and a confirmation box will appear. Once the confirmation has been given, the remote computer will reboot and then offer a dialog to unlock the machine via the passcode.



This device cannot be unlocked remotely and can only be unlocked using this passcode.



https://server17.pretendco.com

Are you sure you want to perform the Lock task on this device?

Managing Profiles Locally

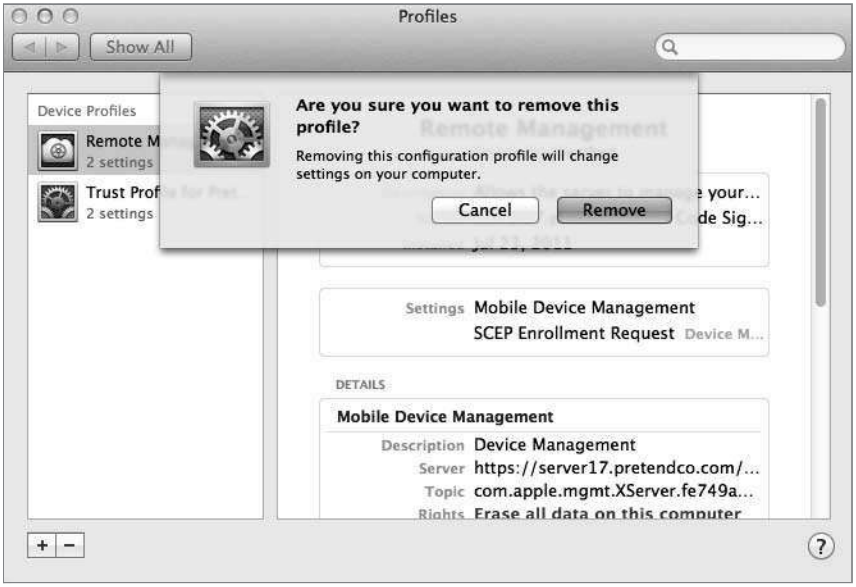
Occasionally a profile will need to be viewed, added, or removed to make way for an updated profile or to simply stop management of the device. Managing the profiles local to a computer is done via the Profiles preference pane located in System Preferences. You added a profile to the computer in the previous exercise and now you will remove one.

To remove a profile local to an OS X computer:

1 Open the Profiles preference pane in System Preferences. The various profiles installed on the computer are listed along with their contents and purposes.

2 Pick the profile you wish to remove such as the remote management profile and click the Remove (-) button.

3 A confirmation dialog box will appear. Click Remove. Enter a local administrator's credentials, if prompted, and click OK.



Are you sure you want to remove this profile?

Removing this configuration profile will change settings on your computer.

Settings Mobile Device Management
SCEP Enrollment Request Device M…

Mobile Device Management
Description Device Management
Server https://server17.pretendco.com/…
Topic com.apple.mgmt.XServer.fe749a…
Rights Erase all data on this computer

To remove a profile local to an iOS device:

1 Navigate to Settings/General/Profiles.

2 Tap the profile to show the details.

3 Tap the Remove button.

4 Confirm the removal by tapping the Remove button on the confirmation box.

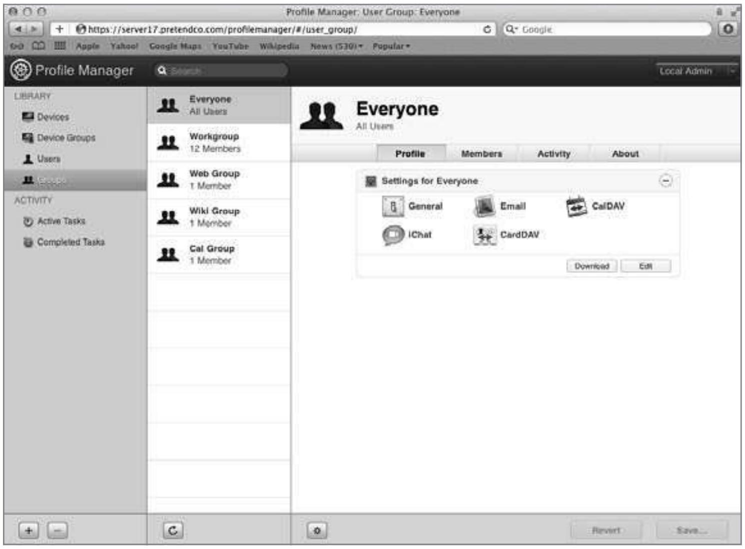
5 Exit Settings.

Using Profile Manager

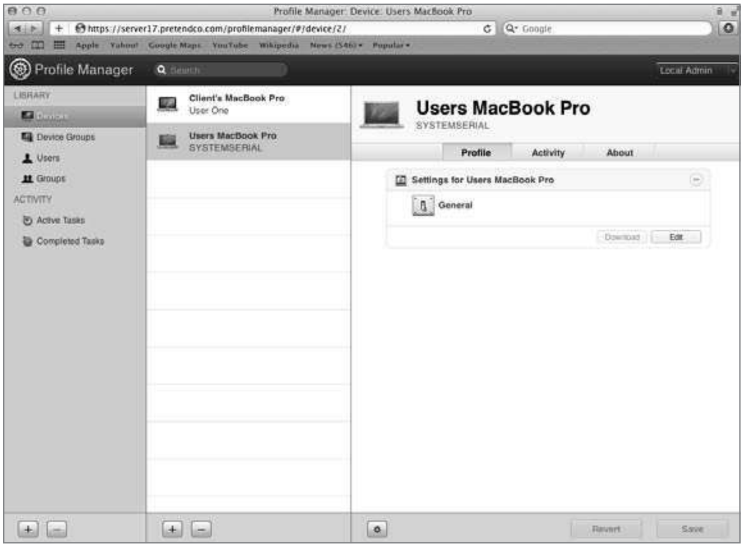
Once Profile Manager has been turned on, you access the actual management interface via a web application. The web application can be reached via web browser on any machine.

1 Navigate to the site https://server17.pretendco.com/profilemanager.

2 Log in to the Profile Manager web app with an administrator's credentials.

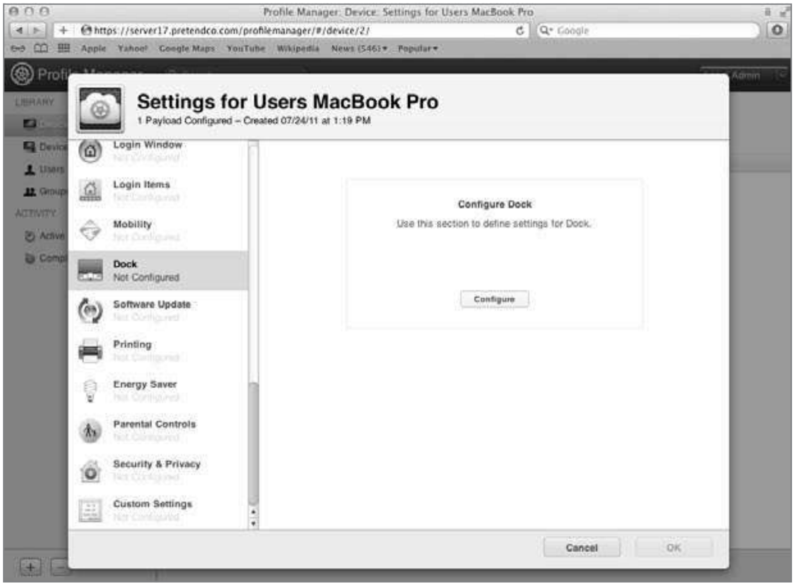


3 The layout is a column view where the selection made in the left column defines the content of the column to the right. Click on Devices under the Library and click an enrolled computer.



4 In the computers information pane, click Profile and then click Edit under Settings.

5 In the new window that opens, scroll down the list to the Mac OS X section, noting that there are sections for iOS and combined iOS and Mac OS X. Click Dock and then click Configure.



Profile Manager: Device: Settings for Users MacBook Pro

https://server17.pretendco.com/profilemanager/#/device/2/

Settings for Users MacBook Pro

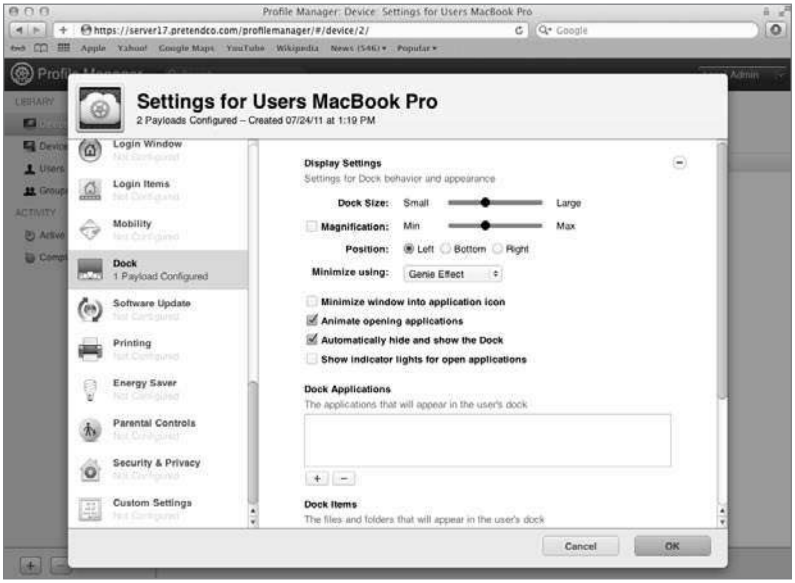
1 Payload Configured – Created 07/24/11 at 1:19 PM

Dock
Not Configured

Configure Dock

Use this section to define settings for Dock.

6 Change the settings to place the Dock on the Left and to automatically hide and show the Dock.



Profile Manager: Device: Settings for Users MacBook Pro

https://server17.pretendco.com/profilemanager/#/device/2/

Settings for Users MacBook Pro

2 Payloads Configured – Created 07/24/11 at 1:19 PM

Dock
1 Payload Configured

Display Settings

Settings for Dock behavior and appearance

Dock Size: Small ——●—— Large

□ Magnification: Min ——●—— Max

Position: ● Left ○ Bottom ○ Right

Minimize using: Genie Effect

□ Minimize window into application icon

☑ Animate opening applications

☑ Automatically hide and show the Dock

□ Show indicator lights for open applications

Dock Applications

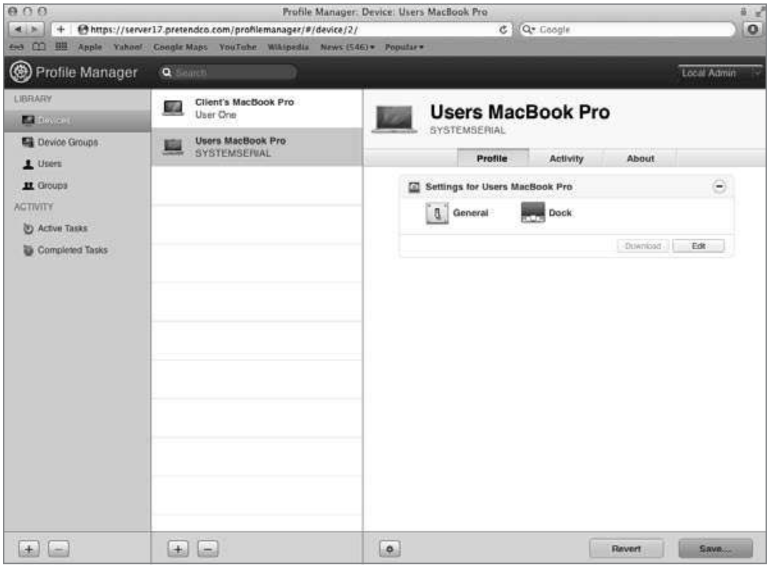
The applications that will appear in the user's dock

Dock Items

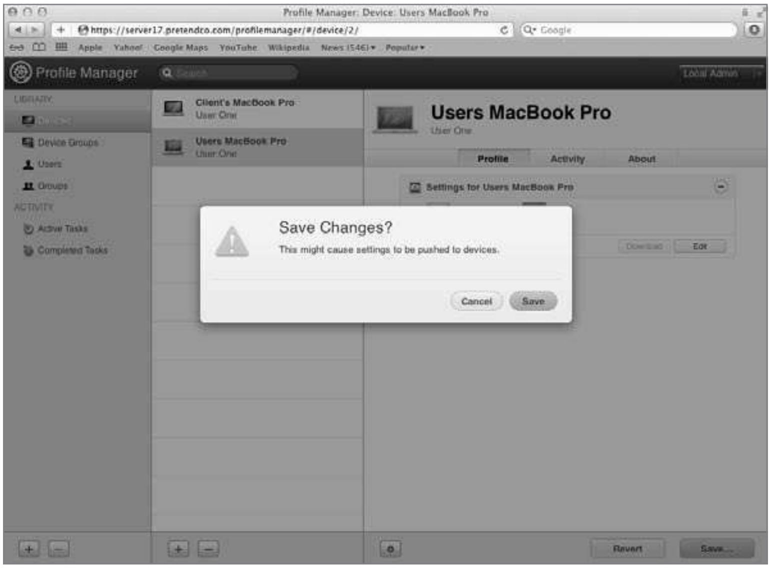
The files and folders that will appear in the user's dock

7 Scroll back to the top of the list in the left column and choose General. Under Profile Distribution Type select Manual Download. Click OK.

8 Note that the Dock preference is indicated in the settings for the computer. Click Save.



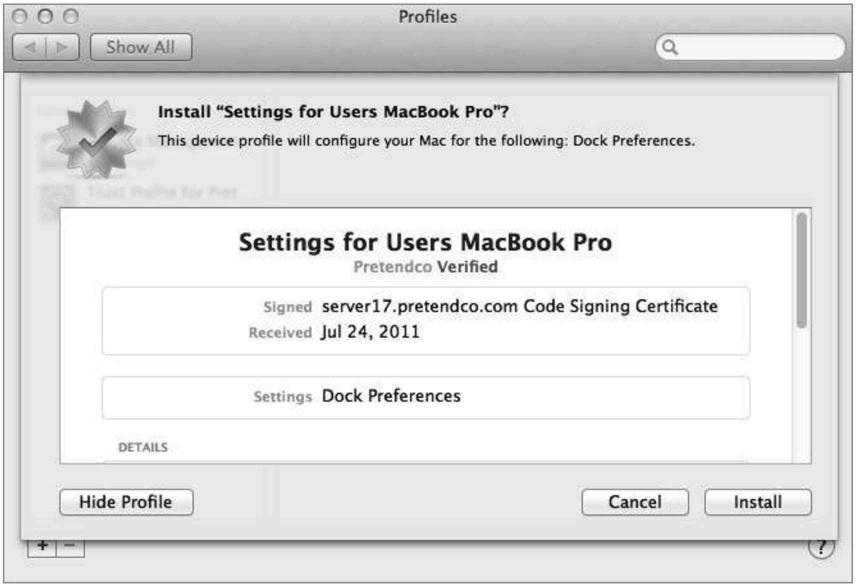
9 A warning that new settings might be pushed to the managed devices is presented. Click Save.


Save Changes?

This might cause settings to be pushed to devices.

10 Under the Settings for the computer, click the Download button. A copy of the preferences is stored in the profile that has been downloaded to the machine Profile Manager is running on. Open the profile in TextEdit.app and view the contents. The profile is simply an XML text file.

11 Copy the file to your client computer and double-click on it to install. Choose Show Profile to view the contents of the profile.



Install "Settings for Users MacBook Pro"?

This device profile will configure your Mac for the following: Dock Preferences.

Settings for Users MacBook Pro

Pretendco Verified

Signed server17.pretendco.com Code Signing Certificate

Received Jul 24, 2011

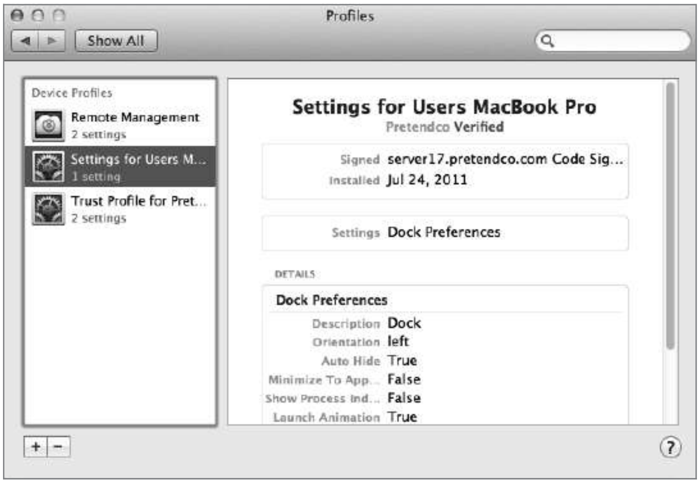
Settings Dock Preferences

DETAILS

12 Click Install and enter the local administrators password.

13 Log out and log back in. Notice the Dock is now hidden on the left side.

14 Open the Profiles preference pane in System Preferences. View the new profile. Remove the profile by clicking the Remove (-) button at the bottom of the left column. Acknowledge the removal and enter a local administrator's credentials. Upon logging out and back in, the original Dock location and behavior will be restored.



Device Profiles

Remote Management
2 settings

Settings for Users M...
1 setting

Trust Profile for Pret...
2 settings

Settings for Users MacBook Pro
Pretendco Verified

Signed server17.pretendco.com Code Sig...
Installed Jul 24, 2011

Settings Dock Preferences

DETAILS

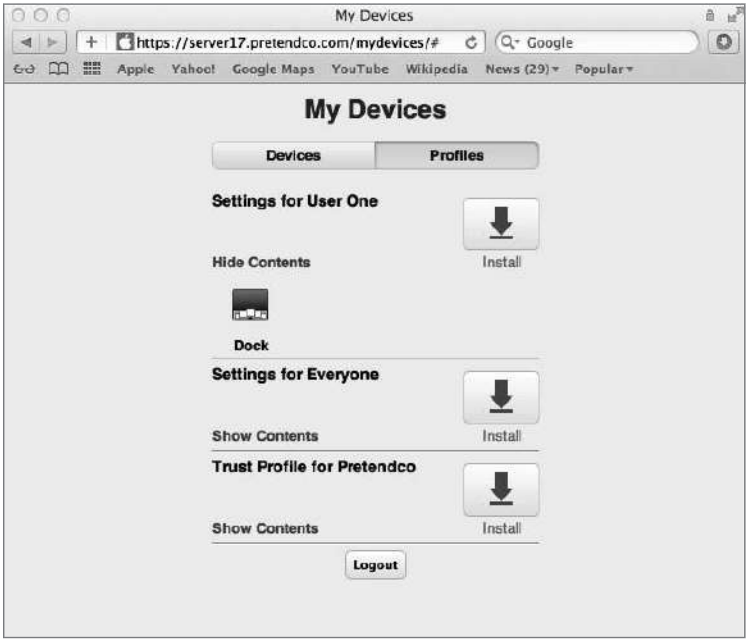
Dock Preferences

Description	Dock
Orientation	left
Auto Hide	True
Minimize To App...	False
Show Process Ind...	False
Launch Animation	True

Delivering Profiles

Once created, profiles can be delivered to users and computers or iOS devices in a number of ways:

- Via the User Portal where users log in to the portal with their account credentials and they are presented with the profiles assigned to them.



My Devices

Settings for User One

Hide Contents

Dock

Settings for Everyone

Show Contents

Trust Profile for Pretendco

Show Contents

- Emailed to users. The profile is a simple text file, so it is easily transported.
- Web link. The profile can be published on a website for users to visit and download.
- Automatic Push. The profile gets automatically pushed to the device with no user interaction (the device must be enrolled for this to work).

Remotely Locking or Wiping a Device

Once enrolled, a device or group of devices can be remotely locked or wiped. In this example, a remote lock will be performed. A remote wipe can be attempted, but only do it on a device you don't mind reconfiguring. The device can be locked via Profile Manager by an administrator or via the User Portal by the users themselves.

Upon requesting a lock, a confirmation pane will appear, a passcode will be requested, and the lock command will be sent. On Lion computers, the machine is shut down and an EFI passcode is set, so it needs to be entered to use the machine again. For iOS devices, the screen is locked and the passcode enforced.

- Profile Manager: Log into Profile Manager and select the device or group of devices to be locked. In the Action (gear) menu at the bottom of the right pane choose Lock.
- User Portal: Once users log in, each device they enrolled will be displayed in the Devices.

Managing User, Group, Device, and Device Group Accounts

You can create settings for four different types of accounts:

- User—Usually relates to a specific person. This is the account that the person identifies himself or herself with when logging in to the machine. A user's short name or UID number uniquely identifies the user on a system.
- Group—Represents a group of users, a group of groups, or a mixture of both.
- Device—Similar to a user account, it's the singular entity that represents a given piece of hardware. Device accounts are uniquely identified by their Ethernet ID, serial number, IMEI, or MEID.
- Device Group—Represents a group of computers or iOS devices, a group of device groups, or a mixture of both.

Which Preferences Can Be Managed?

In addition to various other settings for user, group, devices, and device group accounts, Profile Manager provides control over the preferences listed in Table 4.1. Table 4.2 describes the manageable preferences payloads for devices and device groups.

Table 4.1 Manageable Preferences Payloads for Users and Groups

Preference	OS X	iOS	Description
General	•	•	Profile distribution type, how the profile can be removed, organization, and description
Passcode	•	•	Define passcode requirements such as length, complexity, reuse, etc.
Email	•	•	Configure email settings such as servers, account name, etc.
Exchange	•	•	Configure Exchange ActiveSync settings
LDAP	•	•	Configure connection to LDAP server
CardDAV	•	•	Configure access to CardDAV server
CalDAV	•	•	Configure access to CalDAV server
Network	•	•	Configure network setting on the device, including wireless and wired
VPN	•	•	Configure VPN settings: L2TP, PPTP, IPSec (Cisco), CiscoAnyConnect, Juniper SSL, and F5 SSL
Certificate	•	•	Allows the installation of PKCS1 and PKCS12 certificates
SCEP	•	•	Define connection to Simple Certificate Enrollment Protocol (SCEP) server
Web Clips	•	•	Display defined Web Clips as application icons

Table 4.1 (continued)

Preference	OS X	iOS	Description
Restrictions	•	•	Define application and content restrictions (separate OS X and iOS versions)
Subscribed Calendars		•	Configure calendar subscriptions
APN		•	Configure carrier settings such as the Access Point Name (Advanced use only)
iChat	•		Configure connection to Jabber or AIM chat servers
Login Items	•		Specify applications, items and network mounts to launch at login
Mobility	•		Define mobility settings for OS X clients to allow cached credentials and portable home directories
Dock	•		Configure Dock behavior
Printing	•		Configure printing settings and access to printers or print queues
Parental Controls	•		Define settings for Parental Controls such as content filtering and time limits
Security and Privacy	•		Define whether or not to send diagnostic and usage data to Apple (might change in the future)
Custom Settings	•		Apply custom preferences for items not defined in other payloads. Similar to applying preference manifests in WGM

Table 4.2 Manageable Preferences Payloads for Devices and Device Groups

Preference	OS X	iOS	Description
General	•	•	Profile distribution type, how the profile can be removed, organization, and description
Passcode	•	•	Define passcode requirements such as length, complexity, reuse, etc.
Email		•	Configure email settings such as servers, account name, etc.
Exchange		•	Configure Exchange ActiveSync settings
LDAP		•	Configure connection to LDAP server
CardDAV		•	Configure access to CardDAV server
CalDAV		•	Configure access to CalDAV server
Network	•	•	Configure network setting on the device including wireless and wired
VPN	•	•	Configure VPN settings: L2TP, PPTP, IPSec (Cisco), CiscoAnyConnect, Juniper SSL, and F5 SSL
Certificate	•	•	Allows the installation of PKCS1 and PKCS12 certificates
SCEP	•	•	Define connection to Simple Certificate Enrollment Protocol (SCEP) server
Web Clips		•	Display defined Web Clips as application icons
Restrictions	•	•	Define application and content restrictions (separate OS X and iOS versions)
Subscribed Calendars		•	Configure calendar subscriptions
APN		•	Configure carrier settings such as the Access Point Name (Advanced use only)
Login Items	•		Specify applications, items, and network mounts to launch at login

Table 4.2 (continued)

Preference	OS X	iOS	Description
Mobility	•		Define mobility settings for OS X clients to allow cached credentials and portable home directories
Dock	•		Configure Dock behavior
Printing	•		Configure printing settings and access to printers or print queues
Parental Controls	•		Define settings for Parental Controls such as content filtering and time limits
Security and Privacy	•		Define whether or not to send diagnostic and usage data to Apple (might change in the future)
Custom Settings	•		Apply custom preferences for items not defined in other payloads (similar to applying preference manifests in WGM)
Directory	*		Configure binding to directory services
Login Window	*		Configure Login Window options, such as messages, appearance, access, and Login/LogoutHooks
Software Update	•		Define an Apple Software Update Server to be used by the computer
Energy Saver	•		Define Energy Saver policy such as sleeping, timed actions and, wake settings

Managing Preferences for Users in a Group

Although you can set up preferences individually for users with network accounts, it's more efficient to manage preferences for the groups to which they belong. Using groups allows you to manage users regardless of which devices they use.

Managing Device Group Accounts

A device group account is set up for a group of computers or iOS devices that have the same preference settings and are available to the same set of users and groups. You create and modify these device groups in Profile Manager.

When you set up a device group, make sure you have already determined how the devices are identified. Use descriptions that are logical and easy to remember (for instance, the description might be the computer name). This also makes it easier to find the devices to add them to the correct device group.

Creating a Device Account

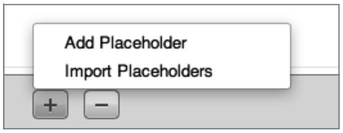
There are two ways to set up a device account:

- During device enrollment the device account is created automatically.
- You can create a placeholder in Profile Manager, so when the user logs into the User Portal, predefined profiles are assigned to the device.

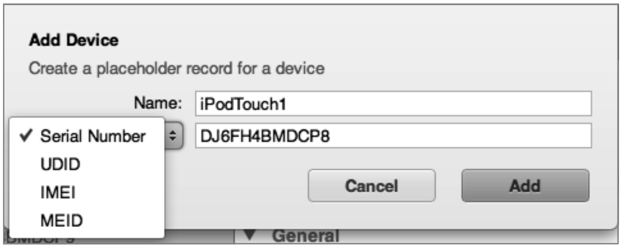
To manually create a placeholder in Profile Manager:

1 Click Devices in the Profile Manager Library.

2 Click the Add (+) button below the list of devices, and select Add Placeholder.



3 Give the placeholder a name and choose how to identify the device by Ethernet ID, serial number, IMEI, or MEID.


Add Device

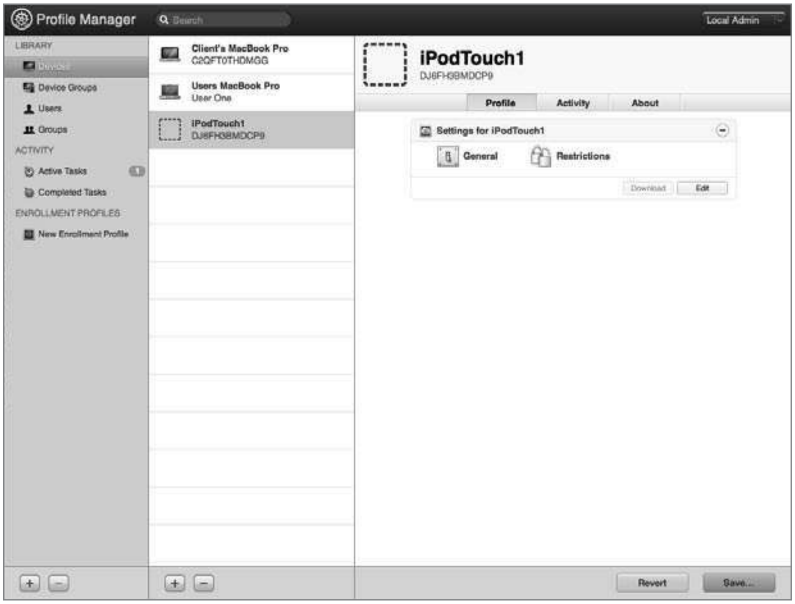
Create a placeholder record for a device

Name: iPodTouch1

✓ Serial Number: DJ6FH4BMDCP8

4 Click the Add button.

5 From the placeholder entry, you can add profiles and management that will be applied automatically once the device is enrolled.



To import a list of placeholders in Profile Manager:

Lists of devices can be imported into Profile Manager via a comma separated value (CSV) file. The file needs to be structured as this:

name, serial number, UDID, IMEI, MEID

Leave a field empty if you're not using that value.

1 Click Devices in the Profile Manager Library.

2 Click the Add (+) button below the list of devices, and select Import Placeholders.

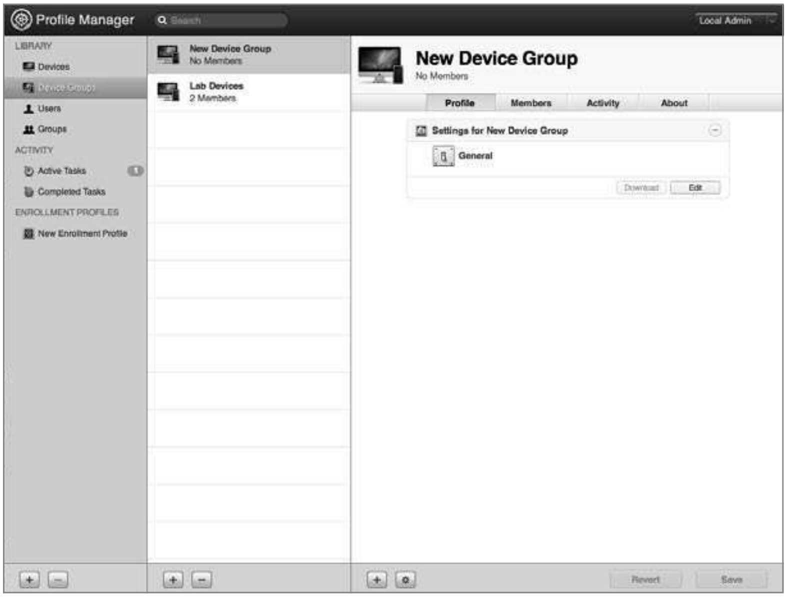
3 Choose the import file and upload.

Creating and Populating a Device Group

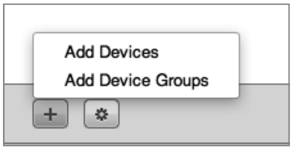
To create and populate a Device Group, Profile Manager is utilized:

1 Click Device Groups in the Profile Manager Library.

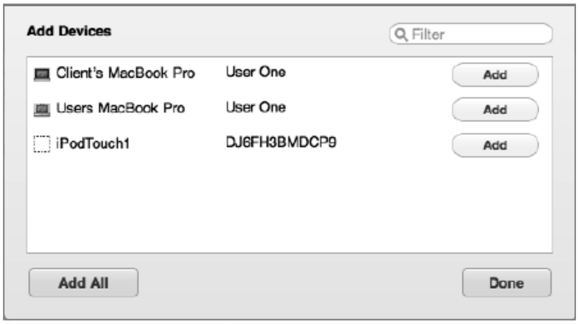
2 Click the Add (+) button below the list of device groups. This creates a new group that can be populated with the desired name.



3 To add devices to the device group, click the Add (+) button under the device group pane.



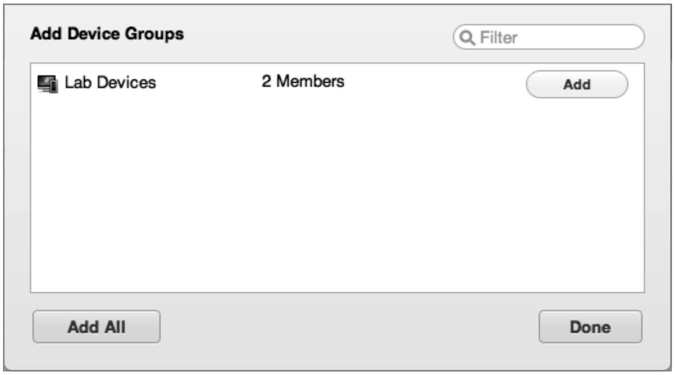
4 Click the device to add to the device group and then click Done.



Client's MacBook Pro	User One	Add
Users MacBook Pro	User One	Add
iPodTouch1	DJ6FH3BMDCP9	Add

5 To add device groups to the device group, click the Add (+) button under the device group pane.

6 Click the device group to add to the device group and then click Done.



Add Device Groups

Lab Devices	2 Members	Add

7 Click Save.

Troubleshooting

Occasionally things won't work the way you expect, and you'll have to troubleshoot the situation. Even a robust service like Profile Manager can have an occasional issue.

Viewing Logs

The profilemanager.log is located at /Library/Server/ProfileManager/Logs and can be viewed with Console by double clicking. Errors may be reported and listed in the logs.

Viewing Profiles

If a device is not behaving as expected, look at the list of installed profiles on the device and see if the proper profiles have been installed. The solution may be as simple as applying the expected profile to the device.

Installing Profiles

If you're having problems installing a profile, you may have improper certificates. Review your SSL certificates for validity and make sure the trust profile has been installed on the device.

Problems Enrolling a Device

A trust profile must be installed prior to enrolling a device, unless you are using a certificate signed by a trusted certificate authority.

What You've Learned

- Account management encompasses fine-tuning the user experience by managing preferences and settings for users, groups, devices, and device groups.
- Profile Manager is the new management tool in Lion Server. It provides profile-based management of users, groups, devices, and device groups—from anywhere on your network or even across the Internet.
- A device group is a list of devices that have the same preference settings and are available to the same users and groups. You can create and modify device groups in Profile Manager web app.
- Preferences can be set for many built-in OS X options for users, workgroups, devices, or device groups. Other preferences can be managed if provided in a .plist format and applied via the Custom Settings profile payload.

References

The following documents provide more information about managing accounts on Lion Server. All these and more are available at http://www.apple.com/macosx/server/resources/documentation.html.

Administration Guides

Lion Server: Advanced Administration
https://help.apple.com/advancedserveradmin/mac/10.7/

Profile Manager Help
https://help.apple.com/profilemanager

Apple Knowledge Base Documents

You can check for new and updated Knowledge Base documents at http://www.apple.com/support/.

Chapter Review

1. What tool is used to create profiles?
2. Name at least three ways a profile can be delivered.
3. Why should a configuration profile be signed?
4. How is a profile removed from an OS X computer? From an iOS device?
5. What is a configuration profile? An enrollment profile?
6. What steps are involved with turning on the Profile Manager service?
7. What steps are involved with specifying that you want to sign your configuration profiles?
8. What three components comprise Profile Manager?

Answers

1. The Profile Manager web app is used to create profiles.
2. User portal, email, web page, manual delivery, or push to enrolled devices via the mobile device management capabilities of Profile Manager enable profile delivery.
3. A configuration profile should be signed to validate the contents of the profile.
4. In OS X 10.7 Lion, the profiles are managed in the Profiles preference pane within System Preferences. On an iOS device, navigate to Settings/General/Profiles to view and remove installed profiles.
5. A configuration profile contains settings and preferences to manage the user experience in a controlled device. An enrollment profile allows the device that it’s installed on to be remotely controlled, performing such tasks as remote wipe and lock, and installation of other configuration profiles.
6. You can just click the On/Off switch in the Server app Profile Manager pane to turn on the Profile Manager service, but to enable device management (also known as Mobile Device Management), click Configure next to “Device Management,” select a valid SSL certificate, and specify a verified Apple ID to obtain an Apple Push Notification Service certificate.
7. In the Server app Profile Manager pane, select the checkbox labeled “Sign configuration profiles,” then choose a valid code signing certificate. Then when you create profiles with the Profile Manager web app, they are automatically signed.
8. The Profile Manager includes the Profile Manager web app, the user portal, and the optional device management (Mobile Device Management) service.

Index

A

About This Mac, 3–4
access. See also authentication; authorization
  ACLs controlling. See ACLs (access control lists)
  Apache log for, 399–400
  concurrent, 374
  Edit Access to Services for, 122
  to file sharing services, 332–333
  in folder hierarchies, 350–353
  guest. See guest access
  in iCal, 422–428
  by local user accounts, 93–95
  monitor only, 131–133
  in NetBoot, 303
  to Open Directory log files, 233–234
  SACLs for. See SACLs (service access control lists)
  Service Access window for, 196, 201–202
  to services, 86–88
  for Time Machine, 367
  of users, 86–87
  to websites, 393–396
access control entries. See ACEs (access control entries)
access control lists. See ACLs (access control lists)
Access pane, 329–331
account management. See Profile Manager
Account Name, 90, 92
ACEs (access control entries)
  adding to ACLs, 339–341
  complex permissions for, 339, 341–342
  creating, 338
  defined, 337
  in file-system ACLs, 347
  in folder hierarchies, 349, 357–361
  information in, 347
  inheriting, 343–345
  in Open Directory masters, 160
  POSIX and, 348
  precedence and, 348
  propagating permissions and, 345
ACLs (access control lists). See also file-system ACLs (access control lists); SACLs (service access control lists)
  complex permissions in, 341–342
  File Sharing pane for, 337–339
  generally, 336
  globally unique IDs in, 337
  group IDs in, 336
  group membership in, 346
  inheritance in, 343–345
  multiple groups in, 346
  nested groups in, 346
  optional, 333–334
  permissions and, 334–335
  portability of, 345
  POSIX permissions vs., 347
  propagating permissions in, 345
  share points and, 320, 329
  Storage pane for, 339–341
  user IDs in, 336
Active Directory, 158, 417
Add User Account, 301
Address Book
  access to monitor only, 133
  configuring OS X to use, 440–444
  configuring with Server app, 439–440
  generally, 439
  iChat and, 443–444
  importing network user accounts, 208
  location of data stores in, 406
  in Open Directory masters, 170–171
  troubleshooting, 445
administration privileges
  accounts with. See administrator accounts
  cleaning up, on servers, 133–136
  complex permissions for, 341–342
  computers with. See administrator computers
  confirming, generally, 131
  File Sharing and, 137
  giving to local user accounts, 95–96

  limiting, generally, 128
  for local user accounts, 96–97, 129–130
  monitoring services, 130
  removing from local user accounts, 97–98
  removing unused services, 136–137
  for specific services, 131–133
administrator accounts
  Administrator Account pane, 25–27
  Administrators group, 329
  configuring, 92–93
  creating, 88
  password policies and, 216
administrator computers
  configuring for exercises, 16–20
  configuring local user accounts on, 93
  configuring SACLs on, 117–119
  for Lion Server, 15
AFP (Apple Filing Protocol)
  authentication and, 87
  case-sensitivity in, 375
  defined, 316–318
  encryption in, 138
  guest access for, 328
  inspecting logs in, 375–376
  inspecting SACLs in, 125–128
  Mac clients using, 318
  network home folders in, 362–363
  POSIX in, 336
  SACLs in, 117–118, 125–128
  setting up, 118–119
  for share points, 320–321, 323
  testing, 119–121
  viewing Error log with Console in, 322–323
Airport devices, 16
Airport Management pane, 37
alerts, 41, 54–55
Aliases, 92
All, 392
Allow or Deny, 347–348
anonymous binding, 184
"Any other logged in user," 413
Apache
  access to files in, 392
  configuration files in, 384
  introduction to, 383
  location of modules in, 384
  viewing log files in, 399–402
Apple
  Airport devices by, 16
  filing protocol. See AFP (Apple Filing Protocol)
  Open Directory by. See Open Directory
  Partition Map by, 6
  ports used by software of, 138
  Push Notification certificates, 254
  Remote Desktop, 281, 289
  software updates from, 55
  System Restore, 281, 303
Apple IDs
  Apple Push Notification certificates and, 254
  configuring pane for, 24–25
  IDs. See Apple IDs
  Profile Manager and, 252
  "Using an Apple ID," 120
Apple Pro Training Series: OS X Lion Support Essentials
  on authentication, 88
  on DNS, 163
  on file system permissions, 334
  on Recovery HD, 8
  on volume formats, 6
Apple Training Series: Mac OS X Server Essentials v10.6, 251
Apply System Configuration Settings, 301
archives
  disk images for, 222–225
  in iChat, 432
  Kerberos KDC for, 222
  in LDAP databases, 222
  in Open Directory generally, 221–222
  in Open Directory masters, 222–224
  in Password Server, 222
ARD (Apple Remote Desktop), 281, 289
ASR (Apple System Restore), 281, 303
audio conferences. See iChat
authenticated binding, 184–185
authentication. See also authorization
  as administrator, 88
  databases in, 156
  encryption in, 138
  in file sharing services, 316
  generally, 85–86
  handshake protocol for, 209
  introduction to, 86–88
  in Kerberos, generally, 219
  in Kerberos, troubleshooting, 235
  of local users, 130
  methods for. See configuration, authentication methods
  of multiple user accounts, 154–155
  of network user accounts, 198–199
  in new websites, 394–395
  in Open Directory, 235
  passwords for. See passwords

- references on, 149
- of remote servers, 189
- review questions on, 150–151
- summary of, 148–149

authorization. See also authentication
- cleaning up, 133–136
- in file sharing services, 316
- introduction to, 85–86
- in new websites, 395
- references on, 149
- review questions on, 150–151
- SACLs for. See SACLs (service access control lists)
- summary of, 148–149
- using, 86–88

Automated Installation, 288
Automater workflow items, 287–288
automatic push for profiles, 269
Automator Library, 301
automountable share points, 362

B

backups, 289, 370–371
badges, 316
bandwidth, 309
binding to Open Directory
- anonymously, 184
- benefits of, 156
- defined, 154
- Lion, 192–193
- multiple servers, 158
- network user accounts, 202
- Users & Groups for, 182

blacklists, 455–456
blogs, 407, 415
Bonjour
- address of, 384
- introduction to, 34
- Server Admin and, 46

boot codes, 299
boot image files, 288
boot ROM (real-only) memory files, 285–286
boot volumes, 7, 406
booting computers. See also NetBoot, 282, 290
bootpd, 307
buddies, 433–434, 444

C

CalDAV support, 417, 428
Calendar Server Extensions, 416
calendar service. See iCal
Caps Lock key, 224
CardDAV
- for Address Book, 439, 441
- for iChat, 444

CAs (Certificate Authorities)
- Certificate Signing Requests for, 68–70
- default certificates and, 63
- importing signed certificates and, 70
- in Open Directory masters, 160, 172–173
- for profiles, 278
- in restoring Open Directory data, 229
- for SSL certificates, 59–61, 72–76
- using another server and, 182

case-sensitivity, 6, 374–375
CD-ROMs, 282
Certificate Authorities. See CAs (Certificate Authorities)
Certificate Signing Requests (CSRs), 68–70
certificates
- authorizing. See CAs (Certificate Authorities)
- importing signed, 70–71
- root, 258
- self-signed, 39–40, 63–68
- Signing Requests for, 68–70
- SSL. See SSL (Secure Sockets Layer) certificates
- verifying trusted, 40, 72–76
- viewing default, 61–63

Challenge Handshake Authentication Protocol, 209
child files, 343
child folders, 343
ClamAV virus scans, 454
classrooms, 283
cleaning up file services, 376–377
cleaning up servers, 133–136
client computers
- binding to Open Directory, 192
- Client Computer ID window, 184
- in NetBoot. See clients in NetBoot

client devices, 249
clients in NetBoot
- configuring, 299–300
- filtering, 303–305
- monitoring, 305–307

Code Signing certificates, 255
collaborative services. See also web services
- Address Book, 439–445
- administrative tools for, 406
- data stores for, locating, 406
- iCal, accessing as user, 422–428
- iCal, adding resources and locations, 420–422
- iCal, configuring and starting, 417–420
- iCal, generally, 416–417

iCal, troubleshooting, 429
iChat, archiving, 432
iChat, configuring users, 433–434
iChat, federation in, 435–436
iChat, managing generally, 429–431
iChat, restricting users, 435
iChat, setting up, 431
iChat, troubleshooting, 438
iChat, viewing service logs, 437–438
introduction to, 405
mail, blacklists for incoming, 455–456
mail, configuring DNS for, 448
mail, enabling for users, 450
mail, enabling web, 451–453
mail, junk filtering for incoming, 455–456
mail quotas, enabling for users, 453–454
mail, relaying outgoing, 449–450
mail services, enabling, 448–449
mail services, generally, 445–447
mail services, troubleshooting, 457
mail, virus scanning incoming, 454–455
references on, 458
review questions on, 458–459
summary of, 457
Wiki service, troubleshooting, 416
wikis, creating, 410–415
wikis, enabling, 407–410
wikis, managing generally, 406–407
complex permissions, 341–342
computational clusters, 284
computer labs, 283
Computer Name, 34–35
concurrent access, 374
configuration
of Administrator Account pane, 25–27
of administrator accounts, generally, 92–93
of Apple ID pane, 24–25
of authentication methods. See configuration, authentication methods
of computers for Software Update, 311
of Lion Server. See configuration, Lion Server
of local user accounts. See local users
of NetBoot. See configuration, NetBoot
of Open Directory, 159–165
of Profile Manager. See configuration, Profile Manager
of SACLs, 117–118
of user accounts, 89–92
configuration, authentication methods
disabling user accounts, 210
generally, 209
global password policies, 215–219
Kerberos, 219–221
per-user password policies, 211–213
Server Admin in, 218–219
single sign-ons, 219–221
single user accounts, 213–214
testing user account policies, 214–215
user account password policies, 211–215
user accounts, 209–210
configuration, Lion Server
administrator computers, 15–20
Airport Management pane, 37
Computer Name, 34–35
Connecting to Your Mac pane, 31–36
data storage on volumes, 58–59
generally, 1, 15, 20
Host Name pane, 30–31, 35–36
initially, 20
introduction to, 1
Keyboard pane, 23
License Agreement pane, 25
Multiple Networks Detected pane, 28
Network Address pane, 32–34
Organization pane, 28–29
Region pane, 23
Registration Information pane, 25
remotely, 20–23
Review pane, 38
with Server Admin, 45–47
Server pane, 24
test networks for exercises in, 15–16
Thank You pane, 38–39
Time Zone pane, 29–30
Xsan pane, 27
Configuration Log, 233–234
configuration, NetBoot
clients, 299–300
images, 297–298, 300–302
NetRestore images, 303
servers, 296–298
configuration, Profile Manager
delivering profiles, 268–269
enabling Profile Manager by, 253–256
generally, 251, 263–268
managing profiles locally, 262–263
preparation for, 252
remotely locking or wiping devices, 269
terminology for, 252
User Profile Portal, 256–262
Configuration Profiles, 252–256, 287

confirmation of administrative capacities
to administer services, 131
to monitor services only, 130
for specific services only, 131–133
"Connect as Guest," 120
Connected Users, 321–322
Connecting to Your Mac pane, 31–36
connection to Lion Server, 39–43
Console
importing users with, 146–147
inspecting logs with, 375–376
logs in, generally, 76–78
viewing AFP Error log with, 322–323, 402
corporate workstations, 283
CPU usage
Server Admin monitoring, 46–48, 130, 321
Server app monitoring, 42–43
Server Status Dashboard Widget for, 56–57
Create Image, 301–302
credentials, defined, 85
crypt passwords, 209–210
CSRs (Certificate Signing Requests), 68–70

D

Dashboard Widget, 56–58
dashes, 212
data
archiving. See archives
restoring Open Directory, 221, 226–232
stores for collaborative services, 406
storing on volumes, 58–59
default websites, 386
Define Image Source, 301
delegates, 421–422
delimited text files, 116
Demo iPad account, 422–428
Deny, or Allow, 347–348
deployment solutions. See NetBoot
descendants, 343
destinations, 367–373
device accounts
creating, 274–275
for groups, 269, 274, 275–277
introduction to, 269
Device Management, 253
devices
accounts for. See device accounts
Airport, 16
client, 249
enrolling in Profile Manager, 249–250, 278
iOS, 249–250, 254, 256
locking, 262, 269
mobile, 249–251
over the air management of, 251
in Profile Manager web app, 264
remote, 262
User Profile Portal for, 256
Devices and Profiles, 256–261
DHCP (Dynamic Host Configuration Protocol)
as Lion Server service, 51
NetBoot IP addresses from servers on, 285–286
ranges in, 16
VPN connections and, 139
directory nodes, 198
directory services. See Open Directory
Directory Utility
binding to Open Directory vs., 162
in configuring servers remotely, 188–192
troubleshooting Open Directory with, 235
disable user accounts, 210
disable websites, 384–385
disk images. See also NetBoot
for archiving data, 222–225
encrypted, 225
on HTTP, 293–294
in NetBoot startup, 285
network, 299
on NFS, 293–294
for restoring Open Directory data, 231–232
sparse, 225, 231–232
System Image Utility for, 290
disk partition support, 288
Disk space, 41–43
Disk Utility
for booting computers, 290
case-sensitive formatting with, 374
First Aid tab in, 78
for installing Lion Server, 6
Diskless checkbox, 295
Distribution Type, 266
DNS (Domain Name System)
Address Book and, 445
administrator computers for, 17–19
availability of records in, 163–165
binding to other servers, 183
in configuring Open Directory replicas, 179
for email, 448, 457
forward records in, 10–11
host names and, 8–9
iCal and, 428–429
iChat and, 438
in Kerberos, 235

Lion Server service for, 51
in NetBoot, 303
for network user accounts, 202
for new websites, 396
Open Directory replicas and, 174–175
Open Directory services and, 159
preparing to configure records in, 236–243
in restoring Open Directory data, 226–227, 229
reverse records in, 10–11
in Server Admin, 136–137
in Server Assistant, 50
supporting multiple servers, 236–243
for websites, 391
for wikis, 416

Dock
hiding graphs, 47
Launchpad in, 10, 21, 44–45, 371
in Profile Manager web app, 265–267
Trash in, 372

Document Root Contents, 392
Domain Name, 386–389
Domain Name System (DNS). See DNS (Domain Name System)
Dovecot, 445
DVD-ROMs, 282
Dynamic Host Configuration Protocol (DHCP). See DHCP (Dynamic Host Configuration Protocol)

E

editing
access to file sharing services, 122
images, 304
SACLs, 332–333
text. See TextEdit

efficiency, 281
EFI (Extensible Firmware Interface), 269, 299
email. See also mail services
in Address Book, 443
alerts, 41, 54–55
blacklists for incoming, 455–456
configuring DNS for, 448
delivering profiles via, 269
enabling for users, 450
enabling web, 451–453
in iCal, 417–420, 423
junk filtering for incoming, 455–456
location of data stores in, 406
relaying outgoing, 449–450
virus scanning incoming, 454–455

emergency boot disks, 284
Empty Trash, 372
empty volumes, 14–15
encrypted sparse disk images, 222, 225
encryption
in AFP, 138
in authentication, 138
of firevault full disks, 8
for iChat, 436
in VPNs, 137–138

Energy Saver preferences, 3
Error log in Apache, 399–400
error logs in AFP, 322–323
Ethernet
IDs, 269, 274–275
MAC addresses for, 5
NetBoot requirements for, 284
ports, 2

Everyone, 392
Everyone Else, 329–331
expired passwords, 216
exporting settings, 52–53
exporting users
Software Update for, 308–311
with Workgroup Manager, 102–104, 107–108

extensible directory-services architecture, 154
Extensible Firmware Interface (EFI), 269, 299
eXtensible Markup Language (XML). See XML (eXtensible Markup Language)
Extensible Messaging and Presence Protocol (XMPP), 430, 436
external FireWire disks, 300

F

Fast User Switching, 362
federation, 435–436
File Sharing pane. See also file sharing services
access to share points in, 329–331
ACLs in, 337–339
adding share points in, 325–327
configuring network mounts in, 363
default share points in, 325
deselecting, 124
in Edit Access to Services, 122
enabling, 117
exploring, generally, 324
individual share points in, 327–328
inheritance rules in, 345
permissions in, 330, 338
removing share points in, 325–327
SACLs in, 125
Time Machine and, 366–367, 372
turning off, 137

turning on, 119
verifying share points in, 297
file sharing services
access to share points in, 329–331
ACEs in. See ACEs (access control entries)
ACLs in. See ACLs (access control lists)
adding share points in, 325–327
AFP for. See AFP (Apple Filing Protocol)
backups excluding system files in, 370–371
case-sensitivity in, 374–375
challenges of, 316–319
cleaning up, 373, 376–377
complex permissions in, 341–342
configuring access to, 332–333
Console for, 322–323
default share points in, 325
destinations in, 367–370
file-system ACLs in. See file-system ACLs (access control lists)
folders in, 329–333
globally unique IDs in, 337
group IDs in, 336
group membership in, 346
groups in, configuring, 319–320
individual share points, 327–328
inheritance in, 343–345
introduction to, 315
local user access to, 93–95
logs for, 375–376
maintenance of, 321
monitoring servers for, 321–322
multiple groups in, 346
nested groups in, 346
network home folders in, 361–366
network mounts for, 362–364
ownership in, 333–335
pane for. See File Sharing pane
permissions in, generally, 333–335, 347
planning, 319–323
portability in, 345
POSIX. See POSIX
precedence in, 347–348
propagating permissions in, 345
protocols for, 316–319, 336
references on, 378–379
removing sharing points, 325–327
requirements for, 319
restoring destinations in, 371–373
review questions on, 379–381
Server app starting and configuring, 320–321
share points in. See share points
SMB. See SMB (Server Message Block)
Storage pane for, 339–341
summary of, 377–378
testing, 320
Time Machine. See Time Machine
troubleshooting, 374
user IDs in, 336
users, configuring generally, 319–320
users, for network home folders, 364–366
WebDAV, 316–319, 335
file-system ACLs (access control lists)
configuring additional ACEs for, 357–361
configuring, generally, 349
configuring permissions, 351–357
creating shared folders, 351
creating users and groups, 350–351
defined, 332
generally, 347
introduction to, 329
precedence in, 347–348
removing share points for, 349–350
File Transfer Protocol (FTP), 318
Filter Computer Models, 288
filters
for junk mail, 455, 457
in NetBoot, 303–305, 308
for viruses, 454–455
Finder
for access in folder hierarchies, 353
AFP testing for SACLs in, 119–121
cleaning up with, 376–377
External Disks in, 300
guest access in, 328
inspecting Open Directory archives with, 225
Kerberos tickets in, 220–221
"MyNewWebsite" folder on, 388
standard settings in, 329
testing user account policies with, 214–215
firevault full disk encryption, 8
firewalls, 137–138, 308
FireWire, 300
firmware, 299, 307
First Aid tab, 78
folders
badges for, 316
configuring access to, 329–333
hierarchies of, 349, 357–361
network home. See network home folders
POSIX ownership of, 334

formatting drives, 5–6
forward DNS records. See also DNS (Domain Name System), 10–11
FQDNs (fully qualified domain names)
  in AFP, 402
  in DNS, 163
  of Lion Server webpages, 384
  for new websites, 386–391
FTP (File Transfer Protocol), 318
Full Name, 90, 106
fully qualified domain names (FQDNs). See FQDNs (fully qualified domain names)

G

Gigabit Ethernet, 2
global password policies, 211
globally unique IDs (GUIDs), 337
graphs
  of CPU usage, 46–48, 130, 321
  monitoring server usage with, 321–322
  in Server app, 42–43
group IDs (GIDs), 336
groups
  in ACLs, 346–347
  for file sharing services, 319–320, 325, 350
  of local users. See groups of local users
  manageable preferences payloads for, 270–273
  managing. See Profile Manager
  multiple, 346
  nested, 346
  in Open Directory masters, 169
  preferences for users in, 273
  in Profile Manager. See Profile Manager
  SACLs for, 117
  user accounts for, 92
groups of local users
  assigning local groups to, 102
  assigning local users to, 99–101
  assigning to local users, 101–102
  creating, 98–99
guest access
  in AFP, 328
  connecting, 120
  implications of, 330
  to share points, 317, 320
  in SMB, 328
guest-enabled share points, 328
GUID Partition Table, 6
GUIDs (globally unique IDs), 337

H

Handshake Authentication Protocol, 209
hardware addresses, 303–304
hardware requirements for Lion Server, 2–3
hardware requirements for NetBoot, 284
hash passwords, 209
home folders
  configuring network mounts in, 362–364
  configuring users in, 364–366
  generally, 361–362
  in NetBoot, 286
  for network user accounts, 201
  share points and, 320
Host Name pane, 30–31, 35–36
host names, defined, 8–9
html (Hypertext Markup Language), 389
HTTP (Hypertext Transfer Protocol)
  disk images on, 293–294
  iCal on, 416, 428
  NetBoot on, 285–286
  port 80 for, 396, 402
  wikis on, 409
HTTPS (HTTP Secure)
  iCal on, 428
  port 443 for, 396, 402
  wikis on, 409

I

iCal
  accessing as user, 422–428
  adding locations, 420–422
  adding resources, 420–422
  configuring and starting, 417–420
  generally, 416–417
  location of data stores in, 406
  troubleshooting, 429
iChat
  Address Book and, 443–444
  archiving, 432
  configuring users, 433–434
  federation, 435–436
  location of data stores in, 406
  managing generally, 429–431
  restricting users, 435
  setting up, 431
  troubleshooting, 438
  viewing service logs, 437–438
IDs
  for Apple. See Apple IDs
  Ethernet, 269, 274–275

globally unique, 337
for groups (GIDs), 336
for images, 287
International Mobile Equipment Identities (IMEIs), 269, 274–275
for mobile devices (MEIDs), 269, 274–275
for users. See user IDs (UIDs)
images. See also NetBoot
configuring, 300–302
configuring to serve, 297–298
creating, 287–293
default, 293
protocols for, 293–294
restoring, 303
types of, 288–289
Images pane, 293
IMAP (Internet Message Access Protocol), 447
IMEIs (International Mobile Equipment Identities), 269, 274–275
importing
formatted lists of users, 108–110
Lion Server settings, 52–53
signed SSL certificates, 70–71
text lists of users, 110–116
users with Workgroup Manager, 102–104
incoming email, 406, 454–456
indexes of images, 287
index.html files, 389, 396
individual software updates, 310–311
inheritance
in ACEs, 337
in ACLs, 343–345
permissions in, 341–342
"Install OS X Lion," 290–291
installation
of image files, 288–289
Install Software pane for, 13
of Lion Server. See installation, Lion Server
of profiles, 277
of Server Admin Tools 10.7, 44–45
of Software Update, 54–56
of VPN Profile, 140–144
installation, Lion Server
DNS records in, 10–11
empty volumes in, 14–15
firevault full disk encryption, 8
formatting drives for, 5–6
generally, 1, 3
hardware requirements for, 2
Lion Recovery and, 78
log inspection and, 76–78
manual IPv4 address configuration, 9–10
networking in, 2
partitioning disks in, 6–8
RAID (Redundant Array of Independent Disks), 8
references on, 80–81
remote configuration in, 5–6
review questions on, 81–83
scenarios for, generally, 8–9
Server app in, 12–13
server components for, 9–13
server components on Snow Leopard servers, 14
summary of, 78–79
system requirements for, 3–6
troubleshooting, 76–78
instant messages. See iChat
International Mobile Equipment Identities (IMEIs), 269, 274–275
Internet Message Access Protocol (IMAP), 447
Internet Service Providers (ISPs), 449–450
invitations, 418–422, 426, 428
iOS devices
locking, 269
manageable preferences payloads for, 270–273
managing settings on, 249–250
permissions and, 335
Profile Manager and, 254
User Profile Portal for, 256
IP addresses. See also IPv4 addresses
configuring Open Directory replicas and, 179
DNS records and, 163–164
introduction to, 19
of Lion Server webpages, 384
in NetBoot, 285–286, 307
for new websites, 386–391, 396
in Open Directory, generally, 226–227
of Open Directory replicas, 175–177
updating DNS service and, 238
iPhones
file sharing services on, 317
iCal and, 417, 428
User Profile Portal for, 256
iPod touch, 417, 428
IPv4 addresses. See also IP addresses
configuring, 9–10
in Lookup, 11
manually assigned, 8–10
for VPN clients, 139
ISPs (Internet Service Providers), 449–450

J

Jabber, 430–436, 443
journaled formats, 6
junk filters, 455–456

K

KDC (Key Distribution Center). See Kerberos KDC (Key Distribution Center)
Kerberize Services. See also Kerberos
  in binding to Open Directory servers, 187
  defined, 219–220
  importing network user accounts and, 208
Kerberos
  binding to other directory services with, 162
  binding to other Open Directory servers via, 187–188
  definition of terms for, 219–221
  KDC in. See Kerberos KDC (Key Distribution Center)
  for Open Directory masters, 160–161
  for Open Directory, generally, 155
  for Open Directory masters, 170
  for Open Directory replicas, 180
  password policies in, 216
  restoring Open Directory data via, 230
  Server Log, 233–234
  for single sign-ons, 219
  tickets in, 219–221
  troubleshooting, 235–236
Kerberos KDC (Key Distribution Center)
  archiving, 222
  for authentication, 156
  defined, 219–220
  for Open Directory, generally, 209
  for Open Directory log files, 233
  for Open Directory replicas, 174
  for restoring Open Directory data, 226–227
Key Distribution Center (KDC). See Kerberos KDC (Key Distribution Center)
Keyboard pane, 23
keyboards, 52
Keychain Access
  remembering credentials in, 40
  in SSL certificate configuration, 60–63
  verifying trusted CAs with, 72–75
Keychain Secure Note, 224
keychains, 172–174, 197
Keynote, 317
keyword searches, 432
kiosks, 283
“known good” logs, 147

L

L2TP (Layer 2 Tunneling Protocol), 137
Launchpad
  Console in, 146, 322
  in Dock, 10
  Network Utility in, 164, 175, 242
  opening, 12
  Server Admin in, 44–45
  Server app in, 21
  Server Status Dashboard Widget in, 57
  System keychains in, 172
  TextEdit in, 110, 354, 371
  Workgroup Manager in, 104
Layer 2 Tunneling Protocol (L2TP), 137
LDAP (Lightweight Directory Access Protocol)
  Address Book and, 439
  archiving databases in, 222
  binding to directory servers in, 287
  configuring servers remotely with, 190–191
  connecting to directories in, 235
  iCal and, 417
  logs in, 233–234
  for Open Directory data restoration, 226–227, 229–230
  for Open Directory, generally, 155–156
  for Open Directory log files, 233
  for Open Directory replicas, 174, 178
  per-user directory password policies and, 211
  populating directories in, 193–194
  Search Base, 170
  Server, 170, 180, 230
  shared databases in, 227
libraries, 274–277, 283
license agreements, 25, 301
Lightweight Directory Access Protocol (LDAP). See LDAP (Lightweight Directory Access Protocol)
limited administration privileges. See also administration privileges, 128–133
Linux, 318
Lion. See OS X Lion
Lion Recovery, 78, 288
Lion Server. See OS X Lion Server
“Lion Server: Installation requires Internet access,” 9
“Lion Server: Installing Lion Server on a blank volume,” 14
“Lion Server: Mass deployment strategies,” 15
“Lion Server Upgrading and Migrating,” 14
Local Admin
  authenticating as, 98
  defined, 95
  UID of, 104
local administrators
  with guest access, 120
  Local Admin for. See Local Admin
  local users as, 93–97
local directories, 197

local directory domains, 88
local users. See also user accounts
  access to services and files by, 93–95
  assigning local groups to, 101–102
  assigning local groups to local groups of, 102
  assigning to local groups of, 99–101
  configuring with Server app, 93
  confirming administrator status of, 96–97
  creating with Workgroup Manager, 106–107
  disabling accounts, 210–211
  exporting with Workgroup Manager, 107–108
  granting administrator status to, 95–96
  groups of, creating, 98–99
  importing with Workgroup Manager, 108–110
  limited admin privileges of, 131
  monitoring services, 130
  removing admin status of, 97–98
  in SACLs for AFP, 118–120
  in SACLs for SMB, 123
  in SACLs in Server app, 121–126
  Server app for, 89–93, 121–126
  Server Assistant options and. See Server Assistant
  in VPN Connection pane, 143
locales, 157–158
location of software updates, 309
locations in iCal
  accessing, 426
  adding, 421–422
  of user accounts, 428
locks, 262, 307
logical port values, 387
login
  disabling, 212
  keychains, 68
  password policies and, 214–217
  remote, 26, 117
  troubleshooting, 233, 235
Login Options, 183, 193, 235
Login Shell, 91
login windows
  for authentication, 86–87
  for authorization, 87
  configuring, 19
  Lion Recovery and, 78
  for Open Directory, 235
  on other computers, 89
  shaking, 87
logs
  for email, 457
  in iChat, 432, 437–438
  import, in Console, 146
  inspecting, 76–78
  in NetBoot, 306–307
  in Open Directory, 233–234
  in Profile Manager, 277
  server, 307
  for VPN services, 147–148
long names, 90
Lookup
  configuring Open Directory replicas with, 175–177
  for DNS, 163
  introduction to, 1–3, 10–11

M

Mac App Store
  Lion from, 14, 291
  Lion Server from, 3, 12, 15
  Server app from, 20, 82
  software updates from, 17
Mac computers
  as administrators. See administrator computers
  installing Lion Server on empty volumes, 14–15
  installing Server app on, 12–13, 15
  remote configuration on, 4–5
  requirements for Lion Server on, 2–3
  scenarios for installing Lion Server on, 8–11
  Snow Leopard updating, 3
  verifying system requirements on, 3–4
MAC (Media Access Control) addresses
  of computers in NetBoot, 301, 303
  of servers, 5, 22
  of target computers, 20, 301
Mac OS X. See also OS X Lion
  computer names in, 34, 49
  Lion Recovery and, 78
  Setup Assistant in, 61
  versions required, 2
"Mac OS X: About file system journaling," 6
Mac OS X Extended (Journaled), 6–7
Mac OS X Lion. See OS X Lion
Mac OS X Server. See OS X Lion Server
Mac OS X Server 10.7. See OS X Lion Server
"Mac OS X Server v10.6: Moving an HFS+ Journal
  to a different volume," 6
Mac OS X Snow Leopard. See Snow Leopard
Mail eXchange (MX) servers, 446, 448
mail services. See also email
  enabling, 448–449
  generally, 445–447
  quotas in, 453–454
  troubleshooting, 457
maintenance of file sharing, 321
maintenance of Lion Server, 1
Manage Network Accounts, 165–168

manageable preferences payloads, 270–273
management
- of computers with NetBoot, 282–289
- of network user accounts. See network user accounts
- of user accounts. See Profile Manager
- of websites, 386

mandatory PDFs, 281
manual IPv4 address configuration, 9–10
Master Boot Record, 6
MDM (Mobile Device Management), 249–251
Media Access Control (MAC) addresses. See MAC (Media Access Control) addresses
MEIDs (mobile equipment identifiers), 269, 274–275
Microsoft Active Directory, 417
Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2), 209
mobile devices, 249–251
modules, 383–384
monitoring
- clients in NetBoot, 305–307
- Lion Server. See monitoring Lion Server
- servers, 321–322
- services, by local users, 129–130
- services, limited admin privileges for, 130
- web services, 399–402

monitoring Lion Server
- introduction to, 1
- moving service data to different volumes in, 58–59
- with Server Admin, 45–47
- with Server app, 39–43
- Server Status Dashboard Widget for, 56–58
- Software Update for, 54–56
- tools for, generally, 39

mounted share points, 316
mounted volumes, 290
mounts, 362–364
mouse, 52
MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol), 209
multicast streams, 303
multiple computers. See also NetBoot, 283
multiple groups. See also groups, 346
Multiple Networks Detected pane, 28
multiple users. See groups
MX (Mail eXchange) servers, 446, 448

N

N key, 293, 299–300
names
- of accounts, 90, 92
- computer, 34–35
- DNS for. See DNS (Domain Name System)
- domain, 386–389
- full, 90, 106
- fully qualified domain. See FQDNs (fully qualified domain names)
- host, 8–9, 30–31, 35–37
- long, 90
- service, 52
- short, 90, 105–107

NAT (Network Address Translation), 437
nested groups, 346
nested replicas, 157
Net Restore, 289
NetBIOS, 317
NetBoot
- configuring clients in, 299–300
- configuring images in, 300–302
- configuring servers for, 296–298
- configuring service to images in, 297–298
- creating images in, 287–293
- default images in, 293
- deployment issues and, 281–282
- Ethernet for, 3
- filtering clients in, 303–305
- hardware requirements for, 284
- home folders in, 286
- image types in, 288–289
- introduction to, 281
- as Lion Server service, 51
- managing computers with, 282–289
- monitor only access in, 131–133
- monitoring clients in, 305–307
- NetRestore images in, 303
- Network Install in, 289
- NFS for, 318
- protocols for images in, 293–294
- references on, 312
- review questions on, 312–313
- shadow files in, 294–295
- Software Update for, 308–311
- startup in, 284–286
- summary of, 312
- System Image Utility in, 287–293
- troubleshooting, 307–308, 311
- verifying share points in, 297

Nethomes folders, 363–366
NetInstall, 284, 291–293
NetRestore
- configuring images in, 303
- default images in, 293
- introduction to, 284

Network Address, 32–34

Network Address Translation (NAT), 437
network disk images, 299
Network File System (NFS). See NFS (Network File System)
network home folders
 generally, 361–362
 network mounts in, 362–364
 share points and, 320
 users in, 364–366
Network Install
 images in, 299
 introduction to, 284
 in NetBoot, 289
network mounts, 315, 362–364
Network preferences, 235–236
Network Time Protocol (NTP). See NTP (Network Time Protocol)
network traffic
 encrypting, 59, 137–138, 317, 319
 firewalls and, 308
 NFS, 294
 patterns of, 321–322
 received, 144
 Server Admin monitoring, 48, 130
 Server app monitoring, 42–43
 SSL for, 396–399
network user accounts. See also user accounts
 disabling, 210–211
 managing, generally, 193–194
 with Server app, 194–196, 202–208
 with Workgroup Manager, 196–202
Network Utility
 binding to other servers with, 183
 configuring Open Directory replicas with, 175–177
 confirming DNS records, 163–165
 introduction to, 10–11
 multiple OD servers, supporting, 242
 MX servers in, 446
 for network user accounts, 201–202
"New users may not have access to services," 107
NFS (Network File System)
 disk images on, 293–294
 for file sharing services, 318
 in NetBoot, 285–286
No Access permissions, 330, 335, 336
NT LAN Manager, 209
NTP (Network Time Protocol)
 in Kerberos, 235
 in Open Directory, 181
 in Time Zone pane, 29

O

Office, 281
Open Directory
 accessing log files in, 233–234
 Address Book and, 439
 another server, configuring to use, 182–188
 another server, connection to, 162–163
 another server, using generally, 158–159
 another server, using remotely, 188–193
 archiving data in, 221–224
 authentication in, generally, 209
 binding Lion to, 192–193
 configuring, generally, 165
 defined, 154–155
 disabling user accounts in, 210
 DNS records in, 163–165, 236–243
 generally, 153
 global password policies in, 215–219
 iCal and, 417
 inspecting archive contents in, 224–226
 introduction to, 51, 154
 Kerberos and, 219–221, 235–236
 locales in, 157–158
 Log in, 233–234
 masters in. See Open Directory masters
 multiple servers in, 236–243
 network user accounts in, generally, 193–196
 network user accounts, using Server app, 202–208
 network user accounts, using Workgroup Manager, 196–202
 Password Server, 209
 per-user password policies in, 211–213
 preparing to configure, 159–165
 references on, 244–245
 replicas in. See Open Directory replicas
 restoring data in, 221, 226–227
 review questions on, 246–247
 SACLs in, 124–125
 Server Admin for, 218–219, 227–233
 Server app for, 165–168, 194–196, 202–208
 service components of, 155–159
 single sign-ons in, 219–221
 single user account settings in, 213–214
 summary of, 243–244
 testing user account policies in, 214–215
 tools for configuring, 159–163
 troubleshooting, 233–236
 user account password policies in, 211–215
 user authentication in, 209–210
 Users & Groups preferences binding, 192–193
 Workgroup Manager for, 196–202

Open Directory masters
- archiving data in, 222–224
- configuring, generally, 165
- configuring servers remotely with, 190–192
- configuring with Server Admin, 227–233
- configuring with Server app, 165–168
- effects of becoming, 168–174
- global password policies in, 216, 218
- iChat in, 435
- importing network user accounts, 203–205
- inspecting archive contents, 224–226
- introducing, 156
- network mounts in, 362–363
- network user accounts and, 194–196
- preparing to configure, 159–163
- Profile Manager and, 252
- replicas and. See Open Directory replicas
- restoring data in, 226–227
- Server Admin configuring, 161–162

Open Directory replicas
- binding Lion to, 192–193
- configuring, 174–182
- importing network user accounts, 202
- introducing, 156–157
- masters and. See Open Directory masters
- preparing to configure, 162
- restoring, dangers of, 233

OpenLDAP (Lightweight Directory Access Protocol). See also LDAP (Lightweight Directory Access Protocol), 155–156

operating systems. See OS (operating systems)

Option key, 299, 307

optional ACLs (access control lists). See also ACLs (access control lists), 333–334

Organization pane, 28–29

OS (operating systems)
- installing Lion Server on, 6–8
- NetBook updating, 282
- NetBoot images and, 290
- OS X. See Mac OS X. See also OS X Lion
- OS X 10.7. See OS X Lion Server

OS X. See Mac OS X. See also OS X Lion

OS X Lion.
- Address Book on, 440–444
- DNS service on, 236–240
- local profiles on, 262
- manageable preferences payloads for, 270–273
- Open Directory for. See Open Directory
- in Profile Manager, 265
- System Image Utility on, 290
- Time Machine on, 369–370

"OS X Lion: About Lion Recovery," 78

OS X Lion Server. See also *specific services*.
- configuring. See configuration, Lion Server
- exported files from, 151
- exporting users and, 103
- installing. See installation, Lion Server
- monitoring. See monitoring Lion Server
- NetBoot on. See NetBoot
- Open Directory in. See Open Directory
- Profile Manager on. See Profile Manager
- requirements for, 2–3
- User Profile Portal for, 256
- web services of. See web services

OTA (over the air) device management, 251

Others share points, 335

outgoing email. See also email, 406, 449–450

over the air (OTA) device management, 251

Overview pane, 4–5, 321

ownership in POSIX. See POSIX

ownership with SMB, 335

P

Packages, 287

parameter random-access memory (PRAM), 299

Partition Map, 6

partitions, 6–8

passcodes, 269, 270–273

Password Server
- archiving databases in, 222
- authentication databases in, 156
- for authentication, generally, 209
- database in, 233
- for network accounts, 170
- for Open Directory replicas, 174, 180
- for restoring Open Directory data, 226–227, 230
- synchronizing with Kerberos, 216

Password Service, 233–234

passwords
- for Address Book, 445
- expired, 215–216
- exporting users and, 103
- firmware and, 307
- global policies for, 215–219
- for iCal, 423, 429
- for iChat, 438
- in Kerberos, 219–220
- login windows requiring, 86–87
- for multiple user accounts, 154
- for network user accounts, 197
- in Open Directory, 155, 167, 209
- per-user policies for, 211–213

policies for, 211–215
in production environments, 110
remembering, 88
Server Admin examining, 218–219
single user, 213–214
testing, 214–215
troubleshooting, 235
in VPN connections, 138
for wikis, 416
payloads
encrypting, 138
manageable preferences, 270–273
in Profile Manager, 270–273
PDFs, 281
per-image filters, 304–305
Permission pop-up menu, 129–130, 132
permissions
ACEs allowing, 337
ACLs for. See ACLs (access control lists)
ACLs vs., 347
authentication and. See authentication
authorization and. See authorization
complex, 341–342
in POSIX. See POSIX
propagating in ACLs, 345
protocols assigning, 336
SACLs for. See SACLs (service access control lists)
types of, 330, 336
physical network connections, 235
PKIs (public key infrastructure), 59
placeholders, 274–275
plist (preference list), 301
Podcast Composer, 44
Podcast Producer, 51, 87
POP (Post Office Protocol), 447
portability, 345
ports
for Address Book, 445
for Apple software, 138
iCal on, 429
for iChat, 430, 438
for new websites, 386–391
security of, 396–398
troubleshooting, 402
for wikis, 416
POSIX
ACLs vs. permissions in, 347
adjusting settings in, 321
introduction to, 329
ownership in, 330, 333–336
permissions in, 333–336
precedence in, 347–348
sharing protocols in, 336
WebDAV and, 335
Post-Install Scripts, 287
Post Office Protocol (POP), 447
Postfix, 445
PRAM (parameter random-access memory), 299
precedence, 347–348
preference list (plist), 301
preferences for users, 273
preferences payloads, 270–273
Primary Zone, 237, 239–241
printers, 154
private keys, 59, 61
Profile Manager
configuring, generally, 251
delivering profiles in, 268–269
device accounts in, 269, 274–275
device group accounts in, 269, 274–277
enabling, 253–256
enrolling devices in, 278
group accounts in, 269
installing profiles in, 277
introduction to, 249–250
manageable preferences payloads in, 270–273
management levels in, 251
managing profiles locally, 262–263
Mobile Device Management in, 251
Open Directory masters and, 159
preferences for user groups in, 273
preparing to configure, 252
references on, 278
remotely locking or wiping devices, 269
review questions on, 279
Software Update Service vs., 311
summary of, 278
terminology in, 252
troubleshooting, 277–278
user accounts in, 269
User Portal in, 251
User Profile Portal in, 256–262
using, 263–268
viewing logs in, 277
viewing profiles in, 277
web app in, 250, 263
Profile, VPN, 140–145
propagation of permissions, 345
protocols. See also *specific protocols*
for file sharing services, 316–319, 336
for images in NetBoot, 293–294
for permissions, 336
for share points, 317

public keys, 59, 61
Public share points, 325, 327–328
push certificates, 252
push for profiles, 269
push notifications, 254, 416

R

RADIUS, 51
RAID (Redundant Array of Independent Disks), 8
RAM, 284
Read & Write permissions
    in file sharing services, 330
    in folder hierarchies, 349–352
    in POSIX, 335–336
Read Only permissions
    for Everybody, 384
    in file sharing services, 330–331
    in folder hierarchies, 349
    in NetBoot, 285
    in POSIX, 335
    for websites, 392
    for Wiki Group, 412
    for wiki users, 413
Read permissions, 341–342, 392
realms in Kerberos, 219, 229
Recovery HD, 78
Redundant Array of Independent Disks (RAID), 8
Region pane, 23
Registration Information pane, 25
relays, 157
remote configuration, 5–6, 20–23
remote devices, 262
remote Lion Servers, 52
Remote Management, 260
"Remote Setup In Progress," 23
removal
    of profiles, 262–263
    of reverse DNS zones, 231–232, 236–240
    of unused services from Server Admin, 136–137
    of VPN Profile, 144–145
Repair Disk, 78
resources, 421–422, 427
restart computers, 295
restoration
    of files with Time Machine, 371–373
    of image files, 288
    of Open Directory data, 221, 226–227
restriction of iChat users, 435
reverse DNS records. See also DNS (Domain Name System), 10–11, 239–241
Review pane, 38
ROM (read-only) memory files, 285–286
root certificates. See also certificates, 258

S

SACLs (service access control lists). See also ACLs (access control lists)
    administering services in, 131
    administering specific services only in, 131–133
    AFP in, 118–121
    authorization in, 116–117
    binding to Open Directory servers, 187–188
    binding to other directory services, 162–163
    cleaning up, 133–136
    for collaborative services, 406
    configuring generally, 117–118
    creating new users in, 126–127
    defined, 85
    editing, 332–333
    File Sharing and, 119, 137
    GUIDs in, 337
    inspecting in Server Admin, 125–128
    inspecting in Server app, 121–125
    limited admin privileges in, 129–138
    modifying with Server app, 125
    monitoring services in, 130
    network user accounts in, 196, 201, 208
    for Open Directory masters, 160, 170–171
    removing unused services and, 136–137
    for SMB, 123
    troubleshooting, 145
    Workgroup Manager for, 126–127
Safari
    Apache error logs and, 400
    creating new websites in, 390
    enabling and disabling websites in, 384–385
    SSL certificates in, 73
    SSL websites in, 397
    web mail in, 451–453
    website access in, 393, 395
    wikis in, 408–415
safety videos, 281
Screen Sharing
    cleaning up with, 377
    confirming DNS records in, 163–165
    importing network user accounts in, 202
    inspecting file-sharing logs in, 375–376
    inspecting Open Directory archives in, 224–226
    multiple Open Directory servers in, 241–243
    Open Directory replicas in, 172–174
    other Open Directory servers in, 183
    in Server Admin, 53–54

Secure Shell. See SSH (Secure Shell)
Secure Sockets Layer. See SSL (Secure Sockets Layer)
security
  in configuring servers remotely, 191
  time sensitivity in Kerberos, 220
  of websites, 396–399
self-signed SSL certificates, 39–40, 63–68
Server Admin
  archiving Open Directory data with, 222–224
  binding to Open Directory servers with, 186–188
  cleaning up authorization with, 133–136
  configuring NetBoot servers with, 296–298
  configuring NetBoot with, 291–293
  configuring Open Directory masters with, 159–161, 170, 227–233
  configuring Open Directory replicas with, 162, 177–181
  configuring Open Directory with, 161–162
  configuring services with, generally, 45–47
  creating SACLs for SMB with, 123
  default images and protocols in, 293–294
  defining Open Directory locales with, 157–158
  Diskless checkbox in, 295
  editing SACLS in, 332
  exporting settings with, 52–53
  general settings in, 47–50
  hardware addresses in, 303
  importing network user accounts with, 207–208
  importing settings with, 52–53
  inspecting SACLs with, 125–126, 127–128
  installing, 44–45
  introduction to, 39
  limited admin privileges in, 129–133
  local users in, 129–131
  logs in, 76, 78
  monitoring Lion Server with, 45–47
  multiple Open Directory servers with, 236–240
  NTP services in, 181
  Open Directory log files in, 233–234
  Open Directory masters in, 156
  Overview pane in, 4–5, 321–322
  password policies in, 211, 214–215
  per-image filters in, 304–305
  removing unused services from, 136–137
  restoring Open Directory data with, 226–227
  for SACLs, 117
  Screen Sharing app in, 53–54
  Software Update in, 54–56
  Software Update Server in, 308–311
  System Image Utility in, 287, 290
  working with services in, 50–52
Server app
  for access in folder hierarchies, 350
  adding users to SACLs with, 102, 105
  Address Book in, 439–440
  Allow or Deny in, 347
  binding servers to Open Directory with, 158
  binding to Open Directory servers with, 182–186
  binding to other directory services with, 162
  cleaning interfaces with, 376–377
  configuring administrator accounts with, 92–93
  configuring administrator computers with, 15–20
  configuring file sharing users with, 319–320
  configuring Lion Server with, generally, 1
  configuring local user accounts with, 93–102
  configuring Open Directory masters with, 159–160, 165–168
  configuring Open Directory replicas with, 175
  configuring services to use certificates, 71–72
  configuring user accounts with, 89–92
  configuring Virtual Private Network with, 138–140
  connecting to Lion Server with, 39–43
  creating new users in SACLs with, 126–127
  creating self-signed SSL certificates with, 63–68
  Directory Utility in, 188–192
  Edit Access to Services in, 122
  editing SACLS in, 332
  Enable Webmail in, 451
  enabling File Sharing in, 117
  enabling Profile Manager in, 253
  enabling Wiki service in, 407–410
  File Sharing pane in. See File Sharing pane
  file sharing services in, 319–321
  global password policies in, 216–218
  granting administrator status with, 92–93
  home folders in, 364–366
  for iCal, 417, 420–422
  for iChat, 431, 435
  importing users from text files with, 103
  inspecting file-sharing logs with, 375–376
  inspecting network user accounts with, 200–202
  inspecting SACLs with, 121–125
  installing, 9, 12–13, 15
  Logs pane in, 76–78
  Mail service in, 448–449, 453–454
  maintenance tasks by, 321
  Manage Network Accounts in, 165–168
  managing websites with, 384–385

modifying SACLs with, 125
monitoring Lion Server with, 41–43
moving service data to volumes with, 58–59
network user accounts in, 194–196, 202–208
password policies in, 211
remote Lion Server configuration with, 20–23
Software Update in, 54–56
SSL websites in, 397–398
Stats pane in, 321
Storage pane in, 339–341
Time Machine access with, 367
troubleshooting with, 145–148
turning File Sharing off with, 137
turning File Sharing on with, 119
verifying share points with, 297
verifying website folder access with, 392–394
web services in, 385
Server Assistant
Administrator Account pane in, 25–27
Airport Management pane in, 37
Apple ID pane in, 24–25
Computer Name in, 34–35
confirming DNS records with, 163
Connecting to Your Mac pane in, 31–36
creating DNS zones with, 239–240
creating SACLs with, 118–119
DNS service in, 50
Host Name pane in, 30–31, 35–37
introduction to, 23
Keyboard pane in, 23
License Agreement pane in, 25
Multiple Networks Detected pane, 28
Network system preferences in, 32–34
Organization pane in, 28–29
Region pane in, 23
Registration Information pane in, 25
remote Lion Server configuration with, 26
Review pane in, 38
Thank You pane in, 38–39
Time Zone pane in, 29–30
Transferring an Existing Server pane in, 24
Xsan pane in, 27
Server Message Block (SMB). See SMB (Server Message Block)
Server Monitor, 44
Server pane, 24
server-side scheduling, 417
Server Status Dashboard Widget, 56–58
servers
additional, 158–159, 162–163, 182–188
administration of. See Server Admin
application for. See Server app
assistance for. See SACLs (service access control lists)
cleaning up authorization on, 133–136
components of, 9–14
configuring for NetBoot, 296–298
Directory Utility for, using remotely, 188–193
filtering, 308
NetBoot impacting performance of, 286–287
Servers list, 46–47
service components, 155–159
service data storage, 58–59
service logs, 437–438
Service Name button, 52
Services list, 51
Setup Assistant, 61
shadow files
defined, 285
of images, 294–295
troubleshooting, 307
shadow passwords, 209
share points
access with, 329–333
adding and removing, 325–327
configuring individual, 327–328
creating, generally, 323
default, 325
defined, 315
File Sharing pane for, 324–328
with Guest access, 120
for local administrators, 120
mounted, 316
in NetBoot, 286, 297
network home folders on, 362
protocols for, 317, 320, 323
Server app for, 320
shared directory services. See Open Directory
shared folders
access in, 351
configuring access to, 329
introduction to, 325
permissions for, 334
POSIX for, 336
Shared Item folders, 326, 367
shared LDAP databases, 227
shared LDAP directories, 193–194, 227
shared secrets, 138–139
shareware, 281
Sharing preferences pane, 17
short names, 90, 105–107
Show Profile, 267

signed certificates. See also SSL (Secure Sockets Layer) certificates
- Code Signing certificates, 255
- importing, 70–71
- self-signed, 39–40, 63–68
- signing requests for, 68–70

Simple Mail Transfer Protocol (SMTP). See SMTP (Simple Mail Transfer Protocol)
single sign-ons, 219–221
Sites folder, 384
SMB (Server Message Block)
- authentication and, 87
- case-sensitivity in, 375
- creating SACLs for, 123
- defined, 316–318
- disabling, 323
- guest access for, 328
- inspecting SACLs for, 126–128
- POSIX for, 335–336
- SACLs for, generally, 117
- for share points, 320–321

SMTP (Simple Mail Transfer Protocol)
- introduction to, 446
- outgoing email, 449–450
- for web mail, 457

Snow Leopard
- Server Admin Tools on, 45
- server components on, 14
- Time Machine on, 366
- upgrading existing Macs with, 3

Software Update Service. See SUS (Software Update Service)
Sort Access Control List Canonically, 348
SpamAssassin software, 455
Spamhaus Project, 455–456
sparse disk images
- archiving data with, 222, 225
- restoring data with, 231–232

SSH (Secure Shell)
- configuring SACLs for, 117–118
- in Open Directory masters, 171–172
- restoring original SACLs in, 135

SSL (Secure Sockets Layer), 396–399, 407
SSL (Secure Sockets Layer) certificates
- for Address Book, 420, 439
- binding Lion to Open Directory and, 193
- binding to other servers and, 184
- Certificate Signing Requests for, 68–70
- creating self-signed, 63–68
- default, 61–63
- for iCal, 420
- for iChat, 431, 436
- importing signed, 70–71
- introduction to, 59–61
- for new websites, 397–398
- in Open Director masters, 160
- Profile Manager and, 252
- services using, 71–72
- trusting, 39–40, 72–76
- for web mail, 451, 457
- for wikis, 408–409

Standalone Directory, 178
standalone servers, 161–162, 226–227
startup delays, 235
Startup Disk pane, 287, 299–300
startup, in NetBoot, 284–286, 299
Startup Manager, 299
startup volumes, 285–286, 295
Statistics, 43
Stats pane, 321
storage of shadow files, 295
Storage pane
- adjusting settings over time, 321
- introduction to, 41–43
- in Server app, 339–341

Store Site Files In, 387, 389, 396
streams, multicast, 303
subnets, 157
SUS (Software Update Service)
- configuring computers for, 311
- individual updates in, 310–311
- for monitoring, 54–56
- for NetBoot, 308–311
- Profile Manager vs., 311
- Server Admin and, 54–56
- troubleshooting, 311
- updating with, generally, 54–56

System Administrator, 329
System Configuration Settings, 287
System CPU, 42
System Image Utility
- Automator Library and, 301
- creating images with, 287–293
- image types in, 288
- installing, 44
- introduction to, 281–282
- for NetBoot, 290–293

System Information, 5
System keychains. See keychains
System Preferences
- binding Lion to Open Directory with, 192–193
- introduction to, 17–20

managing profiles locally with, 262
Profile Manager web app and, 267–268
Startup Disk pane in, 287, 299–300
Time Machine on, 369, 373
system requirements, 3–6

T

T key, 300
Target Disk Mode, 293, 300
TCP (Transfer Control Protocol), 138, 318
Terminal app, 322–323
test networks, 15–16
text messages. See iChat
TextEdit
in Launchpad, 371
for new websites, 388, 396
in Workgroup Manager, 108, 110–112
TextImport, 113–116
TFTP (Trivial File Transfer Protocol), 285–286
TGT (Ticket Granting Ticket), 220
Thank You pane, 38–39
tickets in Kerberos, 219–221, 235–236
Time Machine
backups in, 370–371
configuring destinations in, 367–368
introduction to, 366–367
on Lion computers, 369–370
restoring destinations in, 371–373
time sensitivity, 220–221
Time Zone pane, 29–30
timestamps, 181, 235
traffic. See network traffic
Transfer Control Protocol (TCP), 138, 318
Trash, 371–372
Trivial File Transfer Protocol (TFTP), 285–286
troubleshooting
Address Book, 445
file services, 374
iCal, 429
iChat, 438
Lion Server installation, 76–78
mail services, 457
NetBoot, 307–308, 311
Open Directory, 233–236
Profile Manager, 277–278
SACLs, 145
Software Update, 311
user accounts, 146–147
VPN service, 147–148
Wiki service, 416
Workgroup Manager, 107–108
trusted CAs (Certificate Authorities). See also CAs (certificate authorities), 72–76, 172–173
trusted profiles, 257–258, 277–278
trusted SSL (Secure Sockets Layer) certificates. See also SSL (Secure Sockets Layer) certificates
for binding to Open Directory, 193
configuring, 59–61
for Open Directory servers, 184
verifying, 40

U

UDP (User Datagram Protocol), 138
UIDs (user IDs). See user IDs (UIDs)
UNICODE, 317
UNIX, 318
updates for software. See SUS (Software Update Service)
URLs, 311, 317, 384
user accounts
access of, 86–87
administering, generally, 88
Advanced Options for, 90–91
authentication of, 209–210
configuring with Server app, 89–92
creating with Server app, 126–127
creating with Workgroup Manager, 104–107, 126–127
disabling, 210
email, 450, 453–454
formatted lists of, 108–110
global password policies for, 215–219
in iCal, 422–428
in iChat, 433–435
IDs for. See user IDs (UIDs)
Kerberos defining, 219
local. See local users
manageable preferences payloads for, 270–273
managing. See Profile Manager
network. See network user accounts
in network home folders, 364–366
password policies for, 211–215
per-user password policies for, 211–213
SACLs for. See SACLs (service access control lists)
Server Admin for, 218–219
single user account settings, 213–214
System Image Utility for, 287
testing policies for, 214–215
text lists of, 110–116
troubleshooting, 146–147
Workgroup Manager for, generally, 102–104
User CPU, 42

User Datagram Protocol (UDP), 138
user IDs (UIDs)
  in ACLs, 336
  introduction to, 91–92
  of Local Admin, 104
  sorting user list by, 107
  in Workgroup Manager, 107
User Portal, 250–251, 268–269
User Profile Portal, 256–262
users. See user accounts
Users & Groups
  binding to Open Directory with, 162, 182–185, 192–193
  binding to other OD servers with, 208
  cleaning up authorization with, 135–136
  configuring administrator computers with, 19
  Directory Utility vs., 188
  limiting admin privileges for, 129
  Nethomes in, 364–365
  preferences in, 192–193
  system preferences in, 88
  troubleshooting, 235
Users pane
  for access in folder hierarchies, 350
  adjusting settings over time, 321
  editing SACLS in, 332
  iCal on, 417
  Time Machine access with, 367
Users share points, 325, 329
"Using an Apple ID," 120
Utilities folders, 6, 10–11

V
verification
  of folder access, 392
  of share points, 297
  of trusted certificates, 40, 72–76
Verisign, 69–74
video conferences. See iChat
View Document Root Contents, 387, 392
views
  of Apache log files, 399–402
  of default certificates, 61–63
  of Profile Manager logs, 277
  of Profile Manager profiles, 277
  of website parameters, 386–387
Virtual Private Network. See VPN (Virtual Private Network)
virus scans, 454–455
volumes
  boot, 406
  copying items in, 334
  installing Lion Server on, 6–7
  installing on empty, 14–15
  mounted, 290
  moving service data to new, 58–59
  in NetBoot startup, 285, 287
  RAID, 8
  service data on, 58–59
  in Time Machine, 367–368
  update packages on, 309
VPN (Virtual Private Network)
  configuring, 137–138
  installing, 140–144
  passwords in, 209
  removing, 144–145
  Server app for, 138–140

W
web app in Profile Manager, 250
Web-based Distributed Authoring and Versioning. See WebDAV (Web-based Distributed Authoring and Versioning)
web mail. See also email, 451–453
web services. See also collaborative services
  Apache log files, 399–402
  introduction to, 383
  monitoring, generally, 399
  references on, 403
  review questions on, 403
  starting in Server app, 385
  summary of, 402
  troubleshooting, 402
WebDAV (Web-based Distributed Authoring and Versioning)
  inspecting logs in, 375–376
  introduction to, 316–319
  POSIX and, 335–336
  for share points, 320–321
websites
  access to, 393–396
  basic concepts of, 384
  creating new, 388–391
  delivering profiles via, 269
  disabling, 384–385
  enabling, 384–385
  folder access by, 392–394
  managing, generally, 386

parameters of, 386–387
references on, 403
review questions on, 403
security of, 396–399
SSL for, 396–399
summary of, 402
well-known ports, 138
Who Can Access, 387–389, 393–394, 396
Wi-Fi, 284
Wiki Group, 409, 412
Wiki service
binding to other directory services, 162
creating wikis in, 410–415
data stores in, 406
enabling in Server app, 407–410
troubleshooting, 416
Wiki User, 410
wikis. See also Wiki service, 406–407, 428
Workgroup, 169–170, 194
Workgroup Manager
creating new users with, 104–107, 126–128
disabling user accounts with, 210–211
exporting users with, 102–104, 107–108
formatted lists of users in, 108–110
global password policies in, 217–218
importing users with, 102–104
installing, 44
network user accounts in, 196–202
password policies in, 211–214
Profile Manager vs., 250–251
restoring network users in, 232
Server app vs., 194
text lists of users in, 110–116
troubleshooting, 147–148
Write Only permissions, 330
Write permissions, 341–342

X

Xgrid, 44, 51
XML (eXtensible Markup Language)
downloading profile preferences, 267
exporting users in, 108
in profiles, 250
XMPP (Extensible Messaging and Presence Protocol), 430, 436
Xsan, 27, 417

Z

zones in DNS. See also DNS (Domain Name System), 236–241