Apple Pro Training Series

OS X Server 5.0 Essentials

Using and Supporting OS X Server on El Capitan

Arek Dreyer and Ben Greisler

Apple Certified

Lesson and media files available for download

This page intentionally left blank

Apple Pro Training Series

OS X Server 5.0 Essentials

Arek Dreyer and Ben Greisler

Apple Certified

Apple Pro Training Series: OS X Server 5.0 Essentials
Arek Dreyer and Ben Greisler

Peachpit Press
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: Maureen Forys, Happenstance Type-O-Rama
Technical Editor: Adam Karneboge
Apple Reviewer: Susan Najour
Copy Editors: Darren Meiss, Kim Wimpsett
Proofreader: Darren Meiss
Compositor: Cody Gates, Happenstance Type-O-Rama
Indexer: Jack Lewis
Cover Illustration: Paul Mavrides
Cover Production: Cody Gates, Happenstance Type-O-Rama

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 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.

IMPORTANT: Some of the exercises contained in this guide can be temporarily disruptive, and some exercises, if performed incorrectly, could result in data loss or damage to system files. As such, it's recommended that you perform these exercises on a Mac computer that is not critical to your daily productivity.

ISBN 13: 978-0-13-443477-3
ISBN 10: 0-13-443477-3
9 8 7 6 5 4 3 2 1 Printed and bound in the United States of America

Thanks to my lovely wife, Heather Jagman, for her cheerful support. And congratulations to her on the publication of her recent first book.

—Arek Dreyer

I am a lucky man having my wife, Ronit, and my children, Galee and Noam, supporting me throughout this project. Without them, continued work on these books would be impossible.

—Ben Greisler

Acknowledgments Thank you to Tim Cook, Jonathan Ive, and everyone at Apple for continually innovating, surprising, and delighting customers. And Steve Jobs for having the vision to start it all.

Thank you to all the people who continue to help their users get the most out of OS X and iOS. Keep learning, and don't expect the pace of change to let up any time soon.

Thanks to the amazingly capable Lisa McClain, for gently making sure these materials made it into your hands, and to Darren Meiss, Kim Wimpsett, and Happenstance Type-O-Rama for working their editorial and production magic.

Thanks to Adam Karneboge for adept corrections and suggestions.

Thanks to Schoun Regan for all his help.

Thank you, also, to the following people. Without your help, this book would be much less than what it is:

Craig Cohen

Gordon Davisson

Weldon Dodd

Josh Durham

Charles Edge

Patrick Gallagher

Patrik Jerneheim

Andre LaBranche

Steve Leebove

Ben Levy

Susan Najour

John Poynor

John Signa

Cindy Waller

Simon Wheatley

Kevin White

Eric Zelenka

Contents at a Glance

About This Guide xiii

Configuring and Monitoring OS X Server

Lesson 1 Installing OS X Server 3
Lesson 2 Providing DNS Records 57
Lesson 3 Exploring the Server App 83
Lesson 4 Configuring SSL Certificates 113
Lesson 5 Using Status and Notifications 157
Lesson 6 Backing Up OS X Server 173

Configuring Accounts

Lesson 7 Configuring Open Directory Services 191
Lesson 8 Managing Users 219

Managing Devices with Configuration Profiles

Lesson 9 Configuring OS X Server to Provide Device Management 277
Lesson 10 Managing with Profile Manager 295

Sharing Files

Lesson 11 Configuring the File Sharing Service 335
Lesson 12 Defining File Access 377

Implementing Deployment Solutions

Lesson 13 Leveraging NetInstall 421
Lesson 14 Caching Content from Apple 451
Lesson 15 Implementing the Software Update Service 465

Providing Network Services

Lesson 16 Offering Time Machine Network Backup 471
Lesson 17 Providing Security via the VPN Service. 483
Lesson 18 Configuring DHCP 501
Lesson 19 Hosting Websites 521

Using Collaborative Services

Lesson 20 Providing Mail Service 555
Lesson 21 Configuring the Wiki Service 581
Lesson 22 Implementing the Calendar Service 593
Lesson 23 Managing the Contacts Service 609
Lesson 24 Providing the Messages Service 619

Using Command Line

Lesson 25 Managing OS X Server with the Command-Line Interface 639

Index 681

Table of Contents

About This Guide xiii

Configuring and Monitoring OS X Server

Lesson 1 Installing OS X Server. 3

Reference 1.1 Evaluating OS X Server Requirements 4

Reference 1.2 Preparing to Install OS X Server. 7

Reference 1.3 Installing OS X Server 16

Reference 1.4 Upgrading or Migrating to OS X Server 17

Reference 1.5 Updating OS X Server 19

Reference 1.6 Troubleshooting 19

Exercise 1.1 Configure OS X Before Installing OS X Server on Your Server Computer 20

Exercise 1.2 Perform the Initial Installation of OS X Server on Your Server Computer 36

Exercise 1.3 Configure Your Client Computer. 43

Exercise 1.4 Configure Your Client iOS Device 53

Lesson 2 Providing DNS Records 57

Reference 2.1 What Is DNS? 57

Reference 2.2 Evaluating OS X DNS Hosting Requirements 59

Reference 2.3 Configuring DNS Service in OS X Server. 62

Reference 2.4 Troubleshooting DNS Service in OS X Server 64

Exercise 2.1 Create DNS Zones and Records 65

Exercise 2.2 Restrict Access to the DNS Service 76

Lesson 3 Exploring the Server App 83
Reference 3.1 Allowing Remote Access 83
Reference 3.2 Using Server Sidebar Elements 86
Reference 3.3 Using the Manage Menu 99
Reference 3.4 Using the Tools Menu. 100
Reference 3.5 Using Help and Server Tutorials 100
Reference 3.6 Troubleshooting 102
Exercise 3.1 Turn On Remote Access 103
Exercise 3.2 Inspect the Service Data Volume 105
Exercise 3.3 Explore the Access Tab. 106

Lesson 4 Configuring SSL Certificates 113
Reference 4.1 Describe SSL Certificate Basics. 113
Reference 4.2 Configuring SSL Certificates. 118
Reference 4.3 Troubleshooting 142
Exercise 4.1 Examine the Default SSL Certificate 143
Exercise 4.2 Configure an Open Directory Certificate Authority. 145
Exercise 4.3 Configure Your Client Computer
to Trust an SSL Certificate. 152

Lesson 5 Using Status and Notifications 157
Reference 5.1 Using Monitoring and Status Tools 157
Reference 5.2 Configuring OS X Server Alerts. 158
Reference 5.3 Using Logs in OS X Server 161
Reference 5.4 Using Stats in OS X Server 163
Reference 5.5 Viewing Storage Space 165
Exercise 5.1 Use the Server App to Monitor Your Server. 165

Lesson 6 Backing Up OS X Server. 173
Reference 6.1 Describing Backup Concepts 173
Reference 6.2 Backing up with Time Machine 175
Exercise 6.1 Use Time Machine to Back Up OS X Server. 177
Exercise 6.2 Inspect Time Machine Backup Files 181

Configuring Accounts

Lesson 7 Configuring Open Directory Services 191
Reference 7.1 Introducing Directory Service Concepts. 191

Reference 7.2 Configuring Open Directory Services 199
Reference 7.3 Troubleshooting 209
Exercise 7.1 Back Up and Restore Open Directory 211

Lesson 8 Managing Users 219
Reference 8.1 Describing Authentication and Authorization 220
Reference 8.2 Creating and Administering User and Administrator Server Accounts. 222
Reference 8.3 Managing Access to Services. 237
Reference 8.4 Configuring Authentication Methods on OS X Server. 239
Reference 8.5 Using Single Sign-On and Kerberos. 242
Reference 8.6 Troubleshooting 247
Exercise 8.1 Create and Edit User Accounts 249
Exercise 8.2 Import Accounts 257
Exercise 8.3 Configure Password Policies 265
Exercise 8.4 Manage Service Access. 269

Managing Devices with Configuration Profiles

Lesson 9 Configuring OS X Server to Provide Device Management 277
Reference 9.1 Administering the Profile Manager Service 277
Reference 9.2 Configuring Profile Manager 278
Exercise 9.1 Turn On Profile Manager 285

Lesson 10 Managing with Profile Manager 295
Reference 10.1 Introducing Account Management 295
Reference 10.2 Troubleshooting 310
Exercise 10.1 Use Profile Manager for Shared Devices 311
Exercise 10.2 Use Profile Manager for One-to-One Devices 320

Sharing Files

Lesson 11 Configuring the File Sharing Service 335
Reference 11.1 Addressing the Challenges of File Sharing 336
Reference 11.2 Creating Share Points 345
Reference 11.3 Troubleshooting File-Sharing Services 355
Reference 11.4 Providing FTP Service 355

Exercise 11.1 Explore the File Sharing Service 358
Exercise 11.2 Access Files via iOS (Optional). 370
Exercise 11.3 Use Logs to Troubleshoot Problems with File Sharing 375

Lesson 12 Defining File Access 377
Reference 12.1 Configuring Access to Share Points and Folders 377
Reference 12.2 Comparing POSIX Permissions to ACL Settings. 383
Exercise 12.1 Configure Access Control 400

Implementing Deployment Solutions

Lesson 13 Leveraging NetInstall 421
Reference 13.1 Managing Computers with NetInstall 422
Reference 13.2 Creating Images with System Image Utility 426
Reference 13.3 Describing Shadow Files 431
Reference 13.4 Troubleshooting NetInstall 433
Exercise 13.1 Prepare the NetInstall Service. 433
Exercise 13.2 Create a Customized NetInstall Image 435
Exercise 13.3 Start the NetInstall Service 442
Exercise 13.4 Start Up from a NetInstall Image 446
Exercise 13.5 Monitor the NetInstall Service 448

Lesson 14 Caching Content from Apple. 451
Reference 14.1 Describing the Caching Service 451
Reference 14.2 Configuring and Maintaining the Caching Service. 455
Reference 14.3 Comparing the Software Update and Caching Services 459
Reference 14.4 Troubleshooting the Caching Service 461

Lesson 15 Implementing the Software Update Service 465
Reference 15.1 Managing Software Updates 465
Reference 15.2 Troubleshooting the Software Update Service 467

Providing Network Services

Lesson 16 Offering Time Machine Network Backup 471
Reference 16.1 Configuring Time Machine as a Network Service. 472
Exercise 16.1 Configure and Use the Time Machine Service. 475

Lesson 17 Providing Security via the VPN Service 483
Reference 17.1 Describing VPNs. 483
Reference 17.2 Configuring the VPN Service with the Server App. 484
Reference 17.3 Troubleshooting 490
Exercise 17.1 Configure the VPN Service. 491
Exercise 17.2 Clean Up. 498

Lesson 18 Configuring DHCP 501
Reference 18.1 Describing How DHCP Works. 502
Reference 18.2 Configuring DHCP Service. 505
Reference 18.3 Troubleshooting DHCP 511
Exercise 18.1 Configure the DHCP Service (Optional) 514

Lesson 19 Hosting Websites 521
Reference 19.1 Identifying the Web Service Software 521
Reference 19.2 Describing Basic Website Structure 522
Reference 19.3 Monitoring Web Services. 528
Reference 19.4 Troubleshooting 529
Exercise 19.1 Turn On Web Services 529
Exercise 19.2 Modify the Default Websites. 533
Exercise 19.3 Create and Remove a New Website 540
Exercise 19.4 Restrict Access to a Website 547
Exercise 19.5 Monitor Web Services 549

Using Collaborative Services

Lesson 20 Providing Mail Service 555
Reference 20.1 Hosting Mail Services. 555
Reference 20.2 Troubleshooting Mail Services 563
Exercise 20.1 Turn On the Mail Service 564
Exercise 20.2 Create a Configuration Profile for Mail Settings 569
Exercise 20.3 Send and Receive Mail 573
Exercise 20.4 Examine Mail Service Logs 578

Lesson 21 Configuring the Wiki Service 581
Reference 21.1 Configuring and Managing a Wiki 581
Reference 21.2 Troubleshooting the Wiki Service 584

Exercise 21.1 Turn On the Wiki Service 585
Exercise 21.2 Edit a Wiki 589

Lesson 22 Implementing the Calendar Service 593
Reference 22.1 Describing Calendar Service Data Locations 593
Reference 22.2 Using the Calendar Service 594
Reference 22.3 Troubleshooting the Calendar Service. 598
Exercise 22.1 Configure and Start the Calendar Service. 598
Exercise 22.2 Use the Calendar Service 602

Lesson 23 Managing the Contacts Service. 609
Reference 23.1 Introducing the Contacts Service 609
Reference 23.2 Troubleshooting the Contacts Service 610
Exercise 23.1 Configure the Contacts Service 611
Exercise 23.2 Use the Contacts Service 612

Lesson 24 Providing the Messages Service. 619
Reference 24.1 Managing the Messages Service 619
Reference 24.2 Troubleshooting the Messages Service. 624
Exercise 24.1 Set Up the Messages Service 624
Exercise 24.2 Use the Messages Service. 626

Using Command Line

Lesson 25 Managing OS X Server with the Command-Line Interface. 639
Reference 25.1 Command-Line Basics 639
Reference 25.2 Command-Line Navigation. 645
Reference 25.3 Command-Line File Manipulation 652
Reference 25.4 Command-Line Administration. 661
Reference 25.5 Command-Line Tips and Tricks. 665
Exercise 25.1 Explore the Command-Line Interface. 667
Exercise 25.2 Explore the serveradmin Command 675

Index 681

About This Guide

GOALS

- Learn how this guide is organized to facilitate learning
- Set up an environment for self-paced exercises

This guide serves as a tour of the breadth of functionality of OS X Server and the best methods for effectively supporting users of OS X Server systems. It is for both self-paced learners working independently and those participating in an instructor-led course.

The primary goal of this guide is to prepare technical coordinators and entry-level system administrators for the tasks demanded of them by OS X Server; you will learn how to install and configure OS X Server to provide network-based services, such as configuration profile distribution and management, file sharing, authentication, and collaboration services. To help you become truly proficient, this guide covers the theory behind the tools you will use. For example, not only will you learn how to use 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 OS X Server computer can grow into a 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 guide assumes you have some knowledge of OS X, because OS X Server is an app that you install on OS X (Yosemite or El Capitan). Therefore, you should be comfortable with basic navigation, troubleshooting, and networking in OS X. When working through this guide, a basic understanding and knowledge of OS X is preferred, including knowledge of how to troubleshoot the operating system. Refer to Apple Pro Training Series: OS X Support Essentials 10.11 from Peachpit Press if you need to develop a solid working knowledge of OS X.

NOTE ► Unless otherwise specified, all references to OS X refer to version 10.11, and references to OS X Server refer to version 5.0, which at the time of this writing is the most current version available. You can install Server 5 on OS X 10.10, but some features are not available. Some screenshots, features, and procedures may be slightly different from those presented on these pages because of subsequent upgrades.

Learning Methodology

Each lesson in this guide is designed to give technical coordinators and entry-level system administrators the skills, tools, and knowledge to implement and maintain a network that uses OS X Server by doing the following:

- Providing knowledge of how OS X Server works
- Showing how to use configuration tools
- Explaining troubleshooting and procedures

The exercises contained within this guide are designed to let you explore and learn the tools necessary to manage OS X Server for El Capitan. They move along in a predictable fashion, starting with installing and setting up OS X Server and moving to more advanced topics such as performing multiprotocol file sharing, using access control lists, and permitting OS X Server to manage network accounts. It is required that you start from a Mac that is not yet running OS X Server and that you do not use this server as a production server.

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

OS X Server is by no means difficult to set up and configure, but you should plan in advance how you use OS X Server. Accordingly, this guide is divided into eight parts:

- Part 1, “Configuring and Monitoring OS X Server,” covers planning, installation, initial configuration, and monitoring of OS X Server.
- Part 2, “Configuring Accounts,” defines authentication and authorization, access control, and Open Directory and the vast functionality it can provide.

- Part 3, "Managing Devices with Configuration Profiles," covers managing devices with the Profile Manager service.
- Part 4, "Sharing Files," introduces the concept of sharing files over multiple protocols and controlling access to files with access control lists.
- Part 5, "Implementing Deployment Solutions," teaches you how to effectively use deployment services, NetInstall, the Caching service, and the Software Update service.
- Part 6, "Providing Network Services," introduces the network services, including Time Machine, VPN, DHCP, and Websites.
- Part 7, "Using Collaborative Services," focuses on setting up collaboration services together, starting with Mail, moving through Wiki, Calendar, and Contacts, and finishing with the Messages service.
- Part 8, "Using Command Line," is a single lesson that introduces you to administering your server using the command-line interface.

Lesson Structure

Most lessons in this guide contain a reference section followed by an exercise section (the lessons on Caching and Software Update services do not contain exercises).

> **NOTE ▸** "Note" resources, like this one, offer important information to help clarify a subject. For example, some of the exercises in this guide may be disruptive. Consequently, perform these exercises on an OS X computer that is not critical to your daily productivity.

The reference sections contain initial explanatory material that teaches essential concepts. The exercise sections augment your understanding of concepts and develop your skills through step-by-step instruction for both self-paced learners and the hands-on portions of an instructor-led course.

> **TIP** "Tip" resources, like this one, provide helpful hints, tricks, or shortcuts. For example, each lesson begins with an opening page that lists the learning goals and necessary resources for the lesson.

> **MORE INFO ▸** The "More Info" resources, like this one, provide ancillary information. These resources are merely for your edification and are not considered essential for the coursework.

Throughout this guide you'll find references to Apple Support articles. You can find these articles at the Apple Support website (www.apple.com/support), a free online resource containing the latest technical information for Apple products. We strongly encourage you to read the suggested articles and search the Apple Support website for answers to any problems you encounter.

We encourage you to explore additional resources that Apple provides specifically for OS X Server: OS X Server Support (https://help.apple.com/serverapp/mac/5.0/).

Lesson files are available online when you redeem the access code supplied with your guide at www.peachpit.com/redeem. Detailed instructions for downloading files are provided later in this guide. An "Updates and Errata" document will contain updates and corrections to the guide if any are available.

Exercise Setup

This guide is written so that both the self-paced learner and the attendee of an instructor-led class can complete most of the exercises using the same techniques. Those attending a class may have the exercise setup provided as part of the training experience. Self-paced learners attempting these exercises will have to set up an appropriate environment using their own equipment.

> **NOTE ▸** Some of these exercises can be disruptive (for example, turning on the DHCP service may prevent devices on the local network from being able to browse Internet), and some exercises, if performed incorrectly, could result in data loss or damage to files. As such, perform these exercises on an isolated network, using OS X computers and iOS devices that are not critical to your daily productivity. Apple, Inc., and Peachpit Press are not responsible for any data loss or any damage to any equipment that occurs as a direct or indirect result of following the procedures described in this guide.

Mandatory Requirements

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

- Two Mac computers, each with OS X Yosemite or El Capitan (preferred). One Mac is referred to as your "client computer," and the Mac on which you will install OS X Server is referred to as your "server computer" or, more simply, your "server." After you are done using your server computer with this guide, you should erase and reinstall OS X on its startup volume before using it again in a production environment.

- An Apple ID that is associated with a verified email address so you can obtain Apple Push Notification service (APNs) certificates for Server app notifications and for the Profile Manager service. You can create an Apple ID at the appropriate time during an exercise if you don't already have an Apple ID.
- A valid licensed copy of OS X Server from the Mac App Store.
- An Internet connection for obtaining APNs certificates for alerts and for the Profile Manager service.
- An isolated network or subnet with an exercise-specific configuration. This can be facilitated with something as simple as a small network Wi-Fi router with multiple Ethernet ports. For example, Apple AirPort Extreme is a good choice. You can find instructions for the general setup of an exercise network and specific instructions for the configuration of AirPort Extreme at www.apple.com/airport-extreme.
- A router (such as AirPort Extreme) to connect the small isolated network to the Internet, and familiarity with how to configure it.
- Two Ethernet network cables (to complete the NetInstall exercises); each Ethernet cable will connect a Mac to the Ethernet switch.
- Student Materials demonstration files, which you can download after registering your guide with Peachpit. Instructions for registration and download are included in Exercise 1.1, "Configure OS X Before Installing OS X Server on Your Server Computer."

Optional Add-Ons

If a specific resource is required for an optional exercise, it will be listed as a prerequisite at the beginning of that exercise. Here are some examples:

- An iOS device to test access to OS X Server services, including the Profile Manager service
- A Wi-Fi access point (preferably the same AirPort base station) to provide wireless access for iOS devices to your private network
- For Exercise 18.1, "Configure the DHCP Service (Optional)": To provide DHCP on an extra isolated network, you need either an additional built-in Ethernet port on your Mac (for example, if your server computer is a Mac Pro) or a USB to Ethernet adapter or a Thunderbolt to Gigabit Ethernet Adapter; and an extra Ethernet network switch

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 screenshots to understand the procedures demonstrated.

Network Infrastructure

As was previously stated, the exercises require an isolated network. Replicate the instructor-led classroom environment, which is described in the next sections, as closely as possible so that you do not need to translate between the exercise instructions and your situation.

IPv4 Addresses

The instructor-led environment provides an IPv4 network with a gateway of 10.0.0.1 and subnet mask of 255.255.255.0; if possible, configure your internal network with the same parameters.

Many consumer-level routers are configured with a gateway of 192.168.1.1 and a subnet mask of 255.255.255.0. You might not be able to change this on your router; in many cases you will be able to replace the "10.0.0" portion of an IPv4 address in the exercise with a value appropriate for your isolated network (for example, 192.168.1.171 instead of 10.0.0.171 for a server address for student 17). You will need to remember to substitute your network prefix throughout the exercises.

DHCP

The classroom DHCP service provides IPv4 addresses in the range of 10.0.0.180 to 10.0.0.254; if possible, configure your internal network's DHCP service with the same parameters. It will be helpful to know how to define the IP addresses of DNS servers being provided by DHCP.

If you can configure your isolated network's DHCP service, configure it to use a similar range of IPv4 addresses. If you are unable to change the range of IPv4 addresses, the DHCP service may assign to a device an IPv4 address already in use by your server computer or your administrator computer. This is another reason to keep your network isolated; do not introduce new devices to it.

Domain Names

The exercises and reference material in this guide use the Internet domains pretendco.com, pretendco.private, and megaglobalcorp.com, which are for learning environments only; do not attempt to use these in your production environment.

The exercises are written in such a way that any existing DNS service on your isolated network will be ignored so that you can experience your server setting up the DNS service for itself.

Advanced Administrators

If you already have advanced server administration skills, you may choose to use different settings, including your organization's Internet domain (instead of pretendco.com), your organization's DNS service, and a different IPv4 address scheme, but be warned that this introduces a high level of variability that the exercises cannot address in the given space, and be prepared to modify the exercises on your own as necessary.

Exercise Order

The exercises in this guide are designed to be relatively independent of each other so that you can perform them out of order or skip exercises you are not interested in. However, some exercises you must perform in the correct order, and where appropriate, an exercise lists these prerequisites. Here are some examples:

- You must perform all the exercises in Lesson 1 "*Installing OS X Server*" to install OS X Server and configure your administrator computer before performing any other exercises.
- You must perform Exercise 4.2, "Configure an Open Directory Certificate Authority" and Exercise 8.2, "Import Accounts" to create users who you will use in later exercises; otherwise, if the prerequisites for an exercise include the user account used in the lesson, you can simply create those user (and possibly) group accounts with the Server app's Users pane.
- Several exercises in Part 7, "Using Collaborative Services" instruct you to use a configuration profile to help users access services on your server. You must perform Exercise 9.1, "Turn On Profile Manager" before you can create or modify a configuration profile in exercises, including the following:

  Exercise 20.2, "Create a Configuration Profile for Mail Settings"

  Exercise 21.1, "Turn On the Wiki Service"

  Exercise 21.2, "Edit a Wiki"

  Exercise 22.2, "Use the Calendar Service"

  Exercise 23.2, "Use the Contacts Service"

  Exercise 24.2, "Use the Messages Service"

Lesson 4

Configuring SSL Certificates

You can use OS X Server without doing any additional work to secure its services. However, you can use the Secure Sockets Layer (SSL) technology to prove your server's identity to client computers and devices and to encrypt communication between your server and client computers and devices. This lesson starts by describing the basics of SSL and then shows you how to configure SSL certificates for use with OS X Server.

GOALS

- Describe the basics of SSL certificates
- Create a certificate signing request
- Create a self-signed SSL certificate
- Import a certificate signed by a certificate authority
- Archive your certificate
- Renew your certificate
- Configure which certificate your OS X Server services use

Reference 4.1
Describe SSL Certificate Basics

You want the users who use your server's services to trust your server's identity and to be able to encrypt network traffic with your server.

The OS X solution is to use SSL, which is a system for transmitting data securely between hosts. You can configure your server to use an SSL certificate, which provides the ability to use the SSL system.

An SSL certificate (also referred to as simply a *certificate*) is a file that identifies the certificate holder. A certificate specifies the permitted use of the certificate and has an expiration date. Importantly, a certificate includes a public key infrastructure (PKI) public key.

PKI involves the use of public and private keys. Grossly simplified, a *key* is a cryptographic blob of data, and within PKI, public and private keys are created in a way that they are mathematically linked: Data encrypted with one key can be decrypted only by using the other key. If you can decrypt data with one key, it proves that the data was encrypted with the other key. The public key is made publicly available, and the private key should be kept private. Fortunately, all of this encryption and decryption happens behind the scenes and is the basis for establishing secure communications.

Here are some definitions:

A *digital identity* (or more simply, an *identity*) is an electronic means of identifying an entity (such as a person or a server). An identity is the combination of a certificate (which includes the public key) and the corresponding private key. If you don't have your private key, you can't prove your identity. Similarly, if another entity has your private key, that other entity can claim your identity, so be sure to keep your private key private!

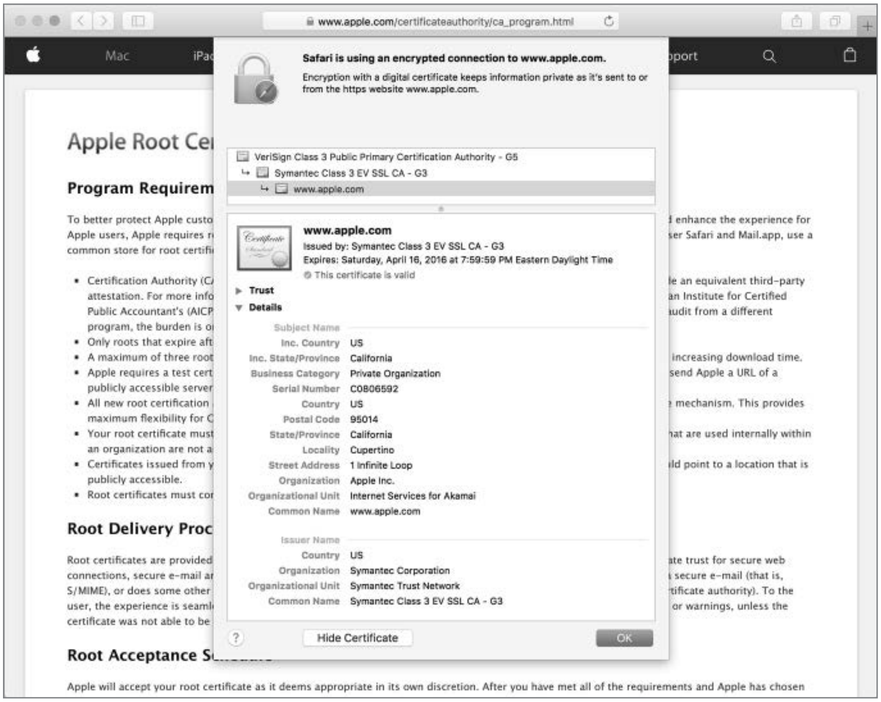
Again simplifying, a *digital signature* is a cryptographic scheme that uses PKI private and public keys to demonstrate that a given message (a digital file such as an SSL certificate) has not been changed since the signature was generated. If a message, which has been signed, changes or is otherwise tampered with, it will be clear that the signature no longer matches the underlying data. Therefore, you can use a digital signature on a certificate to prove its integrity.

A certificate must be either self-signed or signed by a *certification authority* (also known as a certificate authority or, more simply, a CA). In other words, you can sign your own certificate using your private key (remember that a certificate is a file that identifies the holder of the certificate and includes the public key), or you can have someone else, namely, a CA, use their private key to sign your certificate.

An intermediate CA is a CA whose certificate is signed by another CA. So, it's possible to have a hierarchical "chain" of certificates, where an intermediate CA, which in turn is signed by yet another CA, signs a certificate.

In the following figure, the certificate for www.apple.com is signed by an intermediate CA with the name of Symantec Class 3 EV SSL CA - G3, and that intermediate CA is signed by a CA with the name of Symantec Class 3 Public Primary Certification Authority - G5.

You can follow a chain of certificates, starting with a signed certificate, up to the intermediate CA and ending at the top of the chain. The certificate chain ends with a CA that signs its own certificate, which is called a root CA. You aren't required to have an intermediate CA—you could simply have a root CA sign your certificate—but in modern practice, an intermediate CA is often involved.



www.apple.com/certificateauthority/ca_program.html

Safari is using an encrypted connection to www.apple.com.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.apple.com.

VeriSign Class 3 Public Primary Certification Authority - G5
↳ Symantec Class 3 EV SSL CA - G3
↳ www.apple.com

www.apple.com
Issued by: Symantec Class 3 EV SSL CA - G3
Expires: Saturday, April 16, 2016 at 7:59:59 PM Eastern Daylight Time
This certificate is valid

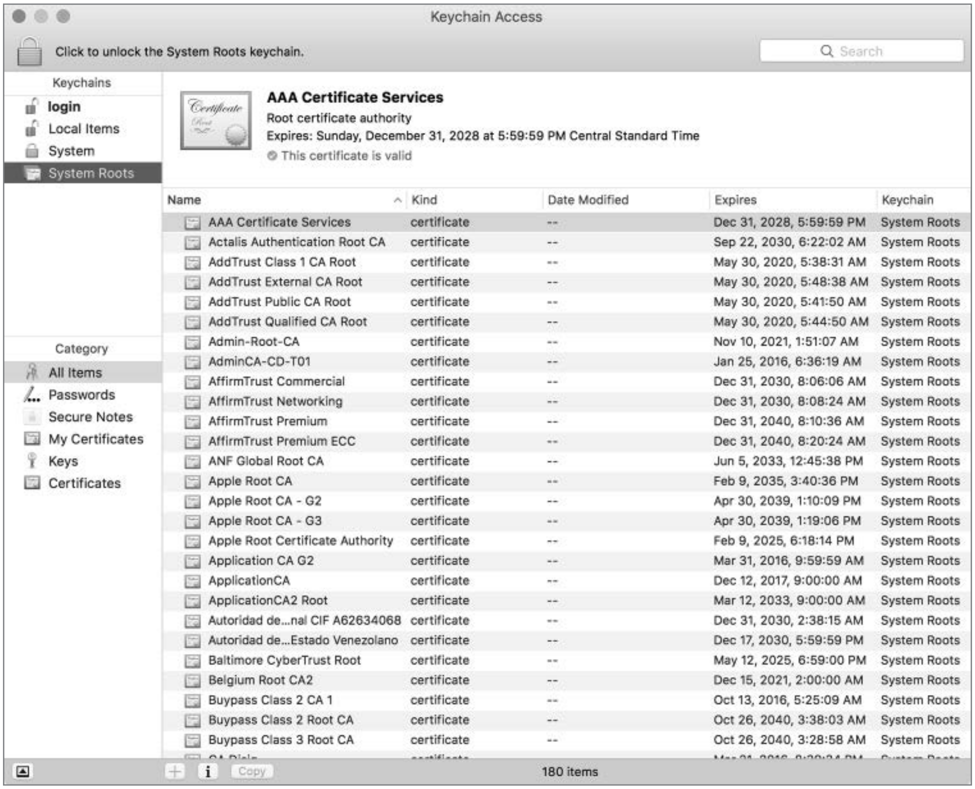
▶ Trust
▼ Details

Subject Name
Inc. Country US
Inc. State/Province California
Business Category Private Organization
Serial Number C0806592
Country US
Postal Code 95014
State/Province California
Locality Cupertino
Street Address 1 Infinite Loop
Organization Apple Inc.
Organizational Unit Internet Services for Akamai
Common Name www.apple.com

Issuer Name
Country US
Organization Symantec Corporation
Organizational Unit Symantec Trust Network
Common Name Symantec Class 3 EV SSL CA - G3

How do you know if you can trust a CA? After all, since a root CA has signed its own SSL certificate, this effectively means that the organization in control of a root CA simply asserts that you should trust that it is who it claims to be.

The answer is that trust has to start somewhere. In OS X and iOS, Apple includes a collection of root and intermediate CAs that Apple has determined are worthy of trust (see the Apple Root Certificate Program page on the Apple site for the acceptance process: www.apple.com/certificateauthority/ca_program.html). Out of the box, your Mac computers and iOS devices are configured to trust those CAs. By extension, your Mac computers and iOS devices also trust any certificate or intermediate CA whose certificate chain ends with one of these CAs. In OS X, these trusted CAs are stored in the System Roots keychain. (See Lesson 8, "Manage Keychain," in *Apple Pro Training Series: OS X Support Essentials 10.11* for more information about the various keychains in OS X.) You can use Keychain Access to view this collection of trusted root CAs. Open Keychain Access (in the Utilities folder). In the upper-left Keychains column, click System Roots. Note that in the following figure the bottom of the window states that there are at least 180 trusted CAs or intermediate CAs by default in El Capitan.



AAA Certificate Services
Root certificate authority
Expires: Sunday, December 31, 2028 at 5:59:59 PM Central Standard Time
This certificate is valid

Name	Kind	Date Modified	Expires	Keychain
AAA Certificate Services	certificate	--	Dec 31, 2028, 5:59:59 PM	System Roots
Actalis Authentication Root CA	certificate	--	Sep 22, 2030, 6:22:02 AM	System Roots
AddTrust Class 1 CA Root	certificate	--	May 30, 2020, 5:38:31 AM	System Roots
AddTrust External CA Root	certificate	--	May 30, 2020, 5:48:38 AM	System Roots
AddTrust Public CA Root	certificate	--	May 30, 2020, 5:41:50 AM	System Roots
AddTrust Qualified CA Root	certificate	--	May 30, 2020, 5:44:50 AM	System Roots
Admin-Root-CA	certificate	--	Nov 10, 2021, 1:51:07 AM	System Roots
AdminCA-CD-T01	certificate	--	Jan 25, 2016, 6:36:19 AM	System Roots
AffirmTrust Commercial	certificate	--	Dec 31, 2030, 8:06:06 AM	System Roots
AffirmTrust Networking	certificate	--	Dec 31, 2030, 8:08:24 AM	System Roots
AffirmTrust Premium	certificate	--	Dec 31, 2040, 8:10:36 AM	System Roots
AffirmTrust Premium ECC	certificate	--	Dec 31, 2040, 8:20:24 AM	System Roots
ANF Global Root CA	certificate	--	Jun 5, 2033, 12:45:38 PM	System Roots
Apple Root CA	certificate	--	Feb 9, 2035, 3:40:36 PM	System Roots
Apple Root CA - G2	certificate	--	Apr 30, 2039, 1:10:09 PM	System Roots
Apple Root CA - G3	certificate	--	Apr 30, 2039, 1:19:06 PM	System Roots
Apple Root Certificate Authority	certificate	--	Feb 9, 2025, 6:18:14 PM	System Roots
Application CA G2	certificate	--	Mar 31, 2016, 9:59:59 AM	System Roots
ApplicationCA	certificate	--	Dec 12, 2017, 9:00:00 AM	System Roots
ApplicationCA2 Root	certificate	--	Mar 12, 2033, 9:00:00 AM	System Roots
Autoridad de...nal CIF A62634068	certificate	--	Dec 31, 2030, 2:38:15 AM	System Roots
Autoridad de...Estado Venezolano	certificate	--	Dec 17, 2030, 5:59:59 PM	System Roots
Baltimore CyberTrust Root	certificate	--	May 12, 2025, 6:59:00 PM	System Roots
Belgium Root CA2	certificate	--	Dec 15, 2021, 2:00:00 AM	System Roots
Buypass Class 2 CA 1	certificate	--	Oct 13, 2016, 5:25:09 AM	System Roots
Buypass Class 2 Root CA	certificate	--	Oct 26, 2040, 3:38:03 AM	System Roots
Buypass Class 3 Root CA	certificate	--	Oct 26, 2040, 3:28:58 AM	System Roots

NOTE ► Some third-party software companies, such as Mozilla, do not use the System Roots keychain and have their own mechanism to store CAs that their software is configured to trust.

In Lesson 7, "Configuring Open Directory Services," you will learn that when you configure your server as an Open Directory master, the Server app automatically creates a new CA and a new intermediate CA and uses the intermediate CA to sign a new SSL certificate with your server's host name as the common name (the Common Name value is part of what identifies the certificate holder). If you haven't engaged a widely trusted CA to sign an SSL certificate for your server, you should use the SSL certificate signed by your Open Directory intermediate CA; in Lesson 9, "Configuring OS X Server to Provide Device Management," you will learn how to use the Trust Profile to configure your iOS devices and OS X computers to trust your Open Directory CA and, by extension, the intermediate CA and the new SSL certificate.

But what about computers and devices that are outside your control and that you cannot configure? When people use computers and devices that are not configured to trust your server's self-signed SSL certificate or your server's Open Directory CA or intermediate CA and they try to securely access services on your server, they will still see a message that the identity of your server cannot be verified.

One way to prove your identity is for your server to use an SSL certificate that's signed by a CA that most computers and devices are configured to trust or trust inherently.

Deciding What Kind of Certificate to Use

Before going through the process of getting a widely trusted CA to sign a certificate for you, consider the services you'll use with the certificate, as well as the computers and devices that will access those services.

If you use a self-signed certificate, there is no additional server configuration to install the certificate on your server, but you do need to configure each client to trust that self-signed certificate. For a Mac client, this involves not only distributing the certificate to the Mac and adding it to the System keychain but also configuring how the operating system will trust the certificate.

> **NOTE ►** If you use a self-signed certificate and are not able to configure all devices to trust that self-signed certificate, when users encounter a service that uses the self-signed certificate, a dialog informs them that the certificate may not be trustworthy and that to access services they must click Continue. This may undermine your efforts to train users not to automatically trust untrusted, expired, or otherwise invalid certificates.

If you use a certificate signed by a widely trusted CA, you need to generate a certificate signing request (CSR), submit the CSR to a CA, and then import the signed certificate.

Of course, you can use a mix of certificates for different services; if your Websites service responds to multiple host names, you'd want a certificate for each host name that you use for web services secured by SSL.

In all cases, you need to configure your server's services to use the appropriate certificates.

The next section shows you how to obtain a certificate that's signed by a widely trusted CA so that you can use it to prove the identity of your server and to encrypt communications between your server and the users of your server's services.

Reference 4.2
Configuring SSL Certificates

Your server has a default SSL certificate that's self-signed. That's a good start, but no other computers or devices will trust services that use that certificate without additional configuration. To get a CA to sign a certificate, start by using the Server app to create a certificate signing request. Specific steps to accomplish this objective follow in more detail, but generally they include the following:

- Generating a new CSR
- Submitting your CSR to a CA that is generally trusted
- Importing the signed certificate
- Configuring your server's services to use your newly signed certificate

The CA's process of using your CSR and signing your SSL certificate with its own private key includes verifying your identity (otherwise, why would anyone trust the CA if it signed certificates from unverified entities?) and optionally charging you money.

To finish the story, computers and devices can now use your server's services without getting a warning that your SSL certificate is not verified (as long as those computers and devices trust the CA you've chosen to sign your certificate). Additionally, your server and the users of its services can use your server's SSL certificate in the process of encrypting communications for services that use that SSL certificate.

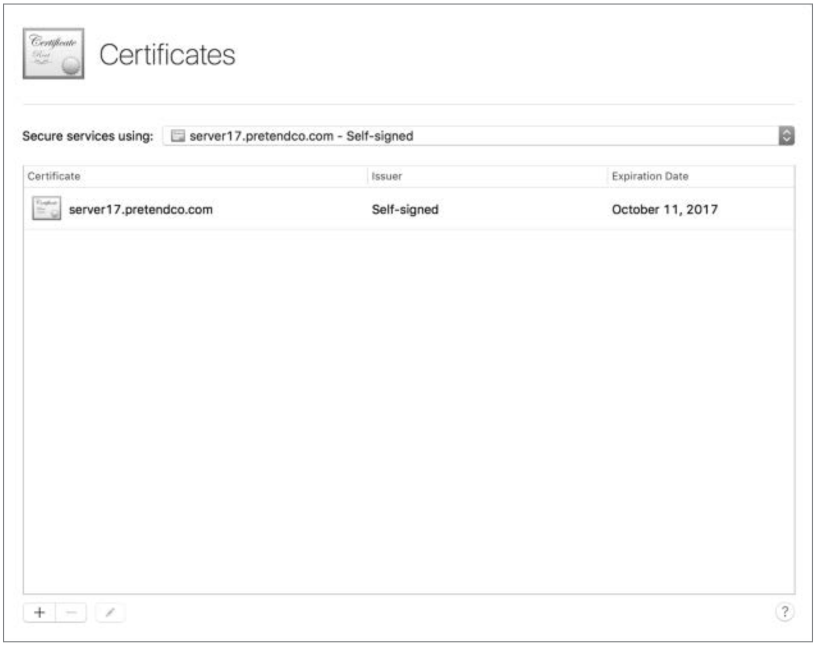
Before you start creating new certificates, take a moment to inspect what you already have.

Viewing Your Server's Default Certificate

You can use the Server app to display certificates (if you're logged in at the server, you can also use the Keychain Access app). The standard behavior of Server app is to show all the certificates where earlier versions only showed some and you needed to pick the option to make all visible.

In the following figure, the certificate has the server's host name and expires in two years.

NOTE ► When you use the Server app Change Host Name Assistant to change your server's host name, it automatically creates a new self-signed certificate for the new host name.

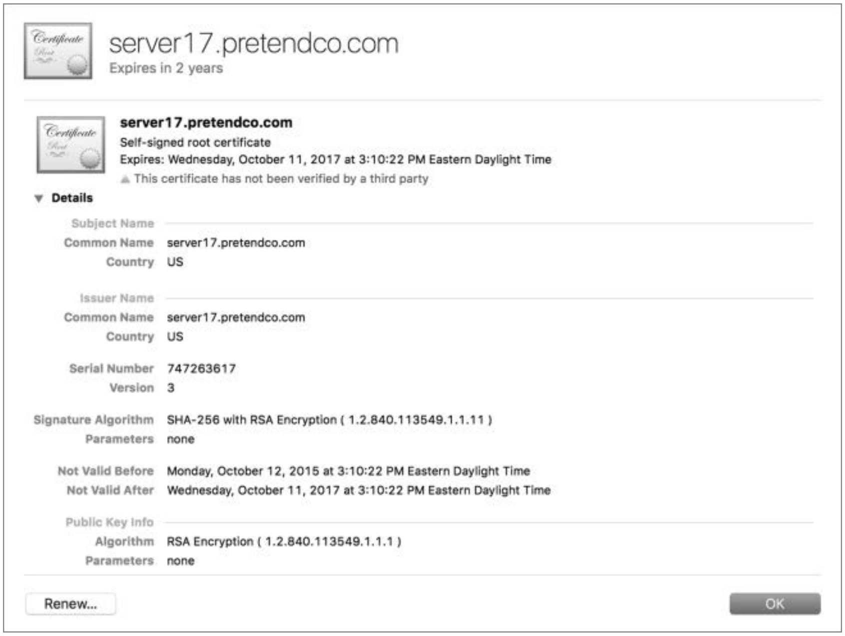


Certificates

Secure services using: server17.pretendco.com - Self-signed

Certificate	Issuer	Expiration Date
server17.pretendco.com	Self-signed	October 11, 2017

To get more details, double-click the certificate; alternatively, select it and click the Edit (pencil icon) button. You'll need to scroll to inspect all of the certificate's information.



server17.pretendco.com
Expires in 2 years

server17.pretendco.com
Self-signed root certificate
Expires: Wednesday, October 11, 2017 at 3:10:22 PM Eastern Daylight Time
⚠ This certificate has not been verified by a third party

▼ **Details**

Subject Name
Common Name server17.pretendco.com
Country US

Issuer Name
Common Name server17.pretendco.com
Country US

Serial Number 747263617
Version 3

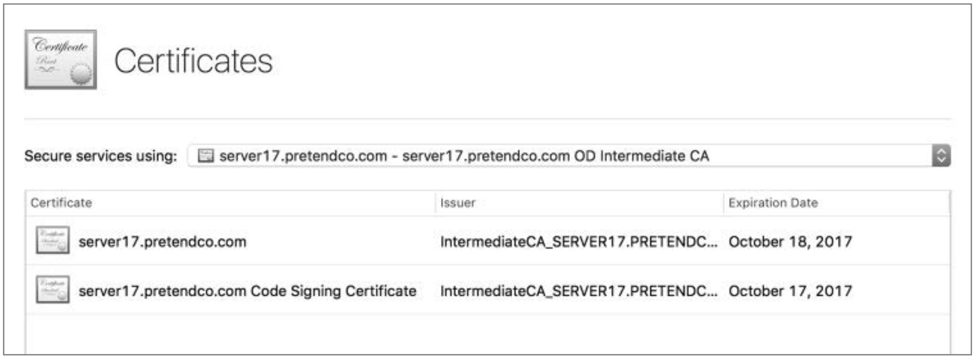
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters none

Not Valid Before Monday, October 12, 2015 at 3:10:22 PM Eastern Daylight Time
Not Valid After Wednesday, October 11, 2017 at 3:10:22 PM Eastern Daylight Time

Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters none

Click OK to return to the Certificates pane.

The following figure illustrates what you'd see after you configure your server as an Open Directory master or replica. At first glance, it looks like there is just one additional certificate, the code signing certificate, but the certificate with the server's host name is no longer a self-signed certificate but a certificate signed by your Open Directory CA; that certificate icon is blue, whereas the original self-signed certificate was bronze.



Secure services using: server17.pretendco.com - server17.pretendco.com OD Intermediate CA

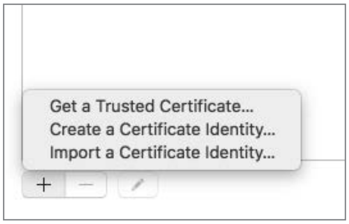
Certificate	Issuer	Expiration Date
server17.pretendco.com	IntermediateCA_SERVER17.PRETENDC...	October 18, 2017
server17.pretendco.com Code Signing Certificate	IntermediateCA_SERVER17.PRETENDC...	October 17, 2017

Explaining Options for Adding New Certificates

The existing self-signed certificates may not meet your needs. In the Server app Certificates pane, you have several options for adding a new certificate.

Click Add (+) to reveal three menu commands:

- Get a Trusted Certificate allows you to quickly generate a certificate signing request.
- Create a Certificate Identity is the command to choose to create a new self-signed certificate.
- Import a Certificate Identity allows you to import a signed certificate or a certificate and private key you've archived.


Get a Trusted Certificate...
Create a Certificate Identity...
Import a Certificate Identity...
+
—

Obtaining a Trusted Certificate

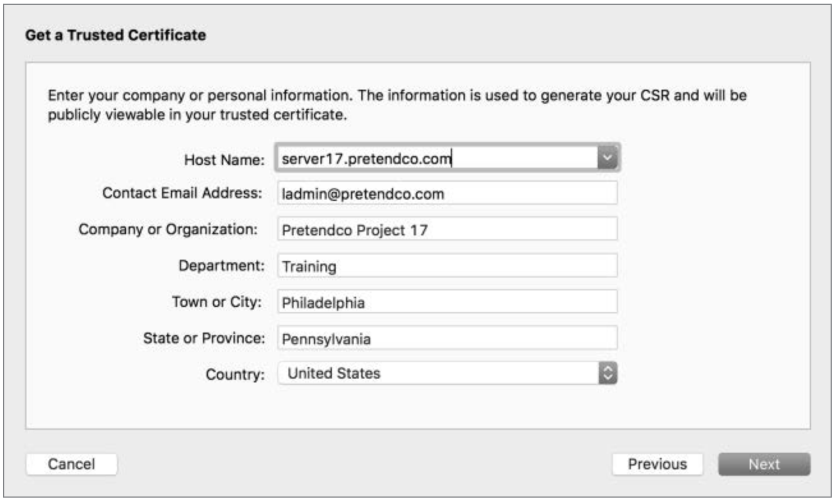
You can choose to get a CA to sign a certificate for you so that users around the world can use your server's services without being notified that your server's identity is not verified.

At the bottom of the Certificates pane, click Add (+), and then choose Get a Trusted Certificate.

After that, you'll see the Get a Trusted Certificate assistant.

In the next pane, you can enter all the information necessary to establish an identity. A CA uses these details to verify your identity.

In the Host Name field, enter the host name you'll use for the services that will use this certificate. Use your organization's full legal name for the Company or Organization field, or if it's for personal use, just use your full name. The Department field is flexible; you can enter information such as your department name, but you should enter some value. To be fully compliant with standards, do not abbreviate your state or province. The following figure illustrates all the fields completed.



Get a Trusted Certificate

Enter your company or personal information. The information is used to generate your CSR and will be publicly viewable in your trusted certificate.

Host Name: server17.pretendco.com

Contact Email Address: ladmin@pretendco.com

Company or Organization: Pretendco Project 17

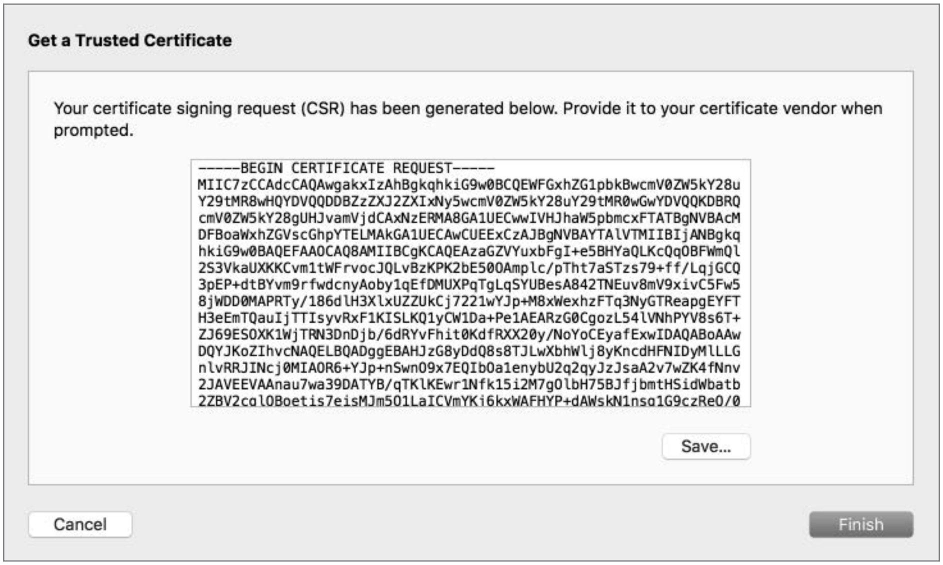
Department: Training

Town or City: Philadelphia

State or Province: Pennsylvania

Country: United States

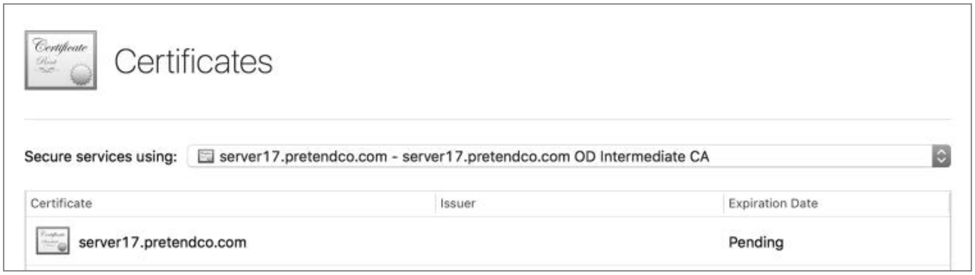
The next pane displays the text of your CSR, which you will submit to the CA of your choice. You can wait and access this text later, or you can select and copy this text, or click Save, now.



Your certificate signing request (CSR) has been generated below. Provide it to your certificate vendor when prompted.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC7zCCAdcCAQAwgakxIzAhBgkqhkiG9w0BCQEWFGxhZG1pbkBwcmV0ZW5kY28u
Y29tMR8wHQYDVQQDDBZzZXJ2ZXIxNy5wcmV0ZW5kY28uY29tMR0wGwYDVQQKDBRQ
cmV0ZW5kY28gUHJvamVjdCAxNzERMA8GA1UECwwIVHJhaW5pbmcxFTATBgNVBAcM
DFBoaWxhZGVscGhpYTELMAkGA1UECAwCUEExCzAJBgNVBAYTAlVTMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzaGZVYuxbFgI+e5BHYaQLKcQqOBFWmQl
2S3VkaUXKKCvm1tWFrvocJQLvBzKPK2bE50OAmplc/pTht7aSTzs79+ff/LqjGCQ
3pEP+dtBYvm9rfwdcnyAoby1qEfDMUXPqTgLqSYUBesA842TNEuv8mV9xivC5Fw5
8jWDD0MAPRTy/186dlH3XlxUZZUkCj7221wYJp+M8xWexhzFTq3NyGTReapgEYFT
H3eEmTQauIjTTIsyvRxF1KISLKQ1yCW1Da+Pe1AEARzG0CgozL54lVNhPYV8s6T+
ZJ69ESOXK1WjTRN3DnDjb/6dRYvFhit0KdfRXX20y/NoYoCEyafExwIDAQABoAAw
DQYJKoZIhvcNAQELBQADggEBAHJzG8yDdQ8s8TJLwXbhWlj8yKncdHFNIDyMlLLG
nlvRRJINcj0MIAOR6+YJp+nSwnO9x7EQIbOa1enybU2q2qyJzJsaA2v7wZK4fNnv
2JAVEEVAAnau7wa39DATYB/qTKlKEwr1Nfk15i2M7gOlbH75BJfjbmtHSidWbatb
2ZBV2cqlOBoetis7eisMJm5O1LaICVmYKj6kxWAFHYP+dAWskN1nsq1G9czReO/0
```

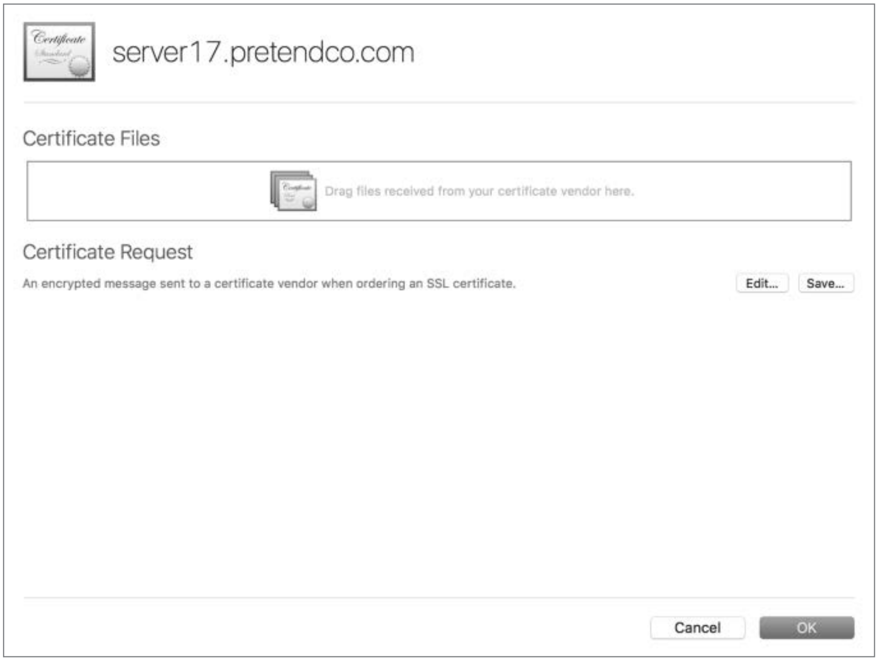
After you click Finish, the Server app displays the pending request.



Secure services using: server17.pretendco.com - server17.pretendco.com OD Intermediate CA

Certificate	Issuer	Expiration Date
server17.pretendco.com		Pending

If you didn't copy the text of your CSR earlier, you can access it again: Select the certificate marked Pending and click the Edit button (pencil icon), or just double-click the pending certificate item.



server17.pretendco.com

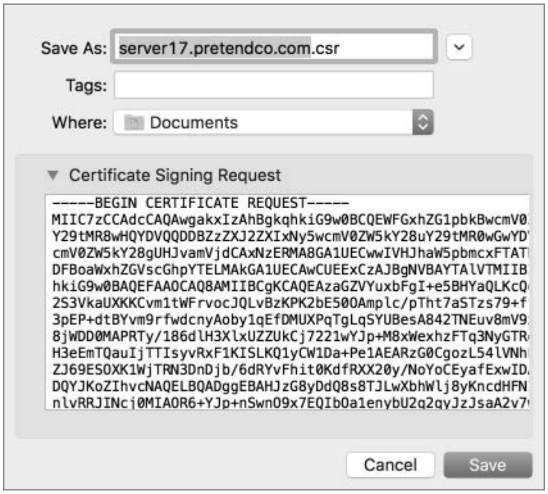
Certificate Files

Drag files received from your certificate vendor here.

Certificate Request

An encrypted message sent to a certificate vendor when ordering an SSL certificate.

Your course of action depends on how your CA accepts CSRs. If your CA allows you to upload a text file, use the Save dialog to save the CSR as a text file. If your CA requires you to paste the text of the CA into a web form, click the disclosure triangle, and then copy the text of the CSR.



Save As: server17.pretendco.com.csr

Tags:

Where: Documents

▼ Certificate Signing Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC7zCCAdcCAQAwgakxIzAhBgkqhkiG9w0BCQEWFGxhZG1pbkBwcmV0
Y29tMR8wHQYDVQQDDBZzZXJ2ZXIxNy5wcmV0ZW5kY28uY29tMR0wGwYD
cmV0ZW5kY28gUHJvamVjdCAxNzERMA8GA1UECwwIVHJhaW5pbmcxFTAT
DFBoaWxhZGVscGhpYTELMAkGA1UECAwCUEExCzAJBgNVBAYTAlVTMIIB
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzaGZVYuxbFgI+e5BHYaQLKcQ
2S3VkaUXKKCvm1tWFrvocJQLvBzKPK2bE50OAmplc/pTht7aSTzs79+f
3pEP+dtBYvm9rfwdcnyAoby1qEfDMUXPqTgLqSYUBesA842TNEuv8mV9
8jWDD0MAPRTy/186dlH3XlxUZZUkCj7221wYJp+M8xWexhzFTq3NyGTR
H3eEmTQauIjTTIsyvRxF1KISLKQ1yCW1Da+Pe1AEARzG0CgozL54lVNh
ZJ69ESOXK1WjTRN3DnDjb/6dRYvFhit0KdfRXX20y/NoYoCEyafExwID
DQYJKoZIhvcNAQELBQADggEBAHJzG8yDdQ8s8TJLwXbhWlj8yKncdHFN
nlvRRJINcj0MIAOR6+YJp+nSwnO9x7EQIbOa1enybU2q2qyJzJsaA2v7
```

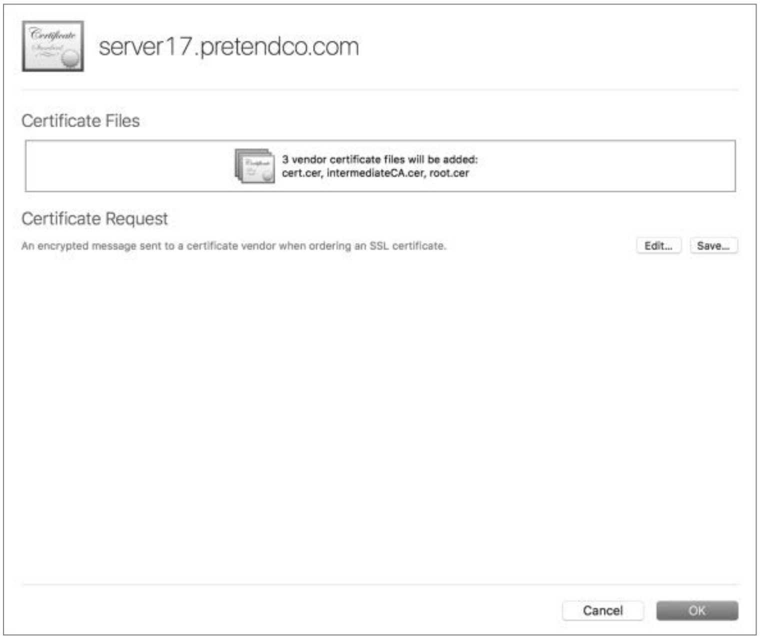
You need to choose an appropriate CA for your organization's needs (choosing a CA is outside the scope of this guide), send the CSR to the CA, and prove your identity to the CA. After some period of time, you will receive a signed certificate from the CA.

Importing a Signed Certificate

After you receive the signed certificate from the CA, you can import it with the Server app. If you are still at the list of certificates, double-click your pending certificate to reveal the field into which you can drag your signed certificate.

> **NOTE ►** If the CA provides you with the certificate in text form rather than in a separate file, you'll need to convert that text into a file. A quick way to do this is to copy the text, open TextEdit, press Command-N to create a new file, and choose Format > Make Plain Text (if that is an available command). Paste the text into the text file, and save it with a .cer extension.

Double-click the pending CSR, and drag the file containing a signed certificate, as well as any ancillary files provided by the CA, into the Certificate Files field (this is also where you could import a certificate and private key you've exported with Keychain Access). Once the certificate is in the Certificate Files field, its color will be blue, as long as the top of the certificate chain is a root CA your server trusts.



server17.pretendco.com

Certificate Files

3 vendor certificate files will be added:
cert.cer, intermediateCA.cer, root.cer

Certificate Request

An encrypted message sent to a certificate vendor when ordering an SSL certificate.

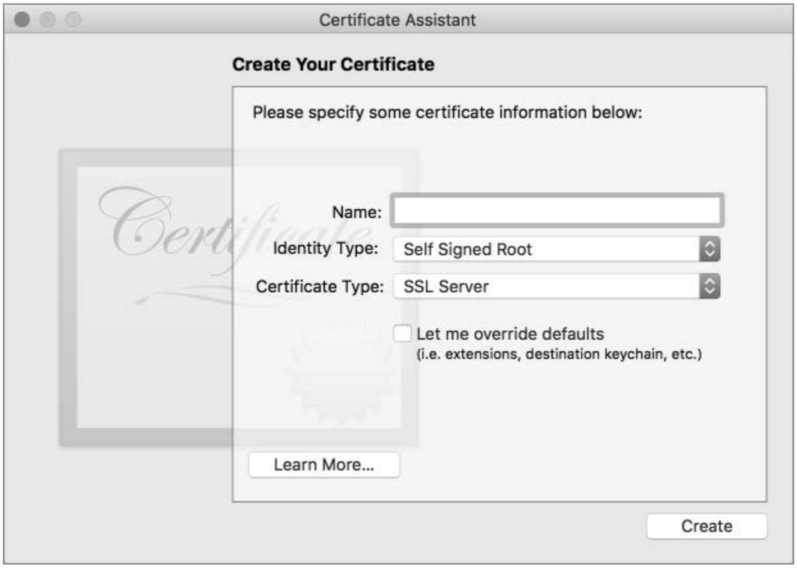
NOTE ▶ If you click Edit next to Certificate Request and then click Edit in the confirming dialog, a new public and private key pair and a new CSR will be generated, and you'll lose the original CSR.

Click OK to save your changes.

Generating a Self-Signed Certificate

In addition to generating a CSR, you can also use the Server app to generate a new self-signed certificate. This is useful if your server offers services at an alternative host name that corresponds to your server's Internet Protocol version 4 (IPv4) address or another IPv4 address your server is configured to use and if you have the ability to configure computers and iOS devices to trust the self-signed certificate.

In the Certificates pane, when you click Add (+) and choose Create a Certificate Identity, you see a blank Name field.



Certificate Assistant

Create Your Certificate

Please specify some certificate information below:

Name:

Identity Type: Self Signed Root

Certificate Type: SSL Server

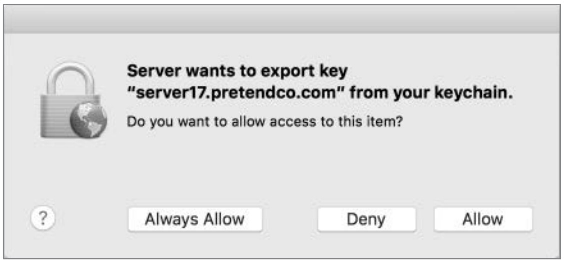
□ Let me override defaults
(i.e. extensions, destination keychain, etc.)

Enter the host name for the self-signed certificate, and then click Create.

NOTE ▶ You can select the "Let me override defaults" checkbox if you have more specific needs, but for most purposes, the defaults will suffice.

At the warning that you are about to create a self-signed certificate, click Continue.

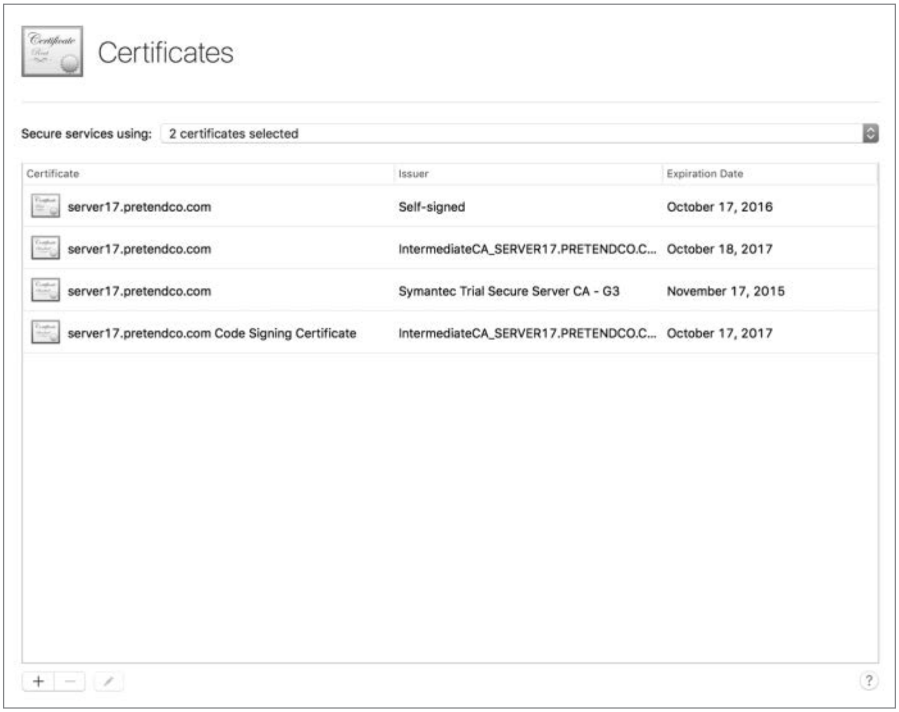
At the Conclusion window, click Done. Finally, click either Always Allow or Allow to allow the Server app to copy the public and private key pair and the certificate from your login keychain to the System keychain and to /private/etc/certificates/.



Server wants to export key "server17.pretendco.com" from your keychain.

Do you want to allow access to this item?

You'll see the certificate in the Certificates field, with the bronze color that denotes a self-signed certificate.

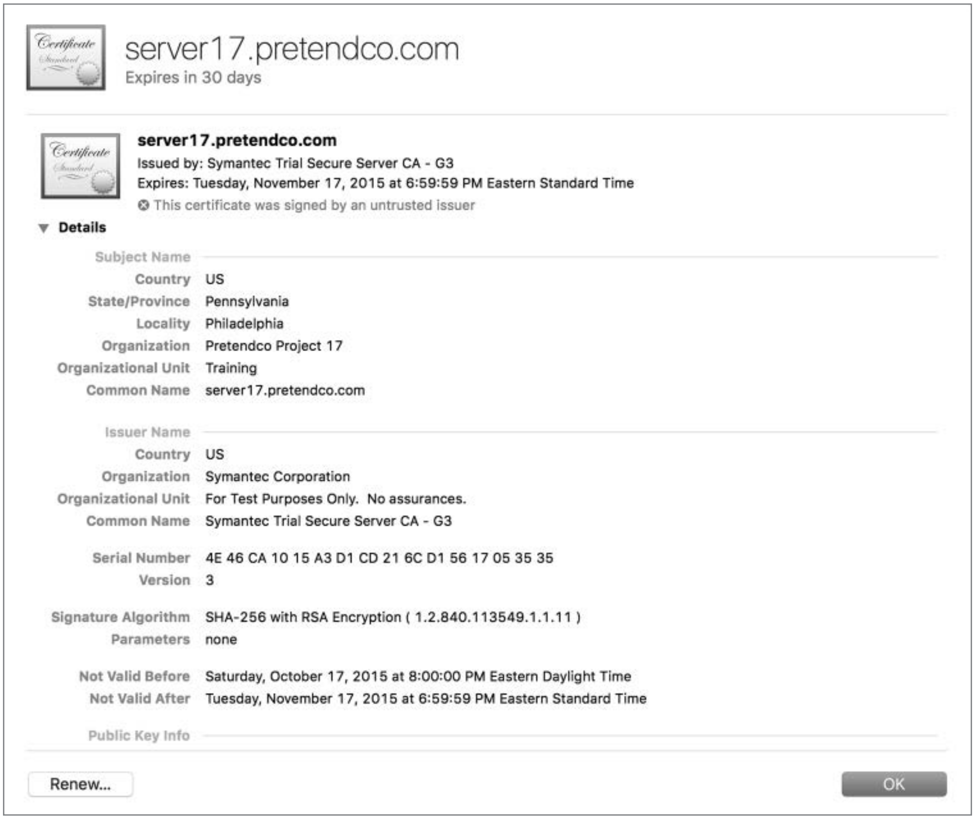


Secure services using: 2 certificates selected

Certificate	Issuer	Expiration Date
server17.pretendco.com	Self-signed	October 17, 2016
server17.pretendco.com	IntermediateCA_SERVER17.PRETENDCO.C...	October 18, 2017
server17.pretendco.com	Symantec Trial Secure Server CA - G3	November 17, 2015
server17.pretendco.com Code Signing Certificate	IntermediateCA_SERVER17.PRETENDCO.C...	October 17, 2017

Inspecting a Certificate

You can inspect your certificates with the Server app, as well as with the System keychain of your server computer (the System keychain contains items that are not user specific and that are available to all users of a system). The following figure shows a certificate that's been signed by a CA for test purposes. Note that the OS has not yet been configured to trust the CA that signed this certificate.



server17.pretendco.com
Expires in 30 days

server17.pretendco.com
Issued by: Symantec Trial Secure Server CA - G3
Expires: Tuesday, November 17, 2015 at 6:59:59 PM Eastern Standard Time
⊗ This certificate was signed by an untrusted issuer

▼ **Details**

Subject Name	
Country	US
State/Province	Pennsylvania
Locality	Philadelphia
Organization	Pretendco Project 17
Organizational Unit	Training
Common Name	server17.pretendco.com
Issuer Name	
Country	US
Organization	Symantec Corporation
Organizational Unit	For Test Purposes Only. No assurances.
Common Name	Symantec Trial Secure Server CA - G3
Serial Number	4E 46 CA 10 15 A3 D1 CD 21 6C D1 56 17 05 35 35
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	none
Not Valid Before	Saturday, October 17, 2015 at 8:00:00 PM Eastern Daylight Time
Not Valid After	Tuesday, November 17, 2015 at 6:59:59 PM Eastern Standard Time
Public Key Info	

You can also use Keychain Access to inspect a certificate and its associated private key. Because the certificate and private key are stored in the System keychain on the server, you need to log in directly on your server (or use a screen-sharing method to control your server) to use Keychain Access to access the private key.

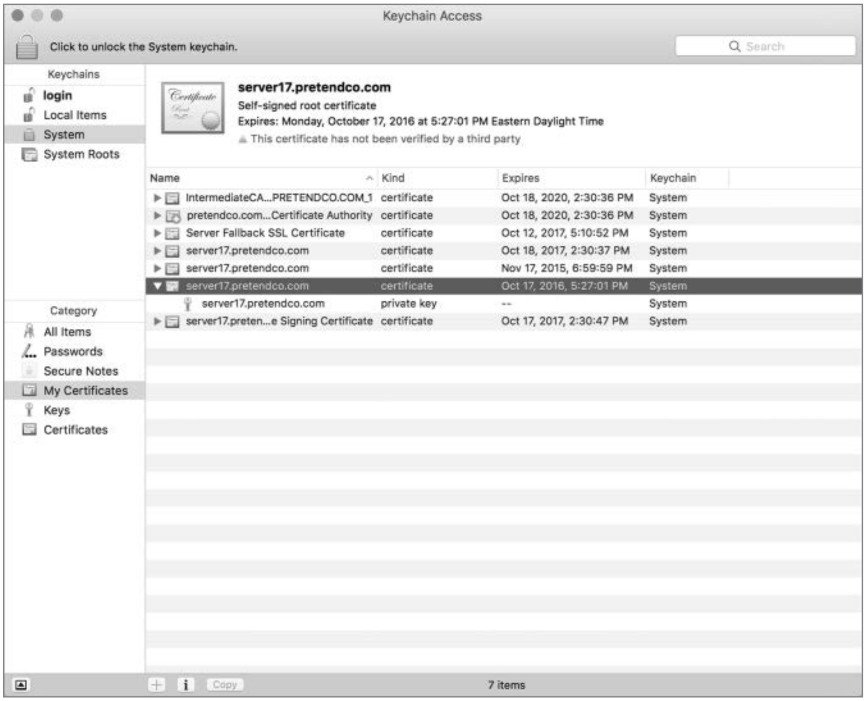
Keychain Access is in the /Applications/Utilities/ folder on your startup volume; you can use Spotlight or Launchpad to search for it (in Launchpad, it is in the folder named Other). Select the My Certificates category to filter the items that Keychain Access displays. If necessary, toggle the show/hide button in the lower-left corner of the Keychain

Access window until you can see all keychains. Select the System keychain to show items that are for the entire system, not just for the user who is currently logged in.

At least three items are listed (if you provided an Apple ID for push notifications, you will see more items):

- com.apple.servermgrd, which is used for remote administration with the Server app
- A certificate named Server Fallback SSL Certificate, which the Server app automatically uses if the default SSL certificate is removed
- An SSL certificate with the host name of your server

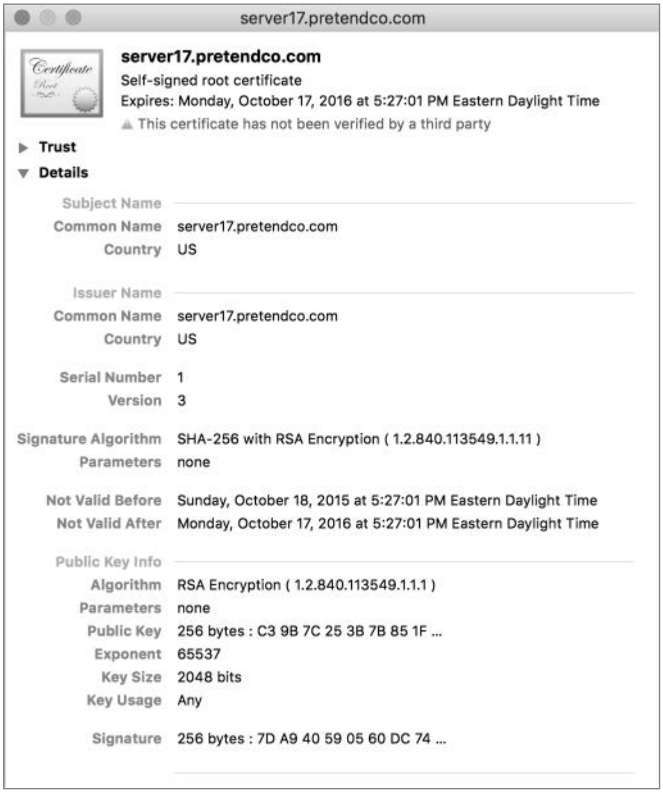
When you select a certificate that is not signed by a trusted CA, Keychain Access displays a warning icon, along with the text that explains the issue. In the following figure, the warning for the self-signed certificate is "This certificate has not been verified by a third party."



server17.pretendco.com
Self-signed root certificate
Expires: Monday, October 17, 2016 at 5:27:01 PM Eastern Daylight Time
This certificate has not been verified by a third party

Name	Kind	Expires	Keychain
IntermediateCA...PRETENDCO.COM_1	certificate	Oct 18, 2020, 2:30:36 PM	System
pretendco.com...Certificate Authority	certificate	Oct 18, 2020, 2:30:36 PM	System
Server Fallback SSL Certificate	certificate	Oct 12, 2017, 5:10:52 PM	System
server17.pretendco.com	certificate	Oct 18, 2017, 2:30:37 PM	System
server17.pretendco.com	certificate	Nov 17, 2015, 6:59:59 PM	System
server17.pretendco.com	certificate	Oct 17, 2016, 5:27:01 PM	System
server17.pretendco.com	private key	--	System
server17.preten...e Signing Certificate	certificate	Oct 17, 2017, 2:30:47 PM	System

If you double-click your default self-signed SSL certificate to open it, you'll see a warning icon and the text "This certificate has not been verified by a third party."

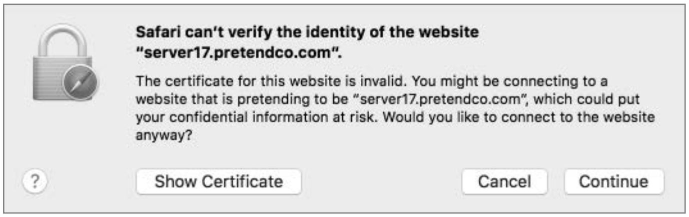


server17.pretendco.com

server17.pretendco.com
Self-signed root certificate
Expires: Monday, October 17, 2016 at 5:27:01 PM Eastern Daylight Time
This certificate has not been verified by a third party

Subject Name	
Common Name	server17.pretendco.com
Country	US
Issuer Name	
Common Name	server17.pretendco.com
Country	US
Serial Number	1
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	none
Not Valid Before	Sunday, October 18, 2015 at 5:27:01 PM Eastern Daylight Time
Not Valid After	Monday, October 17, 2016 at 5:27:01 PM Eastern Daylight Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : C3 9B 7C 25 3B 7B 85 1F ...
Exponent	65537
Key Size	2048 bits
Key Usage	Any
Signature	256 bytes : 7D A9 40 59 05 60 DC 74 ...

If a service on your server uses this self-signed certificate, when users attempt to use services that use that SSL certificate, they may be warned that your SSL certificate is not trusted, as shown in the following figure.



Safari can't verify the identity of the website "server17.pretendco.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "server17.pretendco.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

Train your users that when they see an SSL warning, they should *not* continue using the service that uses the unverified SSL certificate.

Archiving Your Certificate

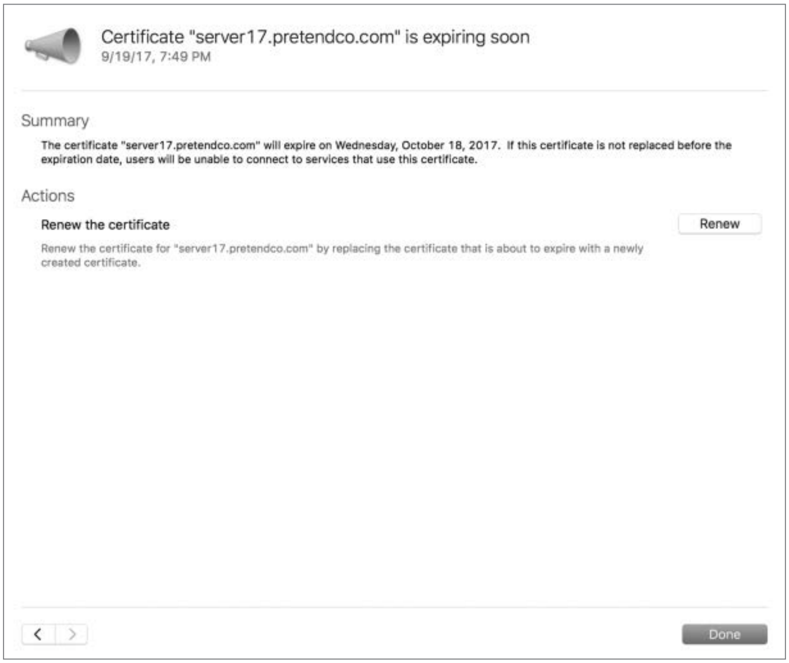
Whether you have a self-signed certificate or a certificate signed by a CA, you should take steps to archive your certificate and its private key. You may need to reinstall your server in the future, or an administrator might accidentally remove your certificate and its private key; if you have an archive of your certificate and private key, you can easily use the Server app to re-import your certificate and its private key.

You use the Keychain Access app to export your certificate and private key. Keychain Access prompts you to specify a password to protect your private key; make sure that you use a strong password.

You use the Server app to import the certificate and private key. You need to provide the password that was entered when the certificate was exported in the first place; otherwise, you will not be able to import.

Renewing Your Certificate

SSL certificates do not last forever. Luckily, renewing SSL certificates is simple. The Server app issues an alert when an SSL certificate expiration date approaches. To renew a self-signed SSL certificate, simply click Renew when viewing the certificate in the Certificates pane or when viewing the alert.



Certificate "server17.pretendco.com" is expiring soon
9/19/17, 7:49 PM

Summary

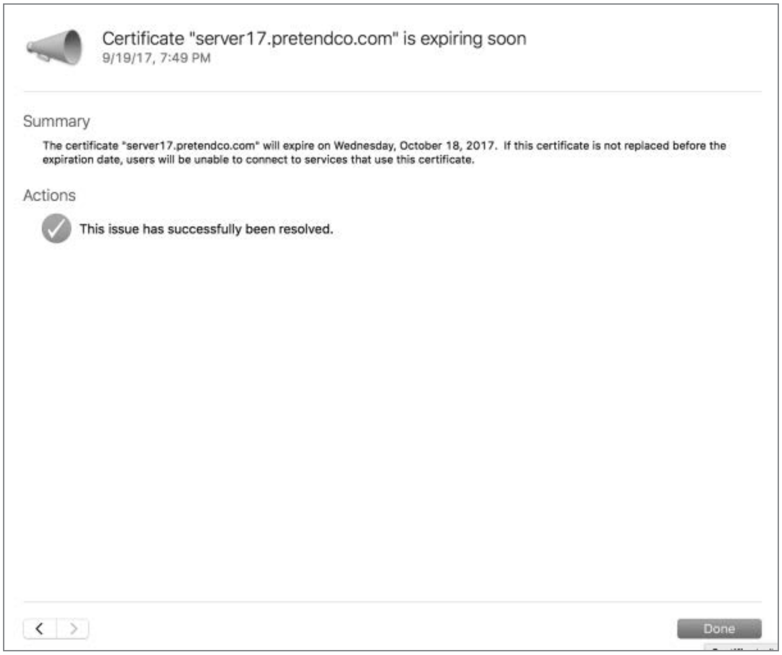
The certificate "server17.pretendco.com" will expire on Wednesday, October 18, 2017. If this certificate is not replaced before the expiration date, users will be unable to connect to services that use this certificate.

Actions

Renew the certificate

Renew the certificate for "server17.pretendco.com" by replacing the certificate that is about to expire with a newly created certificate.

Once you click Renew, the Server app takes care of renewing the certificate, and the alert displays that the issue has been resolved.



Certificate "server17.pretendco.com" is expiring soon
9/19/17, 7:49 PM

Summary

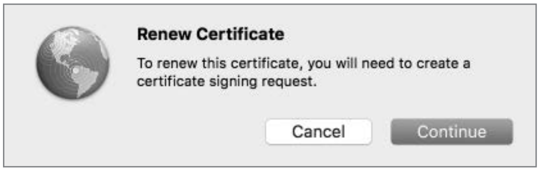
The certificate "server17.pretendco.com" will expire on Wednesday, October 18, 2017. If this certificate is not replaced before the expiration date, users will be unable to connect to services that use this certificate.

Actions

✓ This issue has successfully been resolved.

NOTE ► Do not click Renew for an Open Directory CA because this causes changes to the CA properties, and your Open Directory intermediate CA will no longer be signed by a trusted authority.

If you have a certificate signed by a widely trusted CA, when you click Renew, you will see the message that you need to generate a new CSR. See the earlier section "Obtaining a Trusted Certificate" for more details.



Renew Certificate

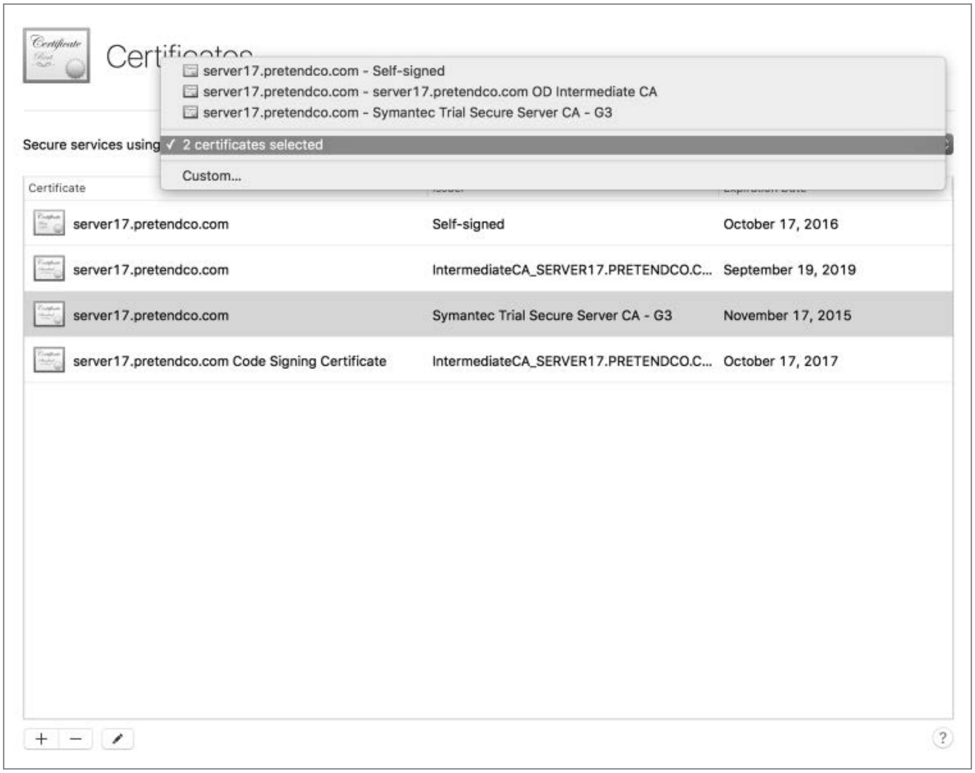
To renew this certificate, you will need to create a certificate signing request.

Configuring OS X Server Services to Use a Certificate

Once you have taken steps to obtain a signed certificate or create a new self-signed certificate or have configured your server as an Open Directory server, you should use the Server app to configure services to use that certificate. You start in the Certificates pane of the Server app.

With the pop-up menu, you can do either of the following:

- Choose one certificate to specify that all services use that certificate.
- Choose Custom to configure each service separately to use or not use a certificate.

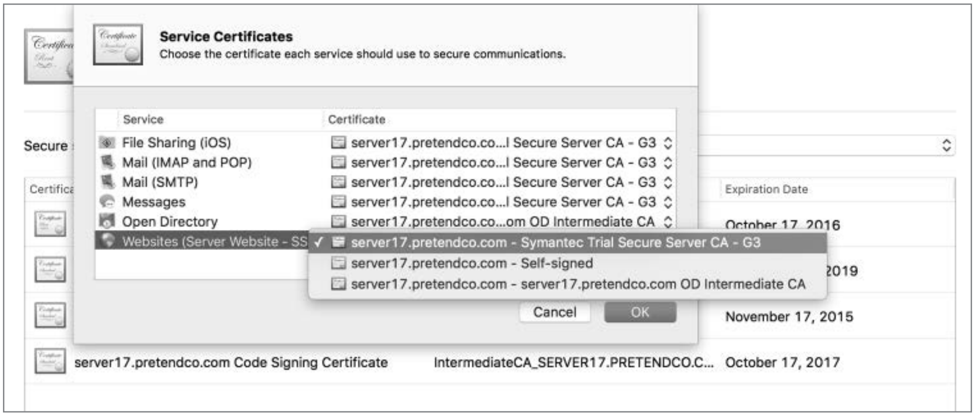


Certificates
server17.pretendco.com - Self-signed
server17.pretendco.com - server17.pretendco.com OD Intermediate CA
server17.pretendco.com - Symantec Trial Secure Server CA - G3
Custom...
+
−
?

Secure services using ✓ 2 certificates selected

Certificate		
server17.pretendco.com	Self-signed	October 17, 2016
server17.pretendco.com	IntermediateCA_SERVER17.PRETENDCO.C...	September 19, 2019
server17.pretendco.com	Symantec Trial Secure Server CA - G3	November 17, 2015
server17.pretendco.com Code Signing Certificate	IntermediateCA_SERVER17.PRETENDCO.C...	October 17, 2017

The following figure shows an example of choosing Custom and then editing the value for the default secure site of the Websites service. Note that there are some extra certificates in the figure. This illustrates that you can configure your server to respond to requests at multiple host names, create a certificate for each host name, and configure each secure site to use the appropriate certificate.



Service Certificates

Choose the certificate each service should use to secure communications.

Service	Certificate
File Sharing (iOS)	server17.pretendco.co...l Secure Server CA - G3
Mail (IMAP and POP)	server17.pretendco.co...l Secure Server CA - G3
Mail (SMTP)	server17.pretendco.co...l Secure Server CA - G3
Messages	server17.pretendco.co...l Secure Server CA - G3
Open Directory	server17.pretendco.co...om OD Intermediate CA
Websites (Server Website - SS	✓ server17.pretendco.com - Symantec Trial Secure Server CA - G3

- ✓ server17.pretendco.com - Symantec Trial Secure Server CA - G3
- server17.pretendco.com - Self-signed
- server17.pretendco.com - server17.pretendco.com OD Intermediate CA

Certifica			Expiration Date
			October 17, 2016
			2019
			November 17, 2015
	server17.pretendco.com Code Signing Certificate	IntermediateCA_SERVER17.PRETENDCO.C...	October 17, 2017

You can use the Server app to configure the following OS X Server services to use SSL:

- File Sharing for iOS
- Mail (IMAP and POP)
- Mail (SMTP)
- Messages
- Open Directory (appears only after starting Open Directory services)
- Websites

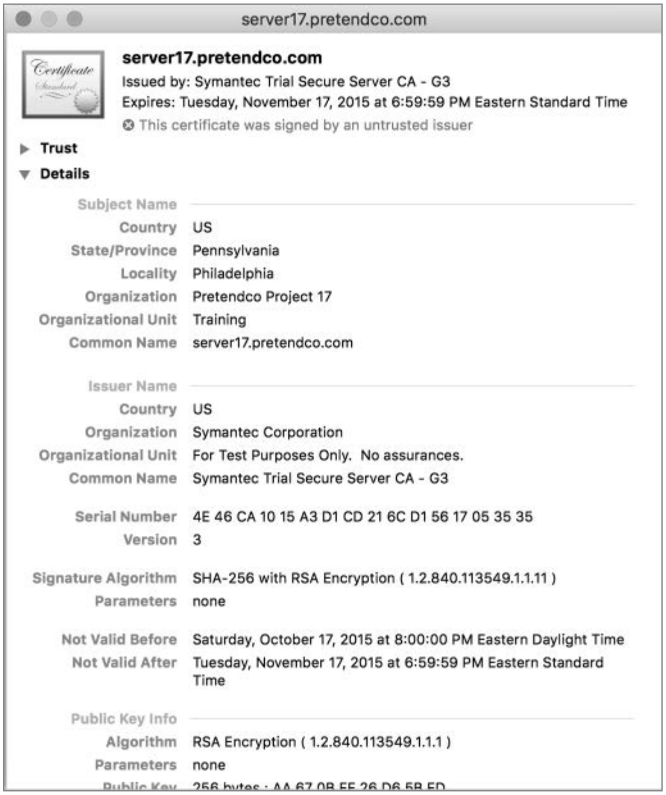
You will see in Lesson 19, "Hosting Websites" that you can granularly specify an SSL certificate for each website you host, and you can use the Profile Manager pane to specify the SSL certificate to use for the Profile Manager service to sign configuration profiles.

A few other services use SSL but do not appear in the Server app:

- com.apple.servermgrd (for remote administration with the Server app)
- VPN
- Xcode
- Calendar and Contacts

Following the Certificate Chain

When choosing a CA to use, make sure that it's a root CA that most computers and devices are configured to trust. Having a CA sign your certificate isn't useful if not many computers or devices will trust that certificate. As an example, the following figure shows how an SSL certificate signed by a trial CA appears in Keychain Access.



server17.pretendco.com

Issued by: Symantec Trial Secure Server CA - G3

Expires: Tuesday, November 17, 2015 at 6:59:59 PM Eastern Standard Time

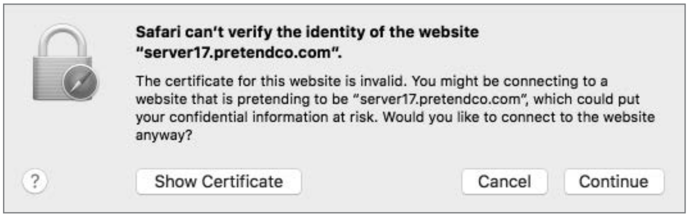
⊗ This certificate was signed by an untrusted issuer

▶ Trust

▼ Details

Subject Name	
Country	US
State/Province	Pennsylvania
Locality	Philadelphia
Organization	Pretendco Project 17
Organizational Unit	Training
Common Name	server17.pretendco.com
Issuer Name	
Country	US
Organization	Symantec Corporation
Organizational Unit	For Test Purposes Only. No assurances.
Common Name	Symantec Trial Secure Server CA - G3
Serial Number	4E 46 CA 10 15 A3 D1 CD 21 6C D1 56 17 05 35 35
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	none
Not Valid Before	Saturday, October 17, 2015 at 8:00:00 PM Eastern Daylight Time
Not Valid After	Tuesday, November 17, 2015 at 6:59:59 PM Eastern Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : AA 67 0B FF 26 D6 5B ED

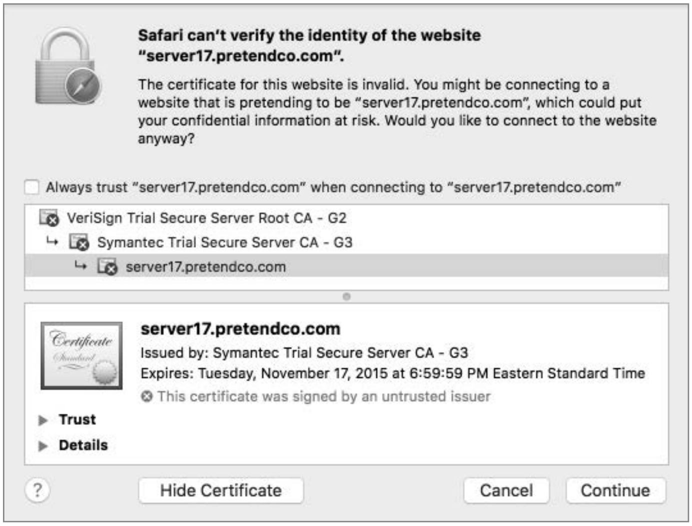
You can see that the "Issued by" field near the top of the window shows Symantec Trial Secure Server CA – G3. Note the red X icon and the text "This certificate was signed by an untrusted issuer." This is a CA that is by default not trusted by computers and devices, so even if you used this signed certificate for OS X Server services, the people who access your services would experience trouble. In some cases, the service might silently fail, or the user may be alerted that the identity of the service cannot be verified. The following figure illustrates that on a client Mac Safari notifies the user that Safari can't verify the identity of the website.



Safari can't verify the identity of the website "server17.pretendco.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "server17.pretendco.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

If you click Show Certificate, Safari displays the certificate chain. The following figure shows what you see when you select the server's certificate at the bottom of the certificate chain: that the certificate was signed by an untrusted issuer.



Safari can't verify the identity of the website "server17.pretendco.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "server17.pretendco.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

□ Always trust "server17.pretendco.com" when connecting to "server17.pretendco.com"

```
VeriSign Trial Secure Server Root CA - G2
 ↳ Symantec Trial Secure Server CA - G3
    ↳ server17.pretendco.com
```

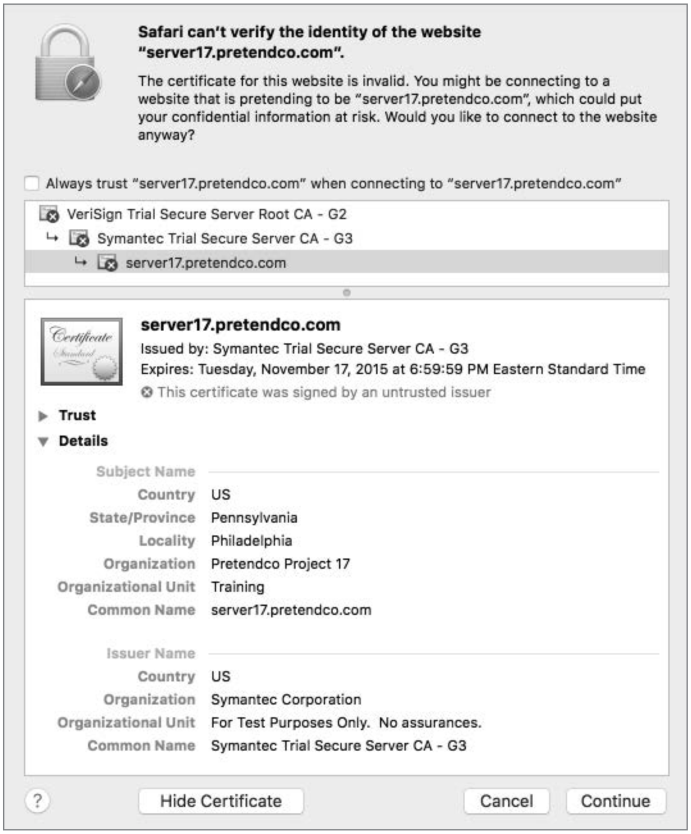
server17.pretendco.com

Issued by: Symantec Trial Secure Server CA - G3

Expires: Tuesday, November 17, 2015 at 6:59:59 PM Eastern Standard Time

⊗ This certificate was signed by an untrusted issuer

The following figure illustrates that if you click the Details disclosure triangle, you'll see information about the identity of the certificate holder, as well as information about the issuer (the entity that signed the certificate). In this case, the issuer's common name is Symantec Trial Secure Server CA – G3.



Safari can't verify the identity of the website "server17.pretendco.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "server17.pretendco.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

□ Always trust "server17.pretendco.com" when connecting to "server17.pretendco.com"

VeriSign Trial Secure Server Root CA - G2
↳ Symantec Trial Secure Server CA - G3
↳ server17.pretendco.com

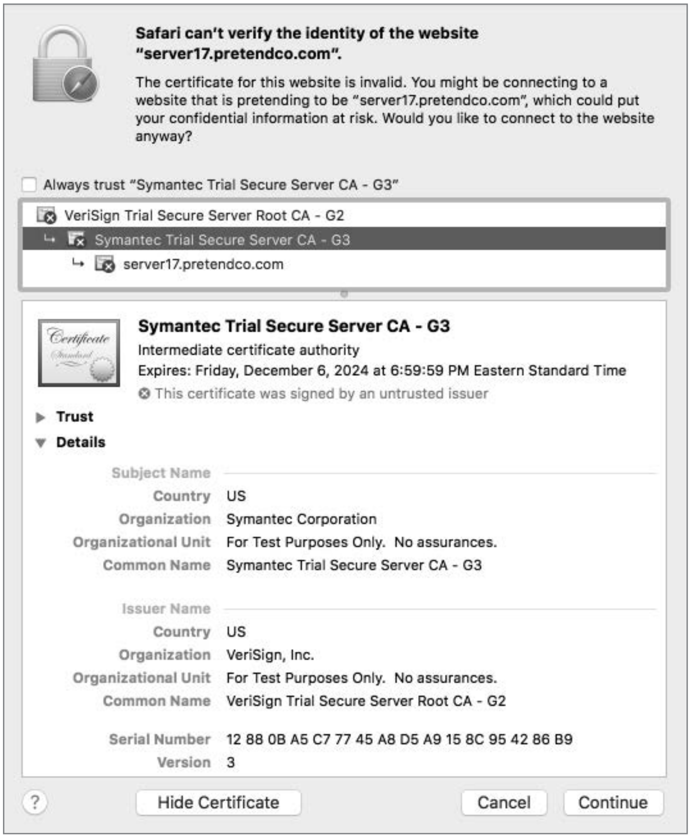
server17.pretendco.com
Issued by: Symantec Trial Secure Server CA - G3
Expires: Tuesday, November 17, 2015 at 6:59:59 PM Eastern Standard Time
⊗ This certificate was signed by an untrusted issuer

▶ Trust
▼ Details

Subject Name	
Country	US
State/Province	Pennsylvania
Locality	Philadelphia
Organization	Pretendco Project 17
Organizational Unit	Training
Common Name	server17.pretendco.com

Issuer Name	
Country	US
Organization	Symantec Corporation
Organizational Unit	For Test Purposes Only. No assurances.
Common Name	Symantec Trial Secure Server CA - G3

When you select the certificate in the middle of the certificate chain, you see that this is an intermediate CA; the window states "Intermediate certificate authority," and the Issuer Name information shows you that the common name of the issuer (or signer) is Symantec Trial Secure Server Root CA – G2.



Safari can't verify the identity of the website "server17.pretendco.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "server17.pretendco.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

□ Always trust "Symantec Trial Secure Server CA - G3"

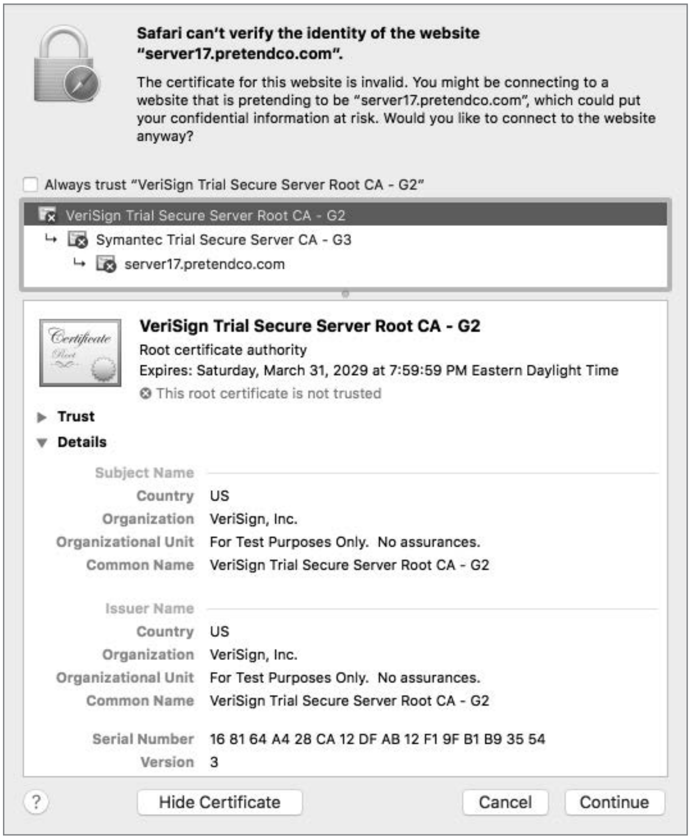
VeriSign Trial Secure Server Root CA - G2
↳ Symantec Trial Secure Server CA - G3
↳ server17.pretendco.com

Symantec Trial Secure Server CA - G3
Intermediate certificate authority
Expires: Friday, December 6, 2024 at 6:59:59 PM Eastern Standard Time
⊗ This certificate was signed by an untrusted issuer

▶ **Trust**
▼ **Details**

Subject Name	
Country	US
Organization	Symantec Corporation
Organizational Unit	For Test Purposes Only. No assurances.
Common Name	Symantec Trial Secure Server CA - G3
Issuer Name	
Country	US
Organization	VeriSign, Inc.
Organizational Unit	For Test Purposes Only. No assurances.
Common Name	VeriSign Trial Secure Server Root CA - G2
Serial Number	12 88 0B A5 C7 77 45 A8 D5 A9 15 8C 95 42 86 B9
Version	3

Finally, when you select the certificate at the top of the certificate chain, you see that this is a root CA; the window states "This root certificate is not trusted." This root CA is not in this computer's System Root keychain, so Safari doesn't trust the intermediate CA, and it doesn't trust the server17.pretendco.com certificate either.



Safari can't verify the identity of the website "server17.pretendco.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "server17.pretendco.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

□ Always trust "VeriSign Trial Secure Server Root CA - G2"

VeriSign Trial Secure Server Root CA - G2
↳ Symantec Trial Secure Server CA - G3
↳ server17.pretendco.com

VeriSign Trial Secure Server Root CA - G2
Root certificate authority
Expires: Saturday, March 31, 2029 at 7:59:59 PM Eastern Daylight Time
This root certificate is not trusted

▶ Trust
▼ Details

Subject Name
Country: US
Organization: VeriSign, Inc.
Organizational Unit: For Test Purposes Only. No assurances.
Common Name: VeriSign Trial Secure Server Root CA - G2

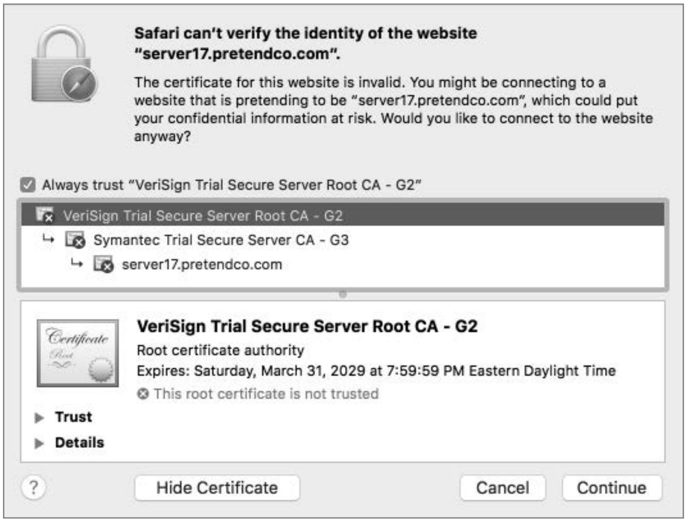
Issuer Name
Country: US
Organization: VeriSign, Inc.
Organizational Unit: For Test Purposes Only. No assurances.
Common Name: VeriSign Trial Secure Server Root CA - G2

Serial Number: 16 81 64 A4 28 CA 12 DF AB 12 F1 9F B1 B9 35 54
Version: 3

Since that example root CA is for trial use only, you should not configure your Mac to always trust it outside of a learning or testing environment.

Configuring Trust

You can configure your Mac to always trust a certificate for the currently logged-in user. Returning to the previous example of your server using its self-signed SSL certificate for a website, you can click Show Certificate and then select the "Always trust..." option.



Safari can't verify the identity of the website "server17.pretendco.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "server17.pretendco.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

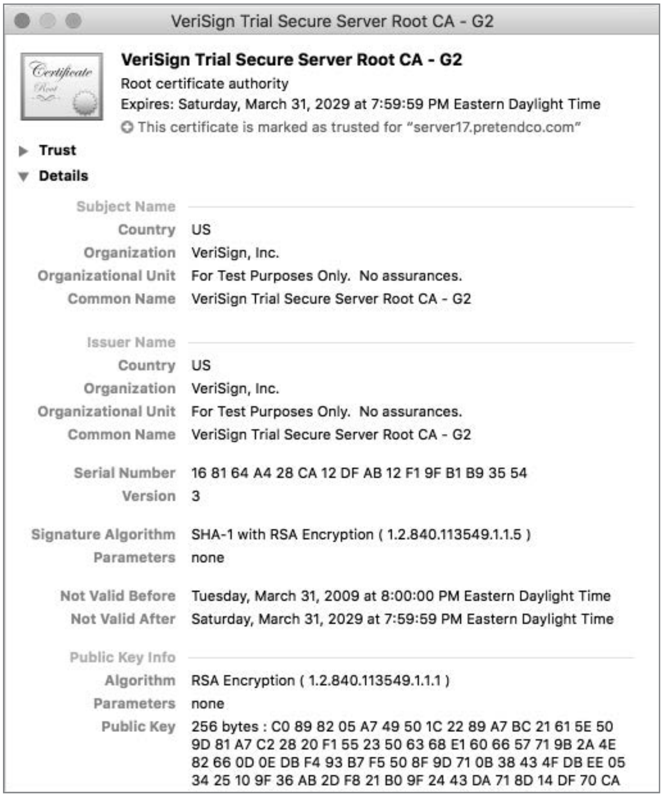
☑ Always trust "VeriSign Trial Secure Server Root CA - G2"

VeriSign Trial Secure Server Root CA - G2
↳ Symantec Trial Secure Server CA - G3
↳ server17.pretendco.com

VeriSign Trial Secure Server Root CA - G2
Root certificate authority
Expires: Saturday, March 31, 2029 at 7:59:59 PM Eastern Daylight Time
This root certificate is not trusted

OS X then asks for your login credentials. After you successfully authenticate, OS X adds the certificate to your personal login keychain and configures your system to always trust the certificate for SSL purposes so that your Mac trusts it when you are logged in with the account you were logged in as when you selected the "Always trust..." option. This will not affect any other computers or devices or any other users who log in to that Mac.

In Keychain Access, you can open and inspect the self-signed certificate you just added. Note the blue (+) icon with the text that states the certificate is marked as trusted for server17.pretendco.com.



VeriSign Trial Secure Server Root CA - G2

VeriSign Trial Secure Server Root CA - G2

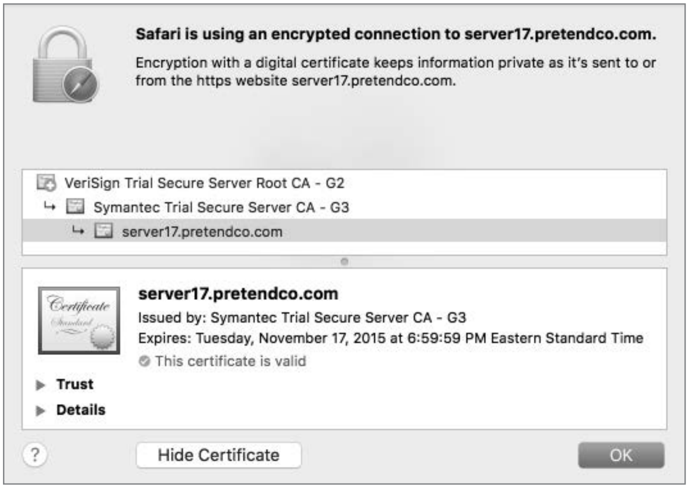
Root certificate authority

Expires: Saturday, March 31, 2029 at 7:59:59 PM Eastern Daylight Time

This certificate is marked as trusted for "server17.pretendco.com"

Subject Name	
Country	US
Organization	VeriSign, Inc.
Organizational Unit	For Test Purposes Only. No assurances.
Common Name	VeriSign Trial Secure Server Root CA - G2
Issuer Name	
Country	US
Organization	VeriSign, Inc.
Organizational Unit	For Test Purposes Only. No assurances.
Common Name	VeriSign Trial Secure Server Root CA - G2
Serial Number	16 81 64 A4 28 CA 12 DF AB 12 F1 9F B1 B9 35 54
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday, March 31, 2009 at 8:00:00 PM Eastern Daylight Time
Not Valid After	Saturday, March 31, 2029 at 7:59:59 PM Eastern Daylight Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : C0 89 82 05 A7 49 50 1C 22 89 A7 BC 21 61 5E 50 9D 81 A7 C2 28 20 F1 55 23 50 63 68 E1 60 66 57 71 9B 2A 4E 82 66 0D 0E DB F4 93 B7 F5 50 8F 9D 71 0B 38 43 4F DB EE 05 34 25 10 9F 36 AB 2D F8 21 B0 9F 24 43 DA 71 8D 14 DF 70 CA

After you visit the site again in Safari, if you click the encryption icon in the Address and Search field and then click Show Certificate, you see similar information.



Safari is using an encrypted connection to server17.pretendco.com.

Encryption with a digital certificate keeps information private as it's sent to or from the https website server17.pretendco.com.

VeriSign Trial Secure Server Root CA - G2
↳ Symantec Trial Secure Server CA - G3
↳ server17.pretendco.com

server17.pretendco.com

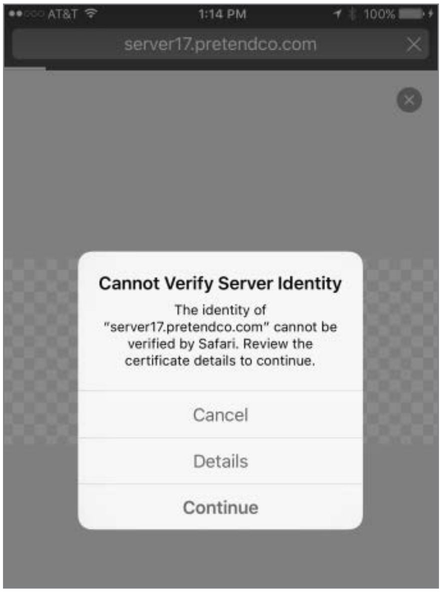
Issued by: Symantec Trial Secure Server CA - G3

Expires: Tuesday, November 17, 2015 at 6:59:59 PM Eastern Standard Time

This certificate is valid

A further option for Mac computers is to download and install the certificate in the System keychain, with the "Always trust..." option selected for SSL. Keep in mind that you would need to do this for *every* Mac that uses SSL-enabled services from your server.

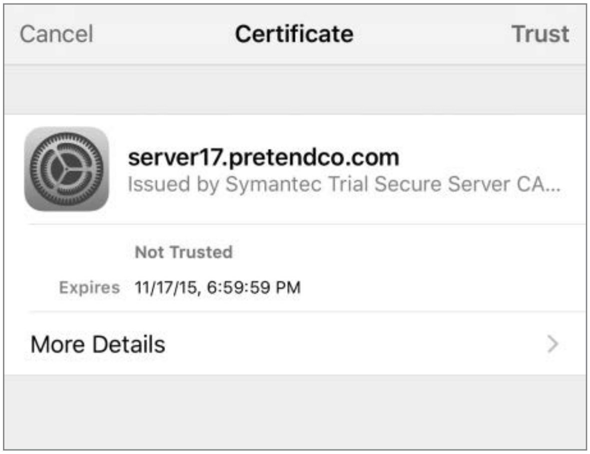
For an iOS device, when you open Safari to a page protected by the server's self-signed certificate, you can tap Details.



Cannot Verify Server Identity

The identity of "server17.pretendco.com" cannot be verified by Safari. Review the certificate details to continue.

Then tap Trust.



server17.pretendco.com
Issued by Symantec Trial Secure Server CA...

Not Trusted

Expires 11/17/15, 6:59:59 PM

Now your iOS device is configured to trust that certificate.

Note that you can use a configuration profile to distribute a certificate to Mac computers and iOS devices. This automatically configures the device to trust the certificate. See Lesson 10, "Managing with Profile Manager" for more information about profiles.

See Exercise 4.3, "Configure Your Client Computer to Trust an SSL Certificate" for complete instructions.

Reference 4.3
Troubleshooting

Certificate Assistant uses the IPv4 address of the Mac from which you run the Server app, so if you're using an administrator computer to configure a remote server and generate a new self-signed certificate, be sure to use the server's host name and IP address where appropriate.

When you configure your server as an Open Directory server, if you have a self-signed certificate with your server's host name in the certificate's Common Name field, the Server app replaces the original self-signed SSL certificate with a new certificate. This new certificate will be signed by a newly created intermediate CA associated with your server's Open Directory service.

However, if you have a certificate with your server's host name in the certificate's Common Name field and the certificate is signed by a CA or an intermediate CA (that is not associated with your Open Directory service), then the Server app doesn't replace it with a new one signed by the Open Directory intermediate CA (however, the Server app still creates the Open Directory CA and intermediate CA).

Each certificate has an expiration date; if the current date is later than a certificate's expiration date, the certificate is not valid.

> **NOTE ►** Some files associated with certificates are stored in /private/etc/certificates/, and possibly /private/var/root/Library/Application Support/Certificate Authority/, on your server.

Exercise 4.1
Examine the Default SSL Certificate

Prerequisite

- Exercise 1.2, "Perform the Initial Installation of OS X Server on Your Server Computer"

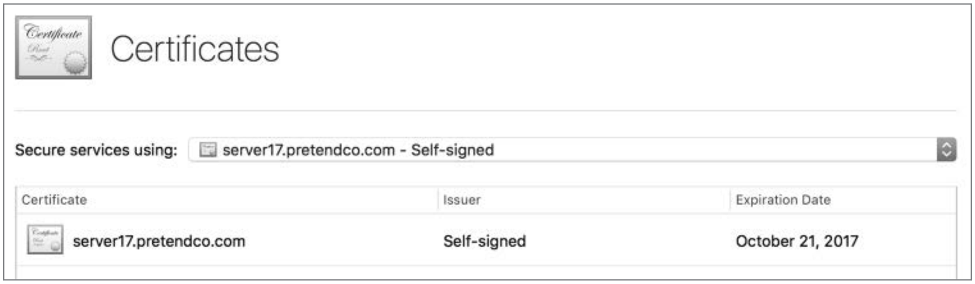
In this exercise, you will examine the default self-signed certificate.

1. If necessary, on your server, open the Server app.

   If the Server app does not automatically connect to your server and you are at the Choose a Mac window, select your server, click Continue, provide administrator credentials (Administrator Name: ladmin; Administrator Password: ladminpw), deselect the "Remember this password in my keychain" checkbox, and then click Connect.

2. In the Server app sidebar, select Certificates.

3. Note that by default your server's services use a certificate that is self-signed.

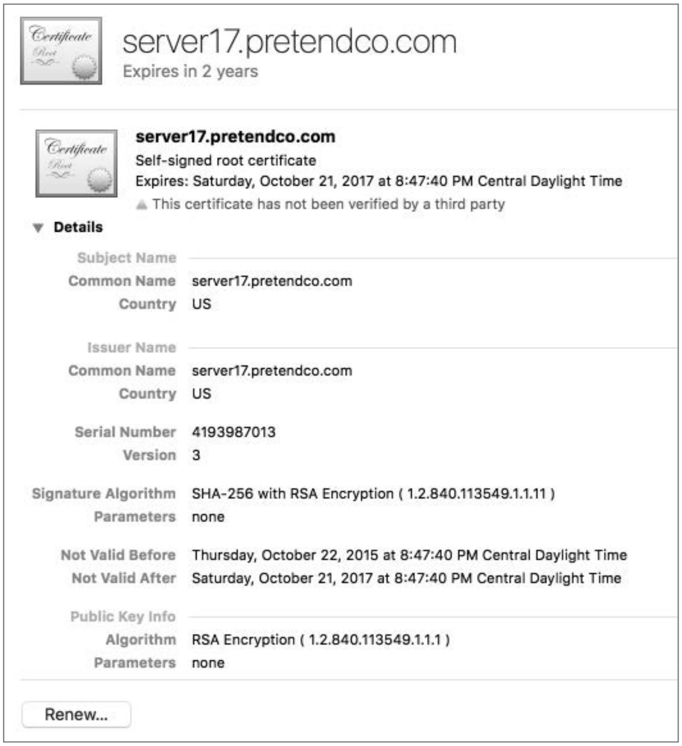


Certificates

Secure services using: server17.pretendco.com - Self-signed

Certificate	Issuer	Expiration Date
server17.pretendco.com	Self-signed	October 21, 2017

4. View the details of the certificate. Double-click the self-signed certificate; alternatively, select the certificate, and then click the Edit (pencil) button.



server17.pretendco.com
Expires in 2 years

server17.pretendco.com
Self-signed root certificate
Expires: Saturday, October 21, 2017 at 8:47:40 PM Central Daylight Time
▲ This certificate has not been verified by a third party

▼ **Details**

Subject Name	
Common Name	server17.pretendco.com
Country	US
Issuer Name	
Common Name	server17.pretendco.com
Country	US
Serial Number	4193987013
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	none
Not Valid Before	Thursday, October 22, 2015 at 8:47:40 PM Central Daylight Time
Not Valid After	Saturday, October 21, 2017 at 8:47:40 PM Central Daylight Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none

5 Click OK return to the Certificates pane.

Note that there is little identifying information associated with this certificate. For example, there is no email address, organization name, department, or city. By default, no other computer or device trusts this self-signed certificate. To use this self-signed certificate to secure your server's services, you could configure your client computers and devices to trust this certificate.

Alternatively, you could click the Add (+) button, choose Get a Trusted Certificate, send the resulting certificate signing request to a widely trusted certificate authority to sign, and then import the signed certificate. However, this is outside the scope of this guide, so the next exercise is a compromise between using a self-signed certificate with little information and using a certificate signed by a widely trusted CA.

Exercise 4.2
Configure an Open Directory Certificate Authority

Prerequisites

- Exercise 1.2, "Perform the Initial Installation of OS X Server on Your Server Computer"
- Exercise 2.1, "Create DNS Zones and Records"

When you configure your server as an Open Directory (OD) master, the Server app automatically creates an OD CA, an intermediate CA, a signed certificate, and a code signing certificate that you can use with the Profile Manager service. When you enroll your Mac computer or your iOS device with your server's Profile Manager service, your computer automatically trusts your server's OD CA. Additionally, if you bind your Mac to your OD server, it automatically trusts your server's OD CA. This guide has not yet covered binding or enrolling, so in Exercise 4.3, "Configure Your Client Computer to Trust an SSL Certificate," you will use Safari to configure your client computer to trust your server's OD CA.

In this exercise, you will configure your OD CA. You will examine the new CA, the intermediate CA, and two new certificates and verify that the Server app automatically removes your server's old default self-signed certificate, updates services to use the certificate signed by the intermediate CA, and configures your server to trust the new certificates.

Configure Open Directory

Because the Server app creates keychain entries on your server, perform the following steps on your server.

Correct DNS records are crucial to the proper functioning of Open Directory services, so double-check DNS before starting the Open Directory service.

1 On your server computer, open Network Utility (use Spotlight if necessary).

2 Click the Lookup tab.

3 Enter your server's host name in the field (server*n*.pretendco.com, where *n* is your student number), and then click Lookup.

4 Confirm that your server's IPv4 address is returned.

5 Enter your server's primary IPv4 address in the field (10.0.0.*n*1, where *n* is your student number), and then click Lookup.

6 Confirm that your server's host name is returned.

Once you've confirmed your DNS records, configure your server as an Open Directory master.

1 In the Server app sidebar under the Advanced section, select Open Directory.

2 Click the on/off switch to turn on the Open Directory service (or in the Server app sidebar, Control-click Open Directory, and choose Start Open Directory Service).

3 Select "Create a new Open Directory domain," and click Next.

4 In the Directory Administrator pane, leave the checkbox "Remember this password in my keychain" selected.

5 Enter and verify a password.

If your server is not accessible from the Internet, in the Directory Administrator pane, enter diradminpw in the Password and Verify fields.

Of course, in a production environment, you should use a secure password and consider using an account name different from the default "diradmin" so that it is more difficult for unauthorized people to guess the username and password combination.

6 Click Next.

7 In the Organization Information pane, enter the appropriate information.

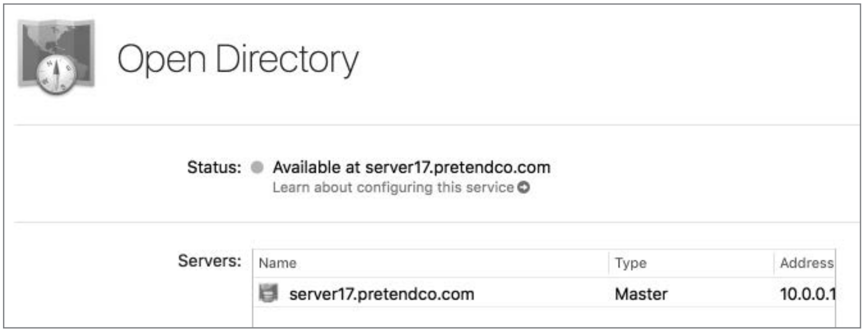
If the following fields do not already contain the information shown, enter it, and click Next.

- Organization Name: Pretendco Project *n* (where *n* is your student number)
- Admin Email Address: ladmin@server*n*.pretendco.com (where *n* is your student number)

8 View the Confirm Settings pane, and click Set Up.

The Server app displays its progress in the lower-left corner of the Confirm Settings pane.

When it has completed the configuration, the Server app displays the Settings tab of the Open Directory pane, with your server listed as the master in the Servers list.



Open Directory

Status: ● Available at server17.pretendco.com
Learn about configuring this service

Servers:

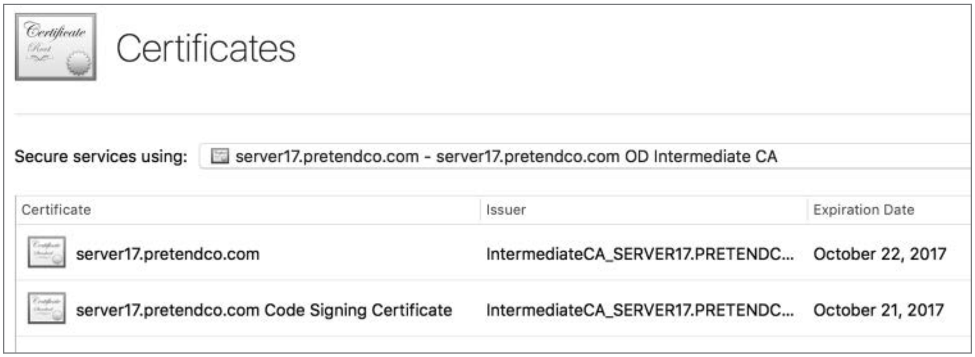
Name	Type	Address
server17.pretendco.com	Master	10.0.0.1

Inspect the OD Certificates

Inspect the certificates that the Server app automatically created.

1 In the Server app sidebar, select Certificates.

2 Confirm that the "Secure services using" pop-up menu is no longer set to a self-signed certificate but rather a certificate signed by your server's OD intermediate CA.



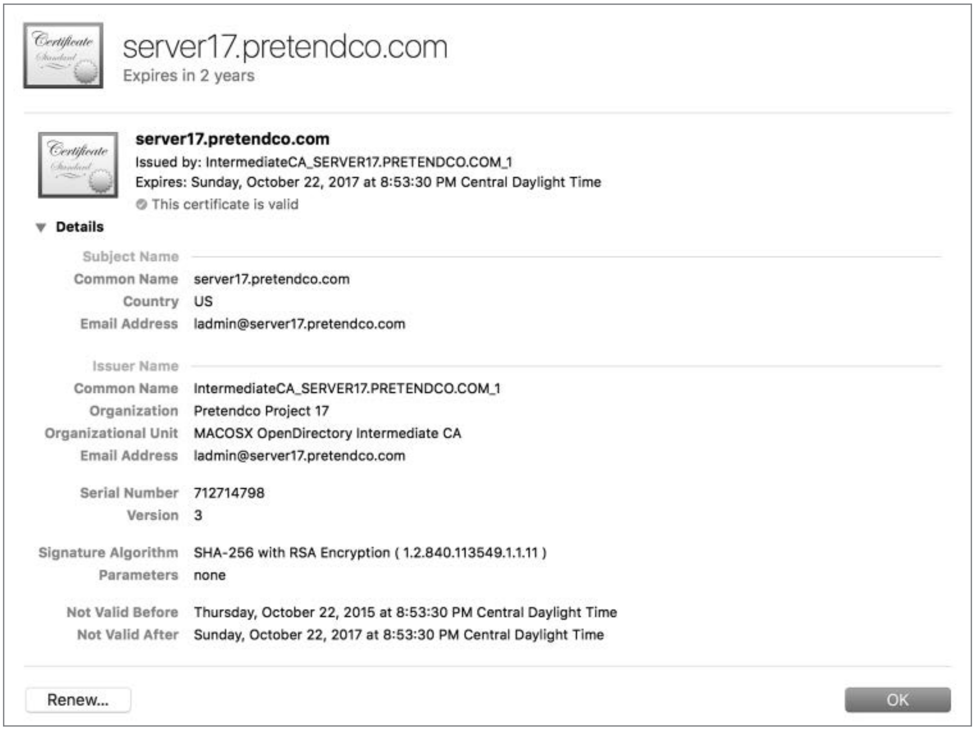
Certificates

Secure services using: server17.pretendco.com - server17.pretendco.com OD Intermediate CA

Certificate	Issuer	Expiration Date
server17.pretendco.com	IntermediateCA_SERVER17.PRETENDC...	October 22, 2017
server17.pretendco.com Code Signing Certificate	IntermediateCA_SERVER17.PRETENDC...	October 21, 2017

3 Confirm that the self-signed certificate is no longer listed in the Certificates field.

4 Double-click the certificate with your server's host name, signed by your OD intermediate CA (the first entry in the Certificates field).



server17.pretendco.com
Expires in 2 years

server17.pretendco.com
Issued by: IntermediateCA_SERVER17.PRETENDCO.COM_1
Expires: Sunday, October 22, 2017 at 8:53:30 PM Central Daylight Time
This certificate is valid

▼ **Details**

Subject Name
Common Name server17.pretendco.com
Country US
Email Address ladmin@server17.pretendco.com

Issuer Name
Common Name IntermediateCA_SERVER17.PRETENDCO.COM_1
Organization Pretendco Project 17
Organizational Unit MACOSX OpenDirectory Intermediate CA
Email Address ladmin@server17.pretendco.com

Serial Number 712714798
Version 3

Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters none

Not Valid Before Thursday, October 22, 2015 at 8:53:30 PM Central Daylight Time
Not Valid After Sunday, October 22, 2017 at 8:53:30 PM Central Daylight Time

5 Confirm that the value for the "Issued by" field has a value made up of the following strings:

- "IntermediateCA_"
- Your server's host name in all capital letters
- "_1"

6 Click OK to close the certificate information pane.

7 Double-click the code signing certificate (the second entry in the Certificates field).

8 Confirm that this is also issued by your OD intermediate CA.

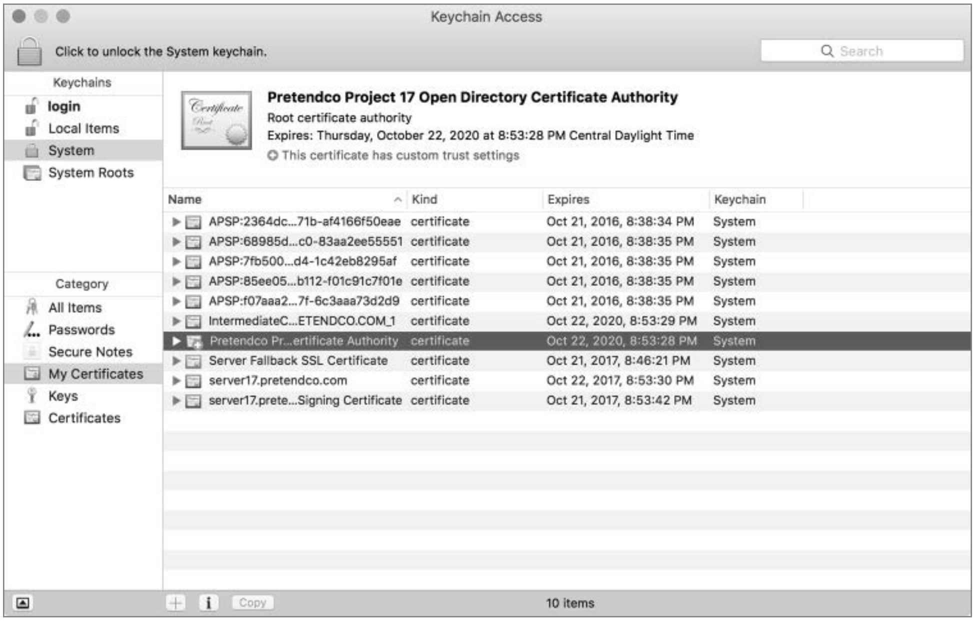
Use Keychain Access to inspect your OD CA, your OD intermediate CA, and the two signed certificates.

1 On your server, use a Spotlight search to open Keychain Access.

2 In the Keychains column, select System.

3 In the Category column, select My Certificates.

4 Select your OD CA. Its name is Pretendco Project *n* Open Directory Certificate Authority (where *n* is your student number).

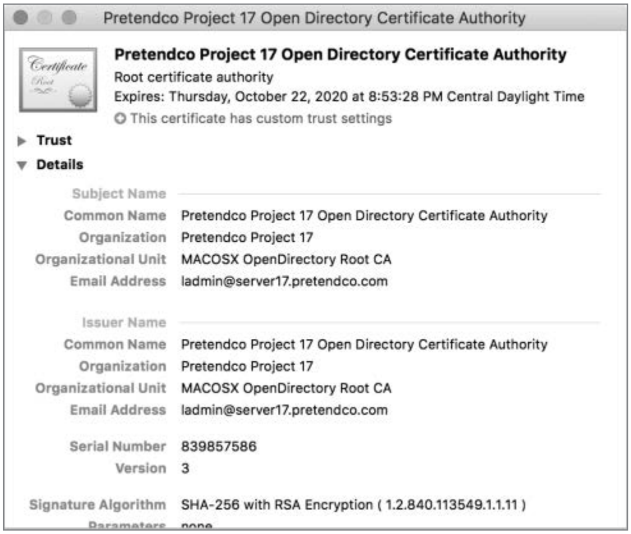


Pretendco Project 17 Open Directory Certificate Authority
Root certificate authority
Expires: Thursday, October 22, 2020 at 8:53:28 PM Central Daylight Time
This certificate has custom trust settings

Name	Kind	Expires	Keychain
APSP:2364dc...71b-af4166f50eae	certificate	Oct 21, 2016, 8:38:34 PM	System
APSP:68985d...c0-83aa2ee55551	certificate	Oct 21, 2016, 8:38:35 PM	System
APSP:7fb500...d4-1c42eb8295af	certificate	Oct 21, 2016, 8:38:35 PM	System
APSP:85ee05...b112-f01c91c7f01e	certificate	Oct 21, 2016, 8:38:35 PM	System
APSP:f07aaa2...7f-6c3aaa73d2d9	certificate	Oct 21, 2016, 8:38:35 PM	System
IntermediateC...ETENDCO.COM_1	certificate	Oct 22, 2020, 8:53:29 PM	System
Pretendco Pr...ertificate Authority	certificate	Oct 22, 2020, 8:53:28 PM	System
Server Fallback SSL Certificate	certificate	Oct 21, 2017, 8:46:21 PM	System
server17.pretendco.com	certificate	Oct 22, 2017, 8:53:30 PM	System
server17.prete...Signing Certificate	certificate	Oct 21, 2017, 8:53:42 PM	System

5 Double-click your OD CA to examine it.

6 Confirm that the second line of text identifies it as “Root certificate authority” and that the Subject Name information matches the Issuer Name information.



Pretendco Project 17 Open Directory Certificate Authority

Pretendco Project 17 Open Directory Certificate Authority
Root certificate authority
Expires: Thursday, October 22, 2020 at 8:53:28 PM Central Daylight Time
This certificate has custom trust settings

▶ Trust
▼ Details

Subject Name
Common Name Pretendco Project 17 Open Directory Certificate Authority
Organization Pretendco Project 17
Organizational Unit MACOSX OpenDirectory Root CA
Email Address ladmin@server17.pretendco.com

Issuer Name
Common Name Pretendco Project 17 Open Directory Certificate Authority
Organization Pretendco Project 17
Organizational Unit MACOSX OpenDirectory Root CA
Email Address ladmin@server17.pretendco.com

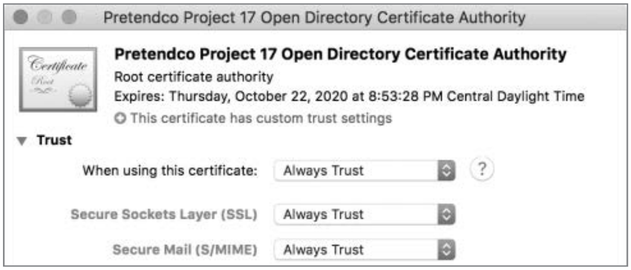
Serial Number 839857586
Version 3

Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters none

7 Note that the certificate's color is bronze, which signifies that it is a root certificate.

8 Click the Trust disclosure triangle to display more details.

9 Confirm that your server is set to always trust this certificate.



Pretendco Project 17 Open Directory Certificate Authority

Pretendco Project 17 Open Directory Certificate Authority
Root certificate authority
Expires: Thursday, October 22, 2020 at 8:53:28 PM Central Daylight Time
This certificate has custom trust settings

▼ Trust

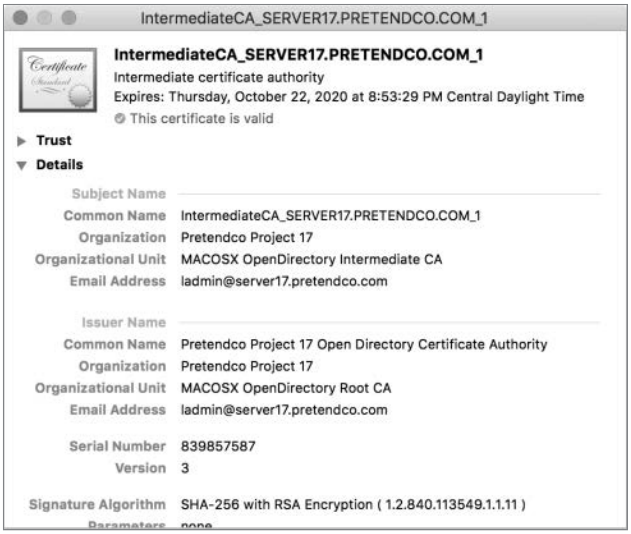
When using this certificate: Always Trust
Secure Sockets Layer (SSL) Always Trust
Secure Mail (S/MIME) Always Trust

10 Close the window with the details of your OD CA.

11 Double-click your OD intermediate CA.

12 Confirm that its second line of text identifies it as "Intermediate certificate authority." Because your server trusts your OD CA and your OD CA signed this intermediate CA, this certificate is marked as valid with a green checkmark.

Note that the color of the certificate is blue, which signifies that it is an intermediate or leaf certificate.



IntermediateCA_SERVER17.PRETENDCO.COM_1

IntermediateCA_SERVER17.PRETENDCO.COM_1
Intermediate certificate authority
Expires: Thursday, October 22, 2020 at 8:53:29 PM Central Daylight Time
This certificate is valid

▶ Trust
▼ Details

Subject Name
Common Name IntermediateCA_SERVER17.PRETENDCO.COM_1
Organization Pretendco Project 17
Organizational Unit MACOSX OpenDirectory Intermediate CA
Email Address ladmin@server17.pretendco.com

Issuer Name
Common Name Pretendco Project 17 Open Directory Certificate Authority
Organization Pretendco Project 17
Organizational Unit MACOSX OpenDirectory Root CA
Email Address ladmin@server17.pretendco.com

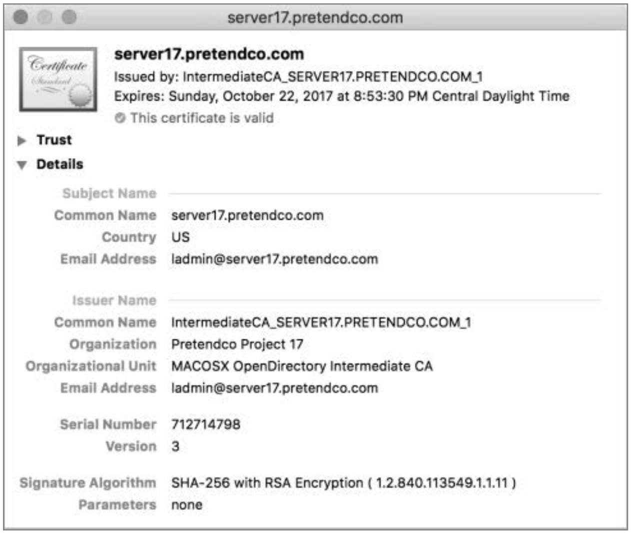
Serial Number 839857587
Version 3

Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters none

13 Close the window with the details of your OD intermediate CA.

14 Double-click the certificate that contains only your server's host name.

15 Confirm that the second line of text indicates that it is signed by your OD intermediate CA. Your server is configured to trust your OD CA, which signed your OD intermediate CA, which signed this certificate, so it is marked as valid with a green checkmark.



server17.pretendco.com

server17.pretendco.com
Issued by: IntermediateCA_SERVER17.PRETENDCO.COM_1
Expires: Sunday, October 22, 2017 at 8:53:30 PM Central Daylight Time
This certificate is valid

▶ Trust
▼ Details

Subject Name
Common Name server17.pretendco.com
Country US
Email Address ladmin@server17.pretendco.com

Issuer Name
Common Name IntermediateCA_SERVER17.PRETENDCO.COM_1
Organization Pretendco Project 17
Organizational Unit MACOSX OpenDirectory Intermediate CA
Email Address ladmin@server17.pretendco.com

Serial Number 712714798
Version 3

Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters none

16 Double-click your code signing certificate, inspect it, and close it.

17 Quit Keychain Access.

In this exercise, you configured your server to be an Open Directory master. The Server app automatically configured a new OD CA, intermediate CA, and two new certificates; it removed your server's old default self-signed certificate, and it updated services to use the certificate signed by the intermediate CA. It automatically configured your server to trust its own OD CA, which means that your server also trusts the OD intermediate CA and the two other certificates that are signed by the OD intermediate CA.

Exercise 4.3
Configure Your Client Computer to Trust an SSL Certificate

Prerequisite

- Exercise 4.2, "Configure an Open Directory Certificate Authority"

NOTE ► If you obtained a certificate from a widely trusted CA, you do not need to perform this exercise.

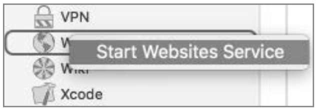
In a production environment, it is best to use a valid SSL certificate that's been signed by a trusted CA. If that isn't possible, you should configure your users' computers and devices to trust your server's certificate so that your users do not get into the habit of configuring their devices to trust unverified SSL certificates.

This lesson shows you how to configure an individual computer to trust your server's OD CA; it is beyond the scope of this exercise to show you how to replicate the end result on multiple computers and devices.

Turn On the Web Service Temporarily

Turn on your server's Websites service so you can quickly access the SSL certificate your server's services use.

1 In the Server app sidebar, rest the pointer over the word *Websites*, Control-click Websites, and then choose Start Websites Service.



Visit Your Server’s Website Protected by SSL

In this exercise, you will use your client computer and confirm that you are using your server’s DNS service; otherwise, you will not be able to connect to its web service using its host name. Then you’ll open Safari to your server’s default HTTPS website. Finally, you’ll configure your client computer to trust the SSL certificate.

1 On your client computer, open System Preferences.

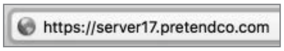
2 Open the Network pane.

3 Select the active network service, and confirm that your server’s IP address is listed for the DNS Service value.

If you are using Wi-Fi, you need to click Advanced, click the DNS tab to view the DNS Service value, and then click Cancel to close the Advanced pane.

4 Quit System Preferences.

5 On your client computer, open Safari, and in the Address and Search field, enter https://server*n*.pretendco.com (where *n* is your student number).


https://server17.pretendco.com

6 Press Return to open the page.

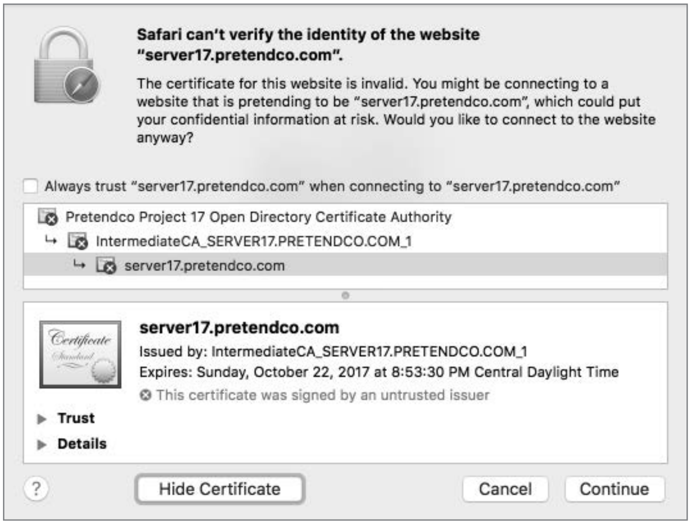
Your certificate is not signed by a CA that your client computer is configured to trust, so you’ll see a message that Safari can’t verify the identity of the website.

Configure Your Client Computer to Trust This SSL Certificate

Once you see the dialog that Safari can’t verify the identity of the website, you can click Show Certificate and configure the currently logged-in user to trust the SSL certificate used by the website.

1 Click Show Certificate.

2 Note that the certificate with your server's host name is marked in red with "This certificate was signed by an untrusted issuer."



Safari can't verify the identity of the website "server17.pretendco.com".

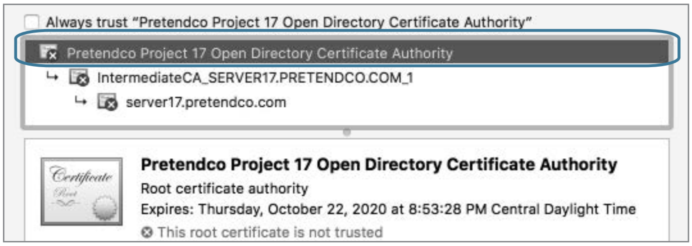
The certificate for this website is invalid. You might be connecting to a website that is pretending to be "server17.pretendco.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

□ Always trust "server17.pretendco.com" when connecting to "server17.pretendco.com"

Pretendco Project 17 Open Directory Certificate Authority
↳ IntermediateCA_SERVER17.PRETENDCO.COM_1
↳ server17.pretendco.com

server17.pretendco.com
Issued by: IntermediateCA_SERVER17.PRETENDCO.COM_1
Expires: Sunday, October 22, 2017 at 8:53:30 PM Central Daylight Time
This certificate was signed by an untrusted issuer

3 In the certificate chain, select your OD CA.



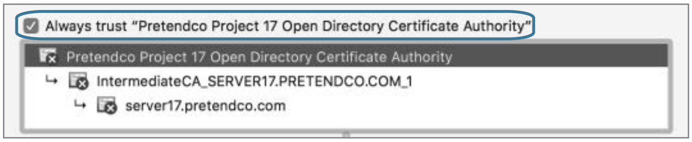
□ Always trust "Pretendco Project 17 Open Directory Certificate Authority"

Pretendco Project 17 Open Directory Certificate Authority
↳ IntermediateCA_SERVER17.PRETENDCO.COM_1
↳ server17.pretendco.com

Pretendco Project 17 Open Directory Certificate Authority
Root certificate authority
Expires: Thursday, October 22, 2020 at 8:53:28 PM Central Daylight Time
This root certificate is not trusted

4 Click the Details disclosure triangle, and inspect the details.

5 Select the checkbox "Always trust Pretendco Project *n* Open Directory Certificate Authority" (where *n* is your student number).



☑ Always trust "Pretendco Project 17 Open Directory Certificate Authority"

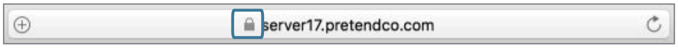
Pretendco Project 17 Open Directory Certificate Authority
↳ IntermediateCA_SERVER17.PRETENDCO.COM_1
↳ server17.pretendco.com

6 Click Continue.

7 Provide your login credentials, and click Update Settings.

This updates the settings only for the currently logged-in user; this does not affect any other user on this computer.

8 Confirm the Safari Address and Search field displays a lock icon, which indicates that the page was opened using SSL.



9 Keep Safari open for the next section of this exercise.

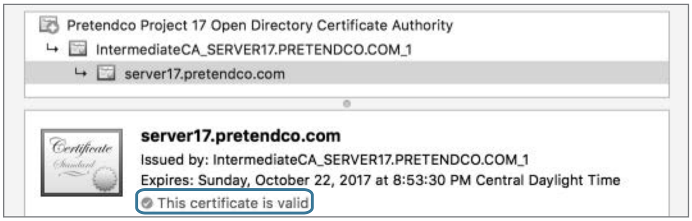
Confirm That Your Mac Trusts the SSL Certificate

To view the SSL certificate the Websites service is using, perform the following steps.

1 In the Safari Address and Search field, click the lock icon.

2 In the pane that informs you that Safari is using an encrypted connection, click Show Certificate.

3 Confirm that the certificate is listed as valid with a green checkmark.



Pretendco Project 17 Open Directory Certificate Authority
↳ IntermediateCA_SERVER17.PRETENDCO.COM_1
↳ server17.pretendco.com

server17.pretendco.com
Issued by: IntermediateCA_SERVER17.PRETENDCO.COM_1
Expires: Sunday, October 22, 2017 at 8:53:30 PM Central Daylight Time
This certificate is valid

NOTE ► If you see a blue icon instead of a green checkmark, and you don't see the certificate chain, it's likely that you trusted the server certificate instead of the CA certificate. Click OK, quit Safari, open Keychain Access, select All Items in the Category column, enter your server's host name in the Search field, select your server's certificate, press Delete, then at the confirmation dialog, click Delete, provide local administrator credentials then click Update Settings. Quit Keychain Access. Repeat the steps of this exercise, starting with the section "Visit Your Server's Website Protected by SSL."

4 Press Command-Q to quit Safari.

Clean Up

To ensure that the rest of the exercises are consistent, turn off the Websites service.

1. On your server computer, in the Server app sidebar, select the Websites service, and Click the on/off switch to turn the service off.

2. Confirm that no green status indicators appear next to the Websites service.

   This indicates that the service is off.

You confirmed that your server's default web service uses the SSL certificate you configured in the previous exercise. You confirmed that by trusting a CA, you trust a certificate that was signed by an intermediate CA that was signed by the CA (at least for the currently logged-in user).

Index

Symbols

.. (double period), 648
\ (backslash character), 647–648
$ (dollar sign), 641
* (asterisk) wildcard, 655
? (question mark) wildcard, 655
[ ] (square brackets) wildcard, 655
~ (tilde) character, 649, 672

A

A (machine) record, 67, 71
About This Mac, 4–5, 26–27
absolute paths, 646
access. See also file access
- to command line, 640–641
- to DNS service, 78–80
- to Mail services, 558–559
- Profile Manager restrictions, 280
- to recursive lookups, 77–78
- restoring default, 80–81
- to services, 237–239, 269–273
- to shared files, 336–337, 370–375
- to shared folders, 365–366
- troubleshooting file sharing, 355
- troubleshooting services, 248
- to web services, 531
- to websites, 547–549
- to wikis, 582

access control entries. See ACEs (access control entries)
access control lists. See ACLs (access control lists)
Access log
- Apple Filing Protocol, 375, 678
- monitoring web services, 528, 549–551

Access pane, Server app, 91–93
Access segment, File Sharing pane, 345
Access tab, Server app
- custom access rules, 110–112
- default access rules, 106–109
- exploring, 106
- overview of, 91–93
- restoring default access, 112
- restricting access to DNS service, 79

account name (short name)
- defined, 296
- disconnecting connected users, 368
- overview of, 224–225
- POSIX/ACL rules of precedence, 399
- UID associated with, 227

ACEs (access control entries)
- ACL inheritance, 391–393
- ACL portability, 394
- ACLs containing, 385
- configuring ACLs, 386–389
- configuring complex permissions, 390–391
- configuring group folders, 353
- features common to POSIX and ACLs, 395–398
- functionality of, 385–386
- how file system ACLs work, 386
- propagating permissions, 394–395
- rules of precedence for POSIX and ACLs, 398–399
- sorting ACLs canonically, 394
- in Storage pane permissions dialog, 383
- updating permissions, 411–413
- views of permissions, 415–416, 418

ACK, DHCP logs, 512–513, 519
ACLs (access control lists)
- accessing files/folders, 377
- adding flexibility to POSIX with, 384
- configuring, 386–389
- configuring complex permissions, 390–391
- confirming access request, 404–410
- features common to POSIX and, 395–398
- inheritance, 391–393
- overview of, 385–386
- propagating permissions, 394–395
- rules of precedence, 398–399
- sorting canonically, 394
- updating permissions, 412
- views of permissions, 415–416, 418

activity logs, AFP, 676–677
Activity Monitor, 462, 464
AD (Active Directory)
- Calendar integration with, 595
- configuring WebDAV service for, 341
- external DNS server for, 61–62

Add (+) button
- ACE, 403–404
- blog to wiki, 591
- Contact, 615
- DHCP network, 509
- DHCP service, 516
- DNS record, 70, 72, 541
- DNS service permissions, 79
- forwarding servers, 68
- nameserver record for reverse zone, 74
- Open Directory locale, 197–198
- share points, 347–349
- website, 524, 543

address book, Contacts, 609
administration
- at command line, 640, 661–663
- complex permissions for ACE, 390
- of wikis, 582

administrator account
- adding in System Image Utility, 427
- configuring, 21, 230–231
- creating for DEP, 288
- creating for VPP, 291
- creating new, 323–324
- local. See Local Admin account
- name. See ladmin command (Administrator Name)
- password. See ladminpw command (Administrator Password)

Advanced Options, user accounts, 226–228
advanced services, 96–98
AFP Access Log, 375
AFP (Apple Filing Protocol)
- adding/removing share points, 347–349
- authentication, 221
- confirming password, 267
- editing share points, 351
- file/folder ownership/permissions, 384
- file-sharing protocols, 340–341

file sharing with, 337
inspecting/modifying with serveradmin, 675–680
inspecting NetInstall shared folders, 445–446
personal folders for iOS with, 353
reviewing file sharing logs, 344
shared folders for home directories, 351–352
shared folders over different protocols, 339
troubleshooting File Sharing, 375–376
VPN file encryption for, 483
AFP Error Log, 375–376
AirDrop, 12–13
Airport, 60, 93–95
alerts
certificate renewal, 130–131
configuring, 158–160, 166–168
host name change, 42
sending test, 168–170
virus filtering, 561
Alerts pane, Server app, 157–160
alias (CNAME) record, 67, 70, 71
aliases
assigning user account, 227
web service, 531
website, 526
Allow remote administration using Server checkbox, 83
Allow rule
ACEs, 385–386
ACLs, 386
Allow, self-signed certificate, 126
Always Allow, self-signed certificate, 126
Always trust… option, 138–139
Amavis virus-scanning, email, 561
anonymous binding, 208
Apache
modules, 523
monitoring web services, 528
OS X Server web service based on, 522
APNs (Apple Push Notifications)
configuring in Settings pane, 88–89
configuring initial install of Server app, 42–43
configuring OS X Server alerts, 158–160
delivering profiles, 298
enabling Profile Manager, 280, 287
process of, 299
troubleshooting Server app, 102
App Analytics screen, client iOS device, 56
App Store, using Caching service with, 452
Apple Filing Protocol. See AFP (Apple Filing Protocol)
Apple ID credentials
Apple Push Notifications, 43
client iOS device setup, 55
configuring OS X before OS X Server install, 23
Device Enrollment Program, 284
Keynote for iOS, 371–372
Local Admin account, 26
as partition scheme for disk, 8
Profile Manager for VPP, 292
Profile Manager setup, 279, 287
Apple Remote Desktop. See ARD (Apple Remote Desktop)
Apple Root Certificate Program, 115
applications, command-line equivalents for, 639
Applications folder, 102
apps
distributing with Profile Manager, 292–293
installing across multiple computers, 422
managing, 297–298
apropos command, 645
archive certificate, SSL, 130
archive files
creating Open Directory, 177, 202–204
Messages personal chat, 622–623
turning on Messages, 625–626
viewing Messages, 635–636
Archive Open Directory Master, 203–204
ARD (Apple Remote Desktop)
administering users and groups remotely, 222
computer name, 12–13
controlling Mac running OS X Server, 84–85
monitoring/managing server from different computer, 158
using command-line instructions, 640
arguments (parameters), command string, 643
asterisk (*) wildcard, command line, 655
Attachment button, 589–590
attributes
creating user/group templates, 227–228
viewing/modifying user account, 226–227
audio conference, Messages service, 619
authenticated binding, 208
authentication
to AirPort device, 93
describing, 220–222
as file-sharing challenge, 336
Kerberos, 242–247
mail service access, 558–559
methods of, 239–242
Open Directory services, 192–193
overview of, 219
using full name/account name for, 225
WebDAV encrypting traffic for, 338
authentication, troubleshooting
Calendar service, 598
Contacts service, 611
Messages service, 624
using Password Server log for, 671–675
Wiki service, 584
authorization
describing, 220–222
as file-sharing challenge, 337
overview of, 219
simulating chat between two Macs, 630
verifying access to service, 271–273
automated installation, System Image Utility, 427
automatic address lookup, Calendar service, 595
automatic push, delivering profiles, 298
automatically configured DNS, 60
availability
hardware considerations for, 7
troubleshooting file-sharing service, 355

B
backslash character (\), command line, 647–648
backup
configuring iOS device iCloud, 53–54
creating backup of your, 174
of network and local home folders, 351
Time Machine. See Time Machine backup
Time Machine network. See Time Machine network backup
backup, OS X Server
concepts, 173–174
creating diversity, 174–175
inspecting Time Machine files, 181–186
overview of, 173
and restore Open Directory, 211–217
with Time Machine, 175–181
viewing in Logs pane, 186–187
behavior, unexpected profile, 310
blacklists, email, 561–562, 565
Bless NetBoot Image Folder, System Image Utility, 427
blogs
adding to wiki, 591
viewing as anonymous user, 592
wikis vs., 583
books, distributing with Profile Manager, 292–293
boot, NetInstall, 433
Boot Service Discovery Protocol (BSDP), NetInstall, 425

BootP (Bootstrap Protocol) network protocol, DHCP, 505
bootpd messages, NetInstall, 433
bound server
  access to services, 199
  to another OD service, 206–208
  using another Open Directory server, 198–199
broadcast request, DHCP, 502
Browse, accessing share points, 380
buddy lists, Messages service, 629

C

cache, flushing DNS, 65, 77, 211
Caching, Bytes Served graph, 163
Caching service
  automatically on local network, 10
  configuring and maintaining, 455–459
  describing, 451–454
  graph of data transfer stats in, 163
  list of content supported by, 451–452
  network scenarios for, 452–453
  Software Update vs., 459–461
  troubleshooting, 461–464
CalDAV (Calendar Server Extensions for WebDAV) calendaring protocol, 594
Calendar service
  configuring and starting, 598–602
  configuring calendar for OS X, 604–605
  describing data locations, 593
  replying to invitation, 606–607
  sending invitation, 605–606
  troubleshooting, 598
  using, 594–597, 602–603
  for wikis, 584
CardDAV protocol, Contacts services
  defined, 614–616
  as extension to WebDAV, 610
  managing preferences, 301, 305
  using, 612, 614–616
CAs (certificate authorities)
  certificates signed by, 114
  configuring SSL certificate, 118
  getting trusted certificate from, 121–123
  importing signed certificate from, 124–125
  intermediate, 114
  Open Directory. See Open Directory certificate authority (OD CA)
  root CA, 114
  trusted, 115
cascade of servers, Software Update, 467
cat command, 652, 670–671
cd command, 647, 672
Certificate Assistant, troubleshooting SSL, 142
Certificate pane, Server app, 216–217
certificate signing request (CSR). See CSR (certificate signing request)
certificates. See also trusted certificates
  following chain of, 133–138
  SSL. See SSL (Secure Sockets Layer) certificates
Certificates pane, Server app, 132–133
chain of certificates, hierarchical, 114–115
challenges, file sharing, 336–337
Change Host Name Assistant
  automatically creates a new SSL certificate, 13
  automatically creates new self-signed certificate, 118
  configuring DNS service in OS X Server, 63–64
  configuring initial install of Server app, 39–41
  specifying DNS service with, 14–15
Change Password, 267–268
characters
  filename wildcard, 654–655
  full names vs. account name, 224–225
  special. See special characters
chats
  archiving/logging in Messages, 622
  managing in Messages, 619–620
  simulating between two Macs, 629–630
  viewing archive, 635–636
child files, 392
child folders, 391, 395
ClamAV virus-scanning, email, 561
clean installs, 8–9
CLI. See command line
Client Addresses field, VPN, 488
client computer
  certificate trust, 144, 152–156
  copying VPN profile to your, 494–495
  software updates, 466
  Time Machine destination, 477–479
  troubleshooting Software Update, 468
  troubleshooting with NetInstall, 423
client computer, configuring
  administrator account, 46–48
  Computer Name, 48
  DNS records, 50–51
  Local Admin account, 45–46
  networking, 48–50
  prerequisites, 43–44
  Setup Assistant, 44–45
  updating software, 52–53
client computer, configuring services
  binding to Open Directory, 208–209
  Calendar, 604
  Contacts to access CardDAV, 614
  DHCP, 516–519
  Messages, 627–628
client iOS devices
  configuring, 53–56
  configuring to trust default self-signed certificate, 144
  Contacts app for. See Contacts app
Clients pane, Server app, 509–510
cloud-based storage, 174–175
CNAME (alias) record, 67, 70, 71
comma-separated value (CSV) file, Profile Manager, 297
command-dragging files, vs. dragging, 367
command line
  accessing, 640–641
  administration, 661–665
  basics, 639–640
  command-line prompts, 641–642
  command strings, 643–644
  file manipulation. See files, managing at command line
  Help for, 680
  learning about commands, 644–645
  remote access via SSH using. See SSH (Secure Shell), remote access via
  serveradmin command, 675–680
  simple example of, 644
  tips and tricks, 665–667
  turning on remote access. See SSH (Secure Shell), remote access via
  viewing contents of personal chats, 623
  viewing Messages service archive, 635–636
command-line navigation
  cd command, 647
  command manual shortcuts, 644
  concepts, 645–646
  ls command, 646–647
  to other volumes, 651
  overview of, 645
  pwd command, 646
  special characters, 647–649
  tab completion, 649–650
  viewing invisible items, 650–651
command strings, 642–644
complex permissions, ACE, 390–391
computer name
  changing, 13–15
  setting before OS X Server install, 28–29
  setting for client computer, 48
  use of, 11
  viewing in Overview pane, Server app, 87–88
computer sleep setting, 7
concurrent access, troubleshooting file-sharing, 355
Config folder, Calendar, 593
configuration files, web services, 522–523

configuration log, Open Directory, 209
configuration profile(s)
- client updates, 466
- customized NetInstall image, 438–439, 442
- defined, 278–279
- Mail settings, 569–572, 573–577
- Messages app, 621
- Profile Manager, 287–288
- System Image Utility, 427
- trusting certificates, 141–142
- updating with web clip for wiki, 588
- VPN service, 487, 490, 494–496

Configure Network Users and Groups pane, restoring Open Directory, 215–216
Confirm Settings pane, Open Directory, 147
Connect to Server, 99
Connected Users graph, File Sharing, 163
Connected Users pane, File Sharing, 353–354
Connected Users tab, File Sharing, 368
connectivity
- Calendar service, 598
- confirming screen sharing, 104
- copying new contents to website folder, 538
- DHCP service, 511, 516–518
- File Sharing service, 264–265, 368
- FTP service, 358
- NetInstall service, 447, 449–450
- Software Update service, 467
- troubleshooting directory services, 211
- troubleshooting Messages service, 624
- VPN, 484, 496–497
- Wiki service, 584

Console app
- inspecting Caching service logs, 463
- inspecting import logs, 262
- inspecting logs in, 20, 163
- monitoring Directory Services login, 211

Contacts app
- allow users to search directory using, 611–612
- configuring contacts on iOS device, 615
- configuring to access Contacts service, 612–613
- confirm directory searches, 616–617

Contacts service
- configuring, 611–612
- configuring Contacts app to contact, 612–613, 615
- confirming directory searches, 616–617
- creating new contact, 615
- overview of, 609–610
- setting up contacts to access CardDAV on client computer, 614
- troubleshooting, 610–611

content, customizing default website, 533–539
continuous backup, 174
Control-C, 666
Coordinated Universal Time (UTC) standard, 186
copying items, at command line, 657
cp command, 657
Create Image, System Image Utility, 427
Create Users and Groups, Calendar service, 595
Create Your Computer Account screen, 24
credentials
- authenticating user account, 219
- configuring Profile Manager for VPP, 288, 292
- confirming access to shared folder, 365
- verifying File Sharing for imported users, 264–265

crypt password, Open Directory authentication, 239
CSR (certificate signing request)
- configuring SSL certificates, 118
- getting a trusted certificate, 121–123
- importing signed certificate, 125
- renewing certificate signed by widely trusted CA, 131
- using certificate signed by widely trusted CA, 115–116

CSV (comma-separated value) file, Profile Manager, 297
cursors, moving, 666
Custom Access, Access pane, 93, 110–112
customizing
- certificates, 132–133
- content of default websites, 533–539
- NetInstall image, 435–442
- System Image Utility, 427

D

data
- disk space requirements, 6
- partitioning, 8

data repository
- location of Calendar, 593
- location of Contacts service, 610

Debug.log, Caching service, 463
decryption, PKI keys, 113–114
Default Locales, Open Directory, 197
Default Network Access, Access pane, 92, 106–109, 112
default self-signed certificates, 118–119, 143–144
default share points, 346
Default User Access, Access pane, 92, 106–109, 112
default websites
- changing folder used by, 533–535
- changing folder used by secure, 535–536
- confirming use of new content, 539
- copying new contents to new folder, 537–539
- exploring, 531–532
- restricting access to, 547–549
- sharing folder via File Sharing, 536–537
- stop sharing via File Sharing, 539

delegate, Calendar service, 596–597, 600–602
deleting items, at command line, 659
delimited text file, importing users from, 258–260
delivering profiles, 298–299
Delivery tab, Alerts pane, 166–168
demilitarized zone (DMZ), web hosting, 522
Deny entries, ACLs, 386
Deny rule
- ACEs, 385–386
- sorting ACLs canonically, 393

DEP (Device Enrollment Program), Profile Manager, 283–285, 288–291, 293
descendants, applying ACL inheritance, 392
Description field, customizing NetInstall image, 439–440
Details disclosure triangle
- configuring client computer to trust certificate, 154
- following certificate chain, 135

device accounts
- preferences, 304–307
- settings, 296

device group accounts
- managing, 297
- preferences, 304–307
- settings, 296

device management
- administering Profile Manager, 277–278
- clean up, 293–294
- configuring Profile Manager, 278–285
- connect Profile Manager with DEP account, 288–291
- connect Profile Manager with VPP account, 291–293
- DHCP leases, 504
- overview of, 277
- turning on Profile Manager, 285–286

DHCP (Dynamic Host Configuration Protocol)
- clean up, 519–520

configuring, 514–519
configuring with Server app, 505–510
DHCP networks and, 502–503
DNS lookups, 58
how it works, 502
leases, 503–504
manually assigning IPv4 vs. using, 11
NetInstall client startup process, 425–426
overview of, 501
serving multiple subnets, 505
as standalone service, 501
static and dynamic address assignments, 504–505
troubleshooting, 511–513
DHCP REQUEST, DHCP logs, 512–513, 519
Diagnostic information, Kerberos tickets, 246–247
Diagnostics & Usage screen, local admin account, 24
digital identity
definition of, 114
getting trusted certificates from, 121–123
proving using signed SSL certificates, 117
diradmin, 195
directory
cd command for changing, 647
removing at command line, 659–660
searches in Contacts, 616–617
use of term in this book, 644
Directory Administrator pane, Open Directory, 146
directory services
Calendar service integration with, 595
concept of, 191–192
Open Directory. See Open Directory services
troubleshooting, 209–211
Directory Utility
binding options, 199, 208–209
troubleshooting directory services, 211
Disconnect, File Sharing users, 368
DISCOVER, DHCP logs, 512–513, 519
disk images
creating NetInstall images from, 428
NetRestore and, 430–431
Time Machine network backups, 473–474
disk space
hardware considerations, 6
monitoring, 170–171
multiple partitions on single disk and, 9
requirements for OS X Server, 27
requirements for OS X Server install, 4
troubleshooting NetInstall, 433
troubleshooting Software Update, 468
Disk Utility
deploying disk image from file server, 431
partitioning disks, 8
Time Machine destination and, 178–180
Diskless option, NetInstall shadow files, 432
disks
backup to, 174
formatting/partitioning, 7–10
listed in Storage pane, Server app, 89–90
Time Machine destination as external, 178–179
DMZ (demilitarized zone), web hosting, 522
DNS (Domain Name Service)
access restrictions for, 76–81
Caching service configuration, 458–459
changing computer name/local hostname, 14–15
client iOS device configuration, 56
confirming DNS records for Open Directory, 199
creating new website, 524, 540–541
DHCP configuration, 515–516
host name and, 12–13
hosting requirements, 59–62
initial install of Server app, 38–42
installing OS X Server, 48–52
internal and external, 61–62
issues caused by bad/nonexistent, 58–59
local hostname and, 12
Mail configuration, 558
Open Directory configuration, 145–147
OS X Server configuration, 62–64
overview of, 57
preparing for OS X Server install, 13, 29, 31
server configuration, 11
troubleshooting Calendar, 598, 607
troubleshooting Contacts, 610
troubleshooting in OS X Server, 64–65
troubleshooting Kerberos, 249
troubleshooting Mail, 564
troubleshooting Messages, 624
understanding, 57–59
upgrading/migrating to OS X Server, 18
VPN configuration, 486, 489, 493–494
web hosting requirements, 522
DNS server, defined, 59
DNS zones and records, creating
adding nameserver for reverse zone, 74
collect DNS configuration data, 66–67
configuring DNS hosts, 69–76
configuring forwarding servers, 67–68
confirming new DNS records, 74–76
inspecting limited default zones, 68–69
inspecting new zones/records, 70–72
new records, 69–70, 72–73
overview of, 65–66
removing redundant zone, 73–74
Dock
installing OS X Server in, 16
opening Server app in, 37
dollar sign ($), command-line prompt, 641
domain names
managing websites, 525–526
turning on web services, 531
domain(s)
adding email, 567
defining for DNS service, 62–63
Mail service hosting email for multiple, 562–563
removing Open Directory, 213
restoring Open Directory, 212–217
DORA acronym, DHCP logs, 512–513
double period (..), command line, 648
Dovecot, Mail service using, 555
Down Arrow keys, command-line tips, 666
downloading
OS X Server, 15–16
student materials, 33–35
trust profile, 436–437
drag and drop, Finder, 648, 665
dragging, copying file by, 367
Duplicate Service, 541–542
dynamic address assignment, DHCP, 504–505, 511
Dynamic Host Configuration Protocol. See DHCP (Dynamic Host Configuration Protocol)

E

Edit Access to Services
inspecting, 270–271
manually managing, 237–238
Messages service, 630–631
using Server app, 236–237
Edit Forwarding Servers, Server app, 67–68
Edit Lookup Clients, 77
Edit Password Policy, 269
Edit Permissions
DNS permissions, 78, 80
Messages service users, 630
Storage pane of Server app, 382–383

Edit Personal Folder Access button, iOS, 353
Edit Recipients button, email, 166–167
editing
  commands before submitting them, 666
  share points, 349–351
  subnet to configure DHCP, 506–509
  user accounts, 253–255
  wikis, 589–592
EFI (Extensible Firmware Interface)
  NetInstall, 447
  remote locks, 300
El Capitan
  checking whether computer can run, 4–5
  configuring OS X with Setup Assistant, 21–24
  installing Server app on another computer, 158
  sending alerts to any Mac, 160
  support for Gigabit Ethernet, 6
  upgrading/migrating to OS X Server, 17–18
email
  Calendar invitation settings, 599–600
  for Calendar invitations, 595
  configuring alert recipients, 166–167
  configuring alerts, 158–159
  delivering profiles, 298
  Mail service. See Mail service
encryption
  full-disk, not recommended, 10
  Messages federation, 623
  as option for SMB connections, 358
  OS X Server install on volume, 8
  PKI keys, 113–114
  VPN. See VPNs (virtual private networks)
  WebDAV, 338
Energy Saver system, for availability, 7
enrollment, troubleshooting device, 310
Enterprise apps, managing, 297–298
Erase All Content and Settings, iOS device, 54
Erase button, Time Machine destination, 178–179
Error log, monitoring web services, 528, 549–551
Ethernet
  Caching service using wired, 456
  setting network interfaces, 32
events, Calendar, 595, 605–606
Everybody
  accessing website files, 523
  troubleshooting web services, 529
Everyone Else, Others permissions displayed as, 381
exclusions, Time Machine destination, 478–479
expiration date, certificates, 113, 142
exported formatted file
  importing users from, 260–261
  updating passwords for imported users, 261–262
Extensible Firmware Interface (EFI)
  NetInstall, 447
  remote locks, 300
Extensible Markup Language (XML), profiles in, 298
external DNS server, 60–62
external images sources, NetInstall, 429
extras, command string, 643

F

FaceTime camera, Messages service, 619
fallback certificate, Open Directory domain, 214
federation, Messages service
  configuring, 623
  restricting, 633
feedback, OS X Server, 102
file access
  features common to POSIX and ACLs, 395–398
  overview of, 377
  POSIX vs. ACL. See POSIX permissions vs. ACLs
  rules of precedence for POSIX and ACLs, 398–399
  to share points and folders, 377–383
  using command line vs. Finder, 639
  via iOS, 370–375
file access, configuring access control
  clean up, 417–418
  comparing views of permissions, 413–417
  configure group and shared folder, 401–404
  confirming permissions, 404–410
  overview of, 400–401
  updating permissions, 411–413
file command, 654
File Sharing pane, Server app
  Access segment of, 345
  comparing views of permissions, 413–415, 418
  configuring access to share points, 378–382
  configuring Time Machine, 480
  creating new shared folder, 364–365
  displayed on server vs. remote Mac, 346
  inspecting NetInstall shared folders, 445–446
  new shared folder location, 345
  propagating permissions, 394–395
  updating ACL inheritance rules for folders, 393
File Sharing service
  accessing files via iOS, 370–375
  challenges, 336–337
  connection for imported users, 264–265
  creating share points, 345–354
  disconnecting connected users, 368
  file-sharing protocols, 337–341
  FTP service, 355–358
  managing access to, 271–273
  overview of, 335
  password, 267–268, 672–675
  planning, 341–344
  shared folders, confirming access to, 365–366
  shared folders, creating, 364–365
  shared folders, creating location for, 363–364
  shared folders, discontinuing website, 539
  shared folders, group, 366
  shared folders, moving files to, 367–368
  shared folders, website, 536–537
  stats in OS X Server, 163
  Time Machine backup destination, 473
  troubleshooting, 355, 375–376
  turning on, 238
file system
  commands for navigating, 646–647
  folders as containers for, 644
  pathnames, 646
  working directory, 641–642
file system ACLs
  access levels within share points using, 377
  POSIX permission similarities to, 395–398
  POSIX permissions vs. See POSIX permissions vs. ACLs
  rules of precedence, 398–399
File Transfer Protocol. See FTP (File Transfer Protocol)
File Vault full-disk encryption, 10
files
  modifying at command line, 656–661
  moving to shared folders, 367–368
  sending through Messages service, 619
files, managing at command line
  file examination commands, 652–654
  modifying files and folders, 656–661
  overview of, 652
  recursive commands, 655–656
  wildcard characters, 655

filters
  alert, 160
  configuring, 565
  in keywords and notes, 225
  spam, 562
  in System Image Utility, 427
  testing spam, 577–578
  troubleshooting NetInstall server, 433
  when real emails are marked as spam, 564
find command, files, 654
Finder
  browsing via computer name, 12–13
  changing startup volume name, 27–28
  confirming access to shared folder, 365–366
  confirming custom access rule, 111–112
  confirming modified default access rules, 109
  confirming password, 267
  connecting to File Sharing, 264
  connecting to FTP service in, 358
  copying new contents to website folder, 537–539
  copying VPN profile to client computer, 494–495
  downloading student materials, 33–35
  examining Time Machine backup files, 181–186
  with File Sharing started/stopped, 361–362
  initial install of Server app, 35
  inspecting customized NetInstall image, 441–442
  moving file to shared folder, 367
  verifying access to service, 271–273
  viewing/disconnecting users, 368
fingerprint. See public key fingerprint, SSH
firewall configuration, 433, 484
folder badges, 336–337
folders. See also home folders; shared folders
  ACL inheritance for, 391
  configuring permissions in Server app Storage pane, 382–383
  creating with mkdir, 656–657
  as file system containers in this book, 644
  ls command listing contents of current, 646–647
  modifying at command line, 656–661
  modifying default website, 533–539
formatting disks, 7–10
forwarding servers, DNS, 58–59, 66–68
FQDN (fully qualified domain name)
  host name as, 12
  troubleshooting web services, 529
  websites, 525
FTP (File Transfer Protocol)
  enabling file sharing, 337–338
  providing service, 355–358
  Secure FTP, 341
  WebDAV as good alternative for, 341
full-disk encryption, not recommended for OS X Server, 10
full file-level copy backup, 174
full image backup, 173
full name, user account, 224
fully qualified domain name. See FQDN (fully qualified domain name)

G

Get Info command, Finder, 384
GIDs (group IDs), POSIX and ACLs, 395–396
Gigabit Ethernet, network requirements, 6
global password policies, Open Directory, 239–242
globally unique ID (GUID), 385, 395–397
globs (wildcard characters), 654–655
Google Talk, Messages federation, 623
grep command, inspecting AFP logs, 676
greylists, email, 562, 565
group attribute, user accounts, 227
group IDs (GIDs), POSIX and ACLs, 395–396
group(s)
  access control for, 401–404
  adding group to, 255
  assigning groups to, 236
  assigning user to, 234–235
  assigning users to, 232–233
  behavior of nested, 397–398
  of computers, configuring with NetInstall, 422
  configuring, 401–402
  configuring in Server app, 342
  creating, 231–232, 251
  creating ACE for, 396
  creating settings for accounts, 296
  creating wiki for, 586–587
  giving shared folder to, 366
  importing, 263–264
  inspecting permissions, 415–417
  persistent chats for, 619
  POSIX permission, 384
  preferences for, 296–297, 301–304
  updating permissions, 411–413
Groups shared folder, 353, 370
guest access, share points, 381
GUID (globally unique ID), 385, 395–397
GUID Partition Table, 8

H

hardware requirements
  availability, 7
  defining minimum, 4
  disks, 6
  NetInstall, 423
  network, 6
  RAM, 6–7
  upgrading/migrating to OS X Server, 17–18
  verifying system, 4–5
hashed passwords, Open Directory, 239
Help Center window, Server app, 101
Help, command line, 680
helper address (relay agent), DHCP, 505
hidden items, viewing at command line, 650–651
home directories, shared folders available for, 351–352
home folders
  ~ character in pathname describing, 649
  creating user accounts, 249–250
  tab completion from, 649
  user account name used for, 224
host command, 74–76, 77
host domain, Messages service, 620
host name
  binding server to another OD service, 207
  creating websites, 540
  DNS records, creating new, 70, 72
  DNS service, configuring, 51–52, 62–64
  initial install of Server app, 38–41
  inspecting limited default zones, 68–69
  OS X Server, configuring as OD replica, 204–205
  OS X Server requirements, 59–62
  for self-signed certificates, 125
  understanding, 12–13
  viewing change alert for, 42
  viewing in Overview pane of Server app, 87–88
  VPN service, configuring, 486, 492
  VPN service, saving configuration profile with, 490
hosting
  evaluating OS X Server requirements, 59–62
  websites. See websites, hosting
hosts, configuring DNS
  adding nameserver for reverse zone, 74
  confirming new DNS records, 74–76
  creating new record, 69–70, 72–73
  inspecting new zones/records, 70–72
  removing redundant zone, 73–74

HTTP (Hypertext Transfer Protocol)
  automatic redirect settings, 532
  Calendar service, 594
  Contacts service, 610
  as default website, 531–532
  NetInstall client startup process, 425
  NetInstall image protocol, 443–444
  replying to Calendar invitation, 607
  setting up redirects to SSL website, 526
httpd process, 521
HTTPS (Hypertext Transfer Protocol Secure)
  automatic redirect settings, 532
  Calendar service, 594
  Contacts service, 610
  as default website, 531–532
  replying to Calendar invitation, 607

I

iChat. See Messages service
iCloud backup, production iOS devices, 53–54
identity. See also digital identity
  Open Directory services and, 192–193
  Ticket Viewer tickets and, 245–246
  troubleshooting in Kerberos, 249
image ID (or index), System Image Utility, 426
Image Name and Network Disk fields, NetInstall image, 439
image source, System Image Utility, 427
images
  creating with System Image Utility. See System Image Utility
  NetInstall client startup process, 425–426
  preparing for NetInstall service, 434
  specifying default NetInstall, 444–445
  types of NetInstall, 424–425
IMAP (Internet Message Access Protocol), 557, 579
Import Users and Groups, Calendar service, 595
importing
  lists of devices into Profile Manager, 297
  signed certificates, 124–125
importing users
  Calendar service, 595
  from delimited text file, 258–260
  from exported formatted file, 260–262
  importing group, 263–264
  importing list of, 228–230
  overview of, 257–258
  reviewing import logs, 262
  troubleshooting, 248
  verifying File Sharing connection for, 264–265
Incoming Mail Server Info, configuration profile, 570–572
incremental backups, 174
index files
  aliases, 526
  turning on web services, 531
index (image ID), System Image Utility, 426
INFORM packet, NetInstall service logs, 449
inheritance
  defining ACL, 391–393
  rules for ACEs, 385
  updating ACL rules for, 393
Install OS X El Capitan, creating NetInstall images, 428
installation, OS X Server
  configuring client computer. See client computer
  configuring client iOS device, 53–56
  configuring OS X. See OS X, configuring before OS X Server install
  initial install, 35–43
  overview of, 16–17
  requirements, 4–7
  troubleshooting, 19–20
  updates, 19
  upgrading/migrating to OS X Server, 17–18
installation, preparing for OS X Server
  changing names/addresses, 13–15
  configuring/name/network, 10–13
  downloading OS X Server, 15–16
  overview of, 7–10
intermediate CA
  binding server to another OD server, 207
  confirming restoration of OD, 216
  defined, 114–115
  inspect OD, 150–151
  troubleshooting SSL certificates, 142
  trusted, 115
  using SSL certificate signed by OD CA, 116
internal DNS server, 60–62
internal volume, as Time Machine destination, 179–180
Internet Accounts preferences, Messages app, 621
Internet Message Access Protocol (IMAP), 557, 579
invitations, Calendar
  configuring email for, 595
  inspecting email settings, 599–600
  replying to, 606–607
  sending, 605–606
iOS devices. See also client iOS devices
  accessing files via, 370–375
  accessing wiki files, 584
  Calendar for. See Calendar service
  configuring Contacts app to access Contacts service, 612–613
  configuring trust, 141–142
  confirming Contacts on multiple, 615–616
  enrolling to send/receive mail, 574
  personal folders for, 352–353
  replying to Mail message, 575–576
  troubleshooting Caching service, 462
  using share points with WebDAV, 338
iOS Log, 376
IPv4 (Internet Protocol version 4) address
  Caching service configuration, 458
  Caching service registration of, 454
  client computer configuration, 49–50
  creating new websites, 541–545
  DHCP configuration, 515–516
  DHCP, editing subnet for, 507
  DHCP networks and, 503
  DHCP server leases and, 503–504
  DHCP static/dynamic address assignments, 504–505
  DNS configuration in OS X Server, 63
  DNS host name correlating to, 59
  DNS lookups and, 57
  DNS records, confirming client computer, 51–52
  managing websites, 525
  NetInstall client startup process, 425–426
  Open Directory configuration, 146
  prior to DNS service setup, 66
  removing additional, 546–547
  services configuration, 10–11
  setting network interfaces, 30–31
  troubleshooting Caching service, 462
  troubleshooting DCHP, 511–513
  troubleshooting NetInstall, 433
  VPN configuration, 488, 493
iSight camera, Messages service, 619
iTunes, troubleshooting Caching service, 462

J

Jabber account, configuring Messages app, 621
journaled formats, 8
junk mail
  filtering, 562
  filtering options, 565
  messages flagged as, 578

K

KDC (Key Distribution Center)
  global password policies, 242–247

in Kerberos, 243–244
Open Directory authentication, 239
Kerberized services, 243–244, 245
Kerberos
basics, 243–245
KDC. See KDC (Key Distribution Center)
Open Directory service leveraging, 192
setting global password policies, 240
single sign-on and, 242
tickets, 245–247
troubleshooting, 249
keyboard layout, 22
Keychain Access
archive certificate, 130
configuring trust, 139
confirming removal of Open Directory domain, 214–215
confirming restoration of Open Directory, 216
inspecting certificates, 127–129
inspecting Open Directory certificates, 149–152
viewing default certificate, 118
viewing trusted root CAs, 115
Keynote
confirming change in iOS device, 374–375
editing file on server, 373–374
free on App Store for iOS 9 devices, 370
getting/installing for iOS, 371–372
signing into WebDAV service on iOS with, 339
keys, PKI public and private, 113–114
keywords, user account, 225
kiosks, using NetInstall, 422

L

L2TP (Layer 2 Tunneling Protocol), VPN service, 484, 485, 488
ladmin command (Administrator Name)
backing up OS X server, 184
Calendar service, 599, 602
command-line interface, 667, 680
configuring access control, 401, 416
configuring alerts, 166–167
configuring forwarding servers, 67
configuring OS X, 24–25, 44, 47
confirming custom access rule, 112
confirming screen sharing connection, 104
Contacts service, 611
creating new folder for home folders, 250
creating websites, 543
examining default SSL certificate, 143
File Sharing service, 359, 364
hosting websites, 530
Mail service, 565, 569, 573
Messages service, 624, 626
NetInstall service, 434, 436, 440
Profile Manager, 285, 311–312, 315, 321
remote access via SSH, 668, 669–670
removing Open Directory domain, 214
Time Machine backup, 475
turning for file-sharing access, 103
VPN service, 492, 495
wiki service, 585–586
ladminpw command (Administrator Password)
access control, 401
alerts, 166
Calendar service, 599, 602
command-line interface, 667, 672, 676–678
configuring OS X, 24–26, 44–45, 47
Contacts service, 611
creating new folder for home folders, 250
creating websites, 543
custom access rule, 112
examining default SSL certificate, 143
File Sharing service, 359
forwarding servers, 67
hosting websites, 530
Mail service, 565, 569, 573
managing with Profile Manager, 285, 311–312, 315, 318, 321
Messages service, 624, 626, 635
NetInstall service, 434, 436
opening Server app, 37
remote access via SSH, 668, 670
removing Open Directory domain, 213–214
screen sharing connection, 104
Time Machine backup, 475
turning for file-sharing access, 103
VPN service, 492, 495
wiki service, 585–586
launchpad, opening Server app, 37
layering management techniques, 307–309
layering profiles, 307–309
LDAP (Lightweight Directory Access Protocol)
Calendar service, 595
OpenLDAP, 192, 194
setting up Contacts for searches using, 609
LDAPv3 node (local network directory), 222
leases, DHCP, 503–504, 509
less command, file management, 652
Lesson & Update Files tab, student materials, 35
libraries, configuring with NetInstall, 422
Lightweight Directory Access Protocol (LDAP), 595, 609
List View button, Storage pane, 363
local accounts
creating user account, 251
defined, 194
Open Directory authentication, 239
Local Admin account. See also ladmin command (Administrator Name)
configuring existing OS X system, 24–26
configuring OS X before OS X Server install, 23–24
local backups, 174–175
local directory node, 222
local group, 231–232
local home folders, backing up, 351
local hostname, 12, 13–15
local network accounts
defined, 194
email address for, 567–568
global password policies, 242
local network directory (LDAPv3 node), 222
local network users and groups
assigning groups to group, 236
assigning groups to user, 234–235
assigning users to group, 232–233
creating/administering, 222
creating group, 231–232
using Contacts app to search directory for, 617
local user accounts
administrator, 230–231
creating with Server app, 223–228
global password policies, 242
using keywords and notes, 225
local users and groups
assigning groups to group, 236
assigning groups to user, 234–235
assigning users to group, 232–233
creating/administering, 222
locales, Open Directory, 196–198
Locales pane, Open Directory, 197
location, Calendar service, 596, 600–601, 605
locking device, remotely, 299–301
logical disks, 8
login credentials, configuring trust, 139, 155
Login Options, Users & Groups preferences, 207, 211
login window, authentication/authorization, 220–222
logout command, 670–671
logs
Apple Filing Protocol, 375, 676–680
backup, 186–187
Caching service, 462–463

Calendar, 593
DHCP service, 519
file sharing, 344
import, 262
increasing detail for Open Directory, 211
inspecting, 20
Messages service, 622–623, 633–634
NetInstall service, 449
OS X Server, 161–163
Password Server, 671–675
removing Open Directory domain, 213
troubleshooting DHCP, 511–513
troubleshooting File Sharing, 375–376
troubleshooting imported users, 248
troubleshooting in Profile Manager, 310
troubleshooting Mail, 564
troubleshooting NetInstall, 433
troubleshooting Software Update service, 468
troubleshooting VPNs, 490–491
troubleshooting with Open Directory log files, 209–210
VPN service, 490–491, 498
web services access, 528, 549–551
Logs pane, Server app, 20, 157
long name (name), as user account full name, 224
lookups, DNS, 57–58
ls command
inspecting public key fingerprint, 668
listing folder contents, 646–647
viewing hidden items, 650–651

M

Mac App Store, 15, 19, 36
MAC (Media Access Control) address, 504–505, 510
Mac OS X Extended (Case-Sensitive, Journaled)
applying ACLs only on, 385
installing OS X Server on volume, 8
machine (A) record, 67, 71
Mail eXchange (MX) server, Mail services, 556
mail exchanger record. See MX (mail exchanger) record
Mail service
access permissions/authentication, 558–559
compatibility with Contacts, 609
configuration profile for, 569–572
defining, 556–557
DNS for, 558
examine logs, 578–579
hosting, 555–556
mail domains, 562–563
relaying outgoing mail, 559–560
sending and receiving mail, 573–577
setting mail quotas for users, 560–561
testing spam filter, 577–578
troubleshooting, 563–564
turning on, 564–569
virus scanning/blacklists/greylists/ junk filtering, 561–562
mainserver, downloading student materials, 33
maintenance
Caching service, 458–459
file-sharing service, 343
Make Inherited Entries Explicit, inherited ACEs, 393
man command, 644–645
man-in-the-middle attacks, SSH preventing, 667
man page, serveradmin command on, 675–680
Manage menu, Server app, 99
manual, for command shortcuts, 644
Master Boot Record, 8
masters. See Open Directory master
mdfind command, Spotlight search, 654
MDM (mobile device management), Profile Manager
administering, 278
device enrollment, 283–285, 288–290
enabling, 280
Media Access Control (MAC) address, 504–505, 510
media, types of backup, 174
member server
access to services, 199
configuring Open Directory as, 192
Server app allowing access to services from, 236–237
using another Open Directory server, 198–199
Memory Pressure graph, stats in OS X Server, 163–164
Memory Usage graph, stats in OS X Server, 163–164
Messages app, configuring, 627–629
Messages service
compatibility with Contacts, 609
configuring Messages app on client computer, 627–628
configuring Messages app on server, 628–629
configuring users, 620–621
federation, 623
logs, 622–623
managing, 619–620
network ports, 621–622
restricting federation users, 633
restricting users, 630–632
sending messages between two Macs, 629–630
setting up, 624–626
troubleshooting, 624
using, 626–627
viewing chat logs, 633–636
migration, to OS X Server, 17–18
mkdir command, 656–661
mobile device management. See MDM (mobile device management), Profile Manager
monitoring
DHCP service, 509
NetInstall service, 448–450
ongoing, 170–172
server. See status and notifications
web services, 549–551
more command, 635
mounted volumes, NetInstall images from, 429
moving items, at command line, 658–659
multi-volume NetRestore, 427
multiple profiles, 307–309
mv command, 658
MX (Mail eXchange) server, Mail services, 556
MX record
configuring DNS for Mail by setting up, 558
confirming new DNS records, 75–76
inspecting new zones/records, 71
prior to DNS service setup, 67

N

N key, startup from NetInstall image, 447
names
blog, 591
changing, 13–15
changing startup volume, 27
command, 643–645
Computer Name. See Computer Name
configuring, 10–13
Kerberos realm, 243
for multiple partitions on single disk, 9
troubleshooting Server app, 102
nameserver. See NS record (nameserver)
NAT (network address translation)
Caching service, 452–453
configuring AirPort in Server app, 93, 95
navigation. See command-line navigation
.nbi file, Mac disk image, 430
nested groups, 397–398
nested replicas, 195
NetBIOS, in Windows, 338
NetBoot boot image, 422, 424, 427

NetBootClients0 shared folder, AFP, 340, 445
NetBootSP0 shared folder, NFS, 445–446
NetInstall (Network Install) image
- client startup process, 425–426
- configuring protocol, 443–444
- overview of, 424
- startup from, 446–448
- working with, 428–430

NetInstall (Network Install) image, customizing
- Download Trust Profile, 436–437
- inspecting, 441–442
- NetInstall image, 437–440
- overview of, 435–436
- saving workflow, 440–441
- with System Image Utility configurations, 427

NetInstall service
- additional share points in, 346
- client startup process, 425–426
- creating customized NetInstall image, 435–442
- creating images with System Image utility, 426–431
- hardware requirements, 424
- image types, 424–425
- managing computers with, 422–424
- monitoring, 448–450
- NFS facilitating, 340
- overview of, 421–422
- preparing, 433–435
- shadow files, 431–432
- starting, 442–446
- startup from NetInstall image, 446–448
- troubleshooting, 433
- turning off, 450

NetRestore
- deploying OS X computers with, 422
- overview, 424–425
- System Image Utility custom configurations for, 427
- working with, 430–431

network address translation. See NAT (network address translation)
Network File System. See NFS (Network File System)
network home folders, 351, 352
Network Install. See NetInstall (Network Install) image
network interface
- client computer, 48–50
- configuring DHCP service, 505–506, 515
- hardware considerations, 6
- initial install of Server app, 40–41
- before OS X Server install, 22–23, 29–32
- overview of, 10–13

Network pane, 153
Network preferences
- configure server to use additional IPv4 address, 541–542
- configuring DHCP service, 502–503, 515
- troubleshooting directory services, 211

Network Time Protocol (NTP), Kerberos, 244, 249
Network Traffic graph, 163, 164–165
Network Utility
- checking external DNS server for AD, 61–62
- configuring Open Directory, 145–147
- confirming DNS records for client computer, 51–52
- confirming new DNS records, 74–75
- inability to test access to server's DNS, 77
- troubleshooting directory services, 211
- troubleshooting DNS, 65

networks
- changing address, 14–15
- default access rules for, 92
- DHCP services. See DHCP (Dynamic Host Configuration Protocol)
- failed startup NetInstall process and, 447
- file service authentication, 221
- Time Machine services. See Time Machine network backup
- troubleshooting Software Update service, 467
- VPN services. See VPNs (virtual private networks)

NFS (Network File System)
- configuring NetInstall image, 443–444
- facilitating NetInstall, 340
- inspecting NetInstall shared folders, 445–446
- NetInstall client startup process, 425
- security issues, 339–340

notes, search/sort user accounts with, 225
Notification Center alerts, 169–170
NS record (nameserver)
- adding for reverse zones, 74
- inspecting limited default zones, 69
- inspecting new zones/records, 71–72

NTP (Network Time Protocol), Kerberos, 244, 249

O

obsolete updates, Software Update service, 466
OD CA. See Open Directory certificate authority (OD CA)
OFFER, DHCP logs, 512–513, 519
one-to-one devices, Profile Manager for
- enrollment with user portal, 323–332
- overview of, 320
- preparations for, 321–323
- unenrollment, 332

online resources
- app extensions, 353
- Apple Root Certificate Program, 115
- configuring Open Directory locales, 198
- Device Enrollment Program, 283
- NetBoot, NetInstall, and Netstore requirements, 422
- NetRestore volume workflow, 431
- new for iOS 9 compatible devices, 375–376
- System Image Utility, 426
- upgrading/migrating to OS X Server, 18
- Volume Purchase Program, 281
- zero-configuration networking, 12

Open Directory certificate authority (OD CA)
- binding server to another OD service, 207
- certificate signed by intermediate CA, 116
- configuring client computer to trust, 152–156
- configuring Open Directory, 145–147
- confirming removal of Open Directory domain, 215
- do not click Renew for, 131
- inspecting certificates, 147–152
- issuing new SSL certificate, 542
- restoring certificate configuration, 216–217
- troubleshooting SSL certificates, 142

Open Directory master
- access to services, 199
- automatic access control with, 237
- configuring Messages federation, 623
- configuring Open Directory as, 192
- configuring OS X Server as, 200–202
- configuring OS X Server as replica of, 204–206
- configuring server as, 199
- configuring server for Profile Manager, 286
- confirming available DNS records, 199
- describing, 194–195
- enabling Profile Manager, 280
- nesting replicas, 195
- Password Server log on, 671–675
- Profile Manager requiring, 199, 279
- promoting Open Directory replica to, 196

sharing information via, 193
transferring data to replica from, 195–196
Open Directory pane, Server app, 242
Open Directory replica
configuring Open Directory as, 192
configuring OS X Server as, 204–206
configuring server as, 199
confirming available DNS records, 199
creating additional locales, 197
describing, 195–196
Open Directory services
access to, 199
authentication, 239
backup and restore, 211–217
Calendar integration with, 595
component overview, 193
configuring server, 10
definition of, 192
directory service concepts, 191–192
Kerberos component of, 244
LDAP database, 239
locales, 196–198
logs, 209, 211
overview of, 191
standalone server role, 193
Time Machine archiving content of, 177
troubleshooting, 209–211
using another OD server, 198–199
viewing backup log, 186–187
Open Directory services, configuring
binding OS to, 208–209
binding server to another OD service with, 206–208
creating archive, 202–204
OS X Server as OD master, 200–202
OS X Server as OD replica, 204–206
overview of, 199
turning off/removing, 202
using Directory Utility remotely, 208
OpenLDAP (Lightweight Directory Access Protocol), 192, 194
operating system
creating NetBoot images with latest version, 429–430
separate partitions for segregating data, 8
Option key, startup from NetInstall image, 447
Organization Information pane, 146–147, 286
OS X, configuring before OS X Server install
changing startup volume name, 27–28
configuring existing system, 24–26
confirming computer qualifications, 26–27
downloading student materials, 33–35
establishing student number, 20
for existing system, 24–26
overview of, 19–20
requirements, 19–20
setting computer name, 28–29
setting network interfaces, 29–32
Setup Assistant, 21–24
updating software, 32–33
OS X Extended (Journaled), Time Machine, 179
OS X Mountain Lion, Shared Items folder for, 353
OS X Recovery, 10
OS X Server account, adding to iOS device, 372–373
OS X Server–hosted DNS, 61
OTA (over-the-air) device configuration, Profile Manager, 277
Others permission, 381
Outgoing Mail, 571–572
Overview pane, About this Mac, 4–5, 27
Overview pane, Server section of Server app, 87–88
ownership, POSIX, 384

P

packages, in System Image Utility, 427
parameter random-access memory (PRAM), NetInstall, 447
parameters (arguments), command string, 643
Partition Map Scheme, 8
Partition Map Type, 8
partitioning
overview of, 7–10
in System Image Utility, 427
for Time Machine destination, 179–180
passcode, client iOS device, 55
passphrase (shared secret), configuring VPN, 487, 492–493
Password Server database
Open Directory master (server), 195
Open Directory replica, 195
setting global password policies, 240
Password Server log
correct password, 674–675
examining, 673
overview of, 671–672
wrong password for File Sharing service, 672–673
Password Service Error log, Open Directory, 210
Password Service Server log, Open Directory, 210
password(s)
administrator. See ladminpw command (Administrator Password)
authentication/authorization, 220–222
clean up policies, 268–269
configuring Calendar for OS X, 604
configuring local admin account, 24
configuring messages on client computer, 627–628
configuring policies, 265–268
configuring VPN service, 487
confirming Contacts on multiple devices, 615–616
importing user accounts, 229–230
Local Admin account, 25
Open Directory authentication, 239
Open Directory storing/validating, 192
removing Open Directory domain, 213
replying to Calendar invitation, 606–607
replying to Mail message, 575
sending Mail to group, 574
setting global policies f, 240–242
troubleshooting Calendar service, 598
troubleshooting Contacts service, 611
updating for imported users, 261–262
verifying access to service, 272
VPN configuration profile for, 490
pathnames
command-line use of, 644
special characters in, 647–649
types of file system, 645
Peachpit account, downloading student materials, 35
performance
graphs, 163–165
improving NetInstall server, 427
installing multiple disks to increase server, 9
troubleshooting Caching service, 464
permissions. See also POSIX (Portable Operating System Interface) permissions
ACE and, 403–404
Calendar service, 595, 600
confirming, 404–410
Contacts service, 610
displaying file system, in command line, 639
DNS service, 78–81
Mail service, 558–559
Messages service, 620, 625
to personal chat archive, 623
to share points, 378–382
Time Machine, 474, 480
updating, 411–413
user account, 223–228
verifying access to services, 271
viewing, 91–93, 413–417
VPN service, 485
website, 525–526, 537
wiki, 586–587, 591

permissions dialog, Storage pane, 383
persistent chats, Messages service, 619
personal folders for iOS use, 352–353
pin placement on map,
  Calendar service, 595
PKI (public key infrastructure), 113–114
placeholders, 284–285
planned events, server upgrades as, 18
planning, file-sharing services, 341–344
plist, 466
Point to Point Tunneling Protocol
  (PPTP), 484, 485, 488
policies, password, 240–242, 265–268
POP (Post Office Protocol), email, 557
port numbers
  allowing remote access, 83
  hosting websites based on, 97
  Messages service, 621–622
  NetInstall client startup process, 425
  troubleshooting Calendar service, 598
  troubleshooting Contacts service, 610
  troubleshooting device enrollment, 310
  troubleshooting DNS in
    OS X server, 64
  troubleshooting Software Update, 467
  troubleshooting Wiki service, 584
  VPN service, 484, 487
  website management, 525–526, 540
portability, ACL, 394
portal websites, delivering profiles via, 298
POSIX permissions vs. ACLs
  ACL portability, 393
  configuring ACLs with Server App
    File Sharing pane, 386–387
  configuring ACLs with Server App
    Storage pane, 388–389
  configuring complex permissions for
    ACE, 390–391
  defining ACL inheritance, 391–393
  defining ACLs, 385–386
  how file system ACLs work, 386
  overview of, 383
  POSIX ownership/permissions,
    384–385
  propagating permissions, 393–394
  sorting ACLs canonically, 393
POSIX (Portable Operating System
  Interface) permissions
  for access levels within
    share points, 377
  comparing views of permissions,
    415–416, 418
  configuring access with Server app
    File Sharing pane, 378–383
  configuring complex permissions for
    ACE, 390–391
  confirming requested access, 404–410
  features common to ACLs and,
    395–398
  rules of precedence, 398–399
  umask variable in, 385
post-install scripts,
  System Image Utility, 427
Post Office Protocol (POP), email, 557
Postfix, for mail service, 555
PPTP (Point to Point Tunneling
  Protocol), 484, 485, 488
PRAM (parameter random-access
  memory), NetInstall, 447
precedence, POSIX and ACL rules of,
  398–399
preferences. See also System Preferences;
  Users & Groups preferences
  adding IPv4 address to server,
    541–542
  Contacts for multiple devices,
    615–616
  customizing command line, 665
  devices/device groups in Profile
    Manager, 304–307
  DHCP service, 502–503, 515
  Messages app, 621
  Time Machine, 180–181, 477–481
  troubleshooting directory services, 211
  users and groups in Profile Manager,
    301–304
primary DNS host name. See host name
primary zone, DNS, 59, 69
principal database, Kerberos, 243–244
private keys, PKI, 113–114
Processor Usage graph, 163–164
Profile Manager
  administering, 277–278
  clean up, 293–294
  configuring VPN service, 487
  connecting with DEP account to,
    288–291
  connecting with VPP account to,
    291–293
  creating configuration profile for
    Mail, 569–572
  installing apps across multiple
    computers, 422
  for one-to-one devices, 320–332
  overview of, 277
  for shared devices, 311–320
  troubleshooting, 310
  turning on, 285–288
  unenrollment from, 332
  web app, 278
Profile Manager, account management
  apps, 297–298
  delivering profiles, 298–299
  device group accounts, 297
  layering and multiple profiles,
    307–309
  levels of, 296
  overview of, 295
  preferences for devices/device groups,
    304–307
  preferences for users/groups, 296–297,
    301–304
  remotely locking/wiping device,
    299–301
Profile Manager, configuring
  Device Enrollment Program, 283–285
  enabling, 280–281
  preparations for, 279
  server, 10, 199
  terminology, 278–279
  Volume Purchase Program, 281–283
profiles
  delivering, 298–299
  device management, 278
  layering and multiple, 307–309
  troubleshooting, 310
  troubleshooting Software Update, 468
  troubleshooting viewing/installing, 310
prompt, command
  overview of, 641–642
  special characters in, 647–649
Propagate Permissions, Server app
  Storage pane, 382–383
protocols
  Calendar service, 594
  email, 556–557
  file sharing, 337–341
PTR (reverse mapping) record, 72
Public folder, in File Sharing, 359–360
public key fingerprint, SSH, 667–670
public key infrastructure (PKI), 113–114
public keys, PKI, 113–114
push notifications. See also APNs (Apple
  Push Notifications)
  inspect recipients of push alerts, 167
  requiring APNs, 158
  sending alerts to any Mac with, 160
  sending test alert, 168–170
  troubleshooting profiles, 310
pwd command, 646

Q

question mark (?) wildcard,
  command line, 655
Quick Look functionality, blogs/wikis, 584
quotas, mail user, 560–561, 566

R

-R (recursive command), 655–656
-r (recursive command), 655–656
RADIUS (Remote Authentication Dial-In
  User Service), configuring AirPort, 94
RAID volume, installing OS X on, 10
RAM, for OS X Server install, 4, 6–7
Reachability Details button, Overview
  pane, 88

Read set of permissions, ACEs, 390–391
realms, Kerberos, 243
records, DNS
  creating. See DNS zones and records, creating
  defined, 59
recursive commands (-R or -r), 655–656
recursive lookups, 76–81
redemption code, downloading student materials, 35
redirects, website, 526, 531, 532
redundant zone, configuring DNS hosts, 73–74
Refresh Calendars pop-up menu, 604
relative paths, 646
relay agent (helper address), DHCP, 505
relay options, Mail service, 566
Relay outgoing mail through ISP checkbox, alerts, 159
relay (replica), Open Directory, 195–196
remote access
  command line, 640
  troubleshooting, 102
  turning on, 103–104
  turning on via SSH. See SSH (Secure Shell), remote access via
  using Server app to configure, 83–86, 88–89
Remote Authentication Dial-In User Service (RADIUS), configuring AirPort, 94
Remote Management
  configuring Server App for, 84–85
  unenrollment from Profile Manager, 332
remotely locking device, 299–301
remotely wiping device, 299–301
Remove (–) button
  clean up shared folders, 369
  configuring DHCP, 516
  configuring forwarding servers, 67
  existing DHCP network, 509
  removing redundant DNS zone, 73–74
  removing share points, 349
removing inherited ACEs, 393
removing items at command line, 659
removing website, 545–547
Renew certificate, 130–131
replicas. See Open Directory replica
Reply, Mail, 576
repurposing computers, with NetInstall, 422
requestor, DNS, 59
requirements
  configuring OS X before OS X Server install, 20, 26–27
  file server organizational, 341–342
  OS X Server DNS hosting, 59–62
  OS X Server hardware, 4–7
Reset iOS device, 54
resources
  accessing with sudo command, 664–665
  adding in Calendar pane, 596–597
  creating for Calendar service, 601–602
restrictions. See recursive lookups
reverse mapping (PTR) record, 72
reverse zone, DNS, 69, 74
rm command, 659
rm -R command, 659
rmdir command, 659
root CA
  following certificate chain using trusted, 133–138
  importing signed certificate, 124
  overview of, 114–115
  trusted, 115
root servers, DNS lookups, 58
routes, advanced VPN configuration, 489–490
rules of precedence, POSIX and ACL, 398–399

S

SACLs (service access control lists), 239, 668
Safari, certificate trust, 153, 155
SCEP (Simple Certificate Enrollment Protocol), 310
schedule, Calendar, 595
scp command, 657
Screen Sharing
  administering users/groups remotely, 222
  copying VPN profile to client computer, 495
  custom access rules for, 110–112
  in Messages service, 619
  monitoring/managing server from different computer, 158
  restoring default access, 112
Screen Sharing and Apple Remote Access app
  allowing remote access, 84–85
  stopping/starting File Sharing, 361
  turning on, 103–104
scripts, creating command line, 640
search domain(s), advanced VPN configuration, 489
search fields, Open Directory log files, 210
secondary zone, DNS, 59
Secure FTP (SFTP), 341
Secure Sockets Layer. See SSL (Secure Sockets Layer) certificates
security
  Kerberos tickets, 244
  limitations of FTP, 337–338
  Messages federation, 623
  VPN. See VPNs (virtual private networks)
  WebDAV as good alternative to FTP, 341
Select Your Time Zone screen, local admin account, 24
self-signed certificates
  adding new, 120–125
  archive, 130
  automatic creation of new, 118
  decision to use, 117
  defined, 114
  examining default, 143–144
  generating, 125–126
  inspecting, 127–129
Send message, Mail, 574–575
Send Test Alert, 169
Server app
  Access tab, 106–112
  Accounts section of, 95
  AirPort pane of, 93–95
  archiving certificates, 130
  changing computer name/local hostname, 13–15
  command-line interface. See SSH (Secure Shell), remote access via
  configuring Contacts service, 611–612
  configuring DHCP, 505–510
  configuring File Sharing service, 342–343
  configuring forwarding servers, 67–68
  configuring OS X as OD replica, 205–206
  configuring OS X Server for certificates, 132–133
  configuring remote access, 83–86, 103–104
  configuring user accounts, 230–236
  configuring VPN service, 484–487, 492–494
  configuring Wiki service, 585
  creating user accounts, 223–228
  defined, 15
  ensuring Caching service, 462
  Help and Server Tutorials, 100–101
  importing list of users, 228–230
  initial install of, 35–36
  inspecting certificates, 127
  inspecting service data volume, 105
  Manage menu, 99
  managing websites, 523–525
  monitoring server, 165–172
  not removing from Applications folder, 17
  opening, 36–37
  overview of, 83
  Profile Manager, 285

remotely administrating OS X Server, 16
renewing certificates, 130–131
Server section of, 87–93
Services section of, 95–98
Time Machine backup destination, 473
Tools menu, 100
troubleshooting, 102
using serveradmin command, 675–680
viewing default certificate, 118
Server Backup volume, Time Machine backup files, 182
Server Help, Server app, 101
Server Message Block (SMB) protocol
authentication, 221
file/folder ownership/permissions, 384
SMB3. See SMB3 (Server Message Block 3) protocol
Server section, Server app. See also status and notifications
Access pane, 91–93
Alerts pane, 158–160
Logs pane, 161–163
Overview pane, 87–88
Settings pane, 88–90
Storage pane, 90–91
Storage tab, 165
server-side scheduling, Calendar service, 595
server token, Profile Manager for VPP, 289–290
Server Tutorials, 37, 100
serveradmin command, 675–680
servers, monitoring for problems, 344
service access control lists (SACLs), 239, 668
service data volume
inspecting, 105
moving location of, 89–90
service token, Profile Manager for VPP, 292–293
services
advanced, 97–98
authentication/authorization for, 220–222
basic OS X Server, 96–97
configuring server for certificates, 117, 132–133
Kerberized, 243–244
managing access to, 237–239, 269–273
planning file sharing, 341–344
troubleshooting access to, 248
troubleshooting availability of file-sharing, 355
troubleshooting Kerberos, 249
Settings app
reset iOS device, 54
stopping/starting File Sharing service, 361
Settings pane, Server app, 88–90
Setup Assistant
client iOS device setup, 55–56
set up OS X before installing OS X Server on server, 21–24
set up OS X on client computer, 44–46
SFTP (Secure FTP), 341
shadow files, 431–432
shadow password, in Open Directory authentication, 239
share points
adding/removing, 347–349
as challenge of file sharing, 336
configuring access with File Sharing pane, 378–382
configuring Groups shared folder, 353
configuring individual, 349–351
creating, 345–354
default, 346
exploring File Sharing, 345–346
FTP service, 356–357
guest access for, 381
overview of, 345
personal folders for iOS, 352–353
shared folders for home directories, 351–352
sharing folders over WebDAV, 338
using Connected Users pane, 353–354
Share pop-up menu, FTP, 356
shared devices, Profile Manager for
clean up, 320
creating enrollment profile, 314–319
importing placeholders/assigning to group, 311–314
overview of, 311
shared files. See File Sharing service
shared folders
accessing share points, 377–382
adding/removing share points, 347–349
clean up, 369
configuring access to share point, 402–403
configuring group folder, 353
configuring/using Time Machine service, 476
confirming access to, 365–366
creating new, 364–365
creating new location for, 363–364
creating user account, 250
default, 346
FTP, 356–357
giving to group, 366
for home directories, 351–352
inspecting NetInstall, 445–446
moving files to, 367–368
public folders as, 359–360
sharing over different protocols simultaneously, 339
Shared Folders segment, Settings pane, 345–346
Shared Items folder, 345, 364–365
shared secret (passphrase), configuring VPN, 487, 492–493
Sharing pane, System Preferences, 13–15
Sharing preferences, 84–86
shell, switching with sudo command, 663
short name. See account name (short name)
shortcuts, command, 644, 647
Show Accounts Browser, 234–235
Show All Records
creating new DNS record, 69–70, 72–73
inspecting limited default zones, 69
inspecting new zones/records, 70–72
Show Certificate
configuring client computer to trust certificate, 153
configuring trust, 138, 140
confirming new website is active, 544
Show Profile, VPNs, 495–496
signed certificate, importing, 124–125
Simple Certificate Enrollment Protocol (SCEP), 310
Simple Mail Transfer Protocol. See SMTP (Simple Mail Transfer Protocol)
single sign-on
defined, 242
Open Directory authentication with KDC, 239
using Kerberos, 242–247
single-user mode, accessing command line in, 641
Siri, client iOS device setup, 55
slapconfig command, Open Directory domain, 213
SMB (Server Message Block) protocol
authentication, 221
file/folder ownership/permissions, 384
SMB3 (Server Message Block 3) protocol
adding/removing share points, 347–349
comparing file-sharing protocols, 340–341
editing share points, 351
enabling file sharing, 337
enabling personal folders for iOS use, 353
encryption, 358, 360
shared folders for home directories, 351–352
sharing folders over different protocols simultaneously, 339
SMTP (Simple Mail Transfer Protocol)
Mail service logs, 579

OS X Server alerts, 158–159
as primary email protocol, 556
relay options, 566
sending Mail to group, 574–575
troubleshooting Mail, 564
snapshots, Time Machine, 177
SoA (Start of Authority), DNS, 63
software
deployment tools. See NetInstall service
license agreement, 17, 37
updating before OS X Server install, 32–33
updating client computer, 52–53
Software Update service
Caching service vs., 459–461
managing software updates, 465–467
troubleshooting, 467–468
troubleshooting Caching service, 462
sorting ACLs canonically, 393
spam
configuring OS X Server alerts, 159
filtering, 562
testing filter, 577–578
troubleshooting Mail, 564
Spam Assassin software, 561
Spamhaus Project, blacklist hosted by, 561
sparse disk image, Time Machine network backup, 473–474
special characters
command-line navigation, 647–649
wildcard characters, 655
speed
Gigabit Ethernet, 6
improving NetInstall, 427
spoofing, SSH preventing server, 667
Spotlight search service, from command line, 654
square brackets ([ ]) wildcard, command line, 655
srm command, 659
ssh-keygen command, 668–669
SSH (Secure Shell), remote access via
closing/inspecting fingerprint file, 670–671
configuring Server App, 85–86
inspecting public key fingerprint, 668–669
open SSH connection/confirm SSH fingerprint, 669–670
Password Server log using, 671–675
remote login, 640, 641
restoring default access, 112
SFTP using, 341
turning on, 667–668
SSL (Secure Sockets Layer) certificates
accessing WebDAV protected with, 338
basics, 113–117
binding server to another OD service, 207
creating new website, 544
decide what kind to use, 117
issuing new, 542–543
managing website, 525–526
Messages federation security, 623
Messages service setup, 624–625
modifying default website, 535–536
overview of, 113
preparing for Profile Manager, 279
protecting wikis, 584
restricting access to default website, 548–549
troubleshooting, 142
turning on Profile Manager, 287
SSL (Secure Sockets Layer) certificates, configuring
adding new certificates, 119
archive certificate, 130
examining default certificate, 118–119, 143–144
following certificate chain, 133–138
generating self-signed certificate, 125–126
importing signed certificate, 124–125
inspecting certificate, 127–129
Open Directory CA, 145–152
OS X Server, 13
OS X Server services for, 132–133
overview, 118
renewing certificate, 130–131
trust, 120–124, 138–142, 152–156
standalone server
access to services, 199
configuring Open Directory as, 192
describing, 193
Start of Authority (SoA), DNS, 63
startup
accessing command line in single-user mode, 641
DHCP service, 509
from NetInstall image, 446–448
from NetInstall, NetBoot or NetRestore image, 424–425
NetInstall service, 442–446
Startup Disk preferences, 447–448, 450
startup disk, Time Machine service, 475–477, 478–479
Startup Manager, NetInstall image, 447
startup volume
changing name of, 27–28
confirming computer is qualified, 26
performing clean install, 8–9
preparing for NetInstall service, 434–435
static address assignment, DHCP configuring, 510
troubleshooting, 511
understanding, 504–505
Stats pane, Server app, 158, 163–164, 457
Stats, Server app, 164–165
status and notifications
monitoring and status tools, 157–158
OS X Server alerts, 158–160
overview of, 157
using logs, 161–163
using Server app to monitor server, 165–172
using stats, 163–164
storage
mail quotas for users, 560–561
preparing for NetInstall service, 433–434
System Image Utility, 426–427
Wiki file, 584
Storage pane, Server app
comparing views of permissions in, 414–415, 418
configuring access to share points/folders, 382–383
configuring Time Machine, 481
confirm computer is qualified for OS X Server, 27
creating new location for shared folders, 363–364
overview of, 5, 90–91
propagating permissions manually in, 395
Storage tab, Server app
defined, 158
monitoring disk space, 170–171
viewing storage space in OS X Server, 165
student number
establishing for exercises in this book, 21
setting Computer Name, 48
su command, 661–662
subnets
configuring DHCP, 516
DHCP serving multiple, 505
editing for DHCP, 506–509
placing Caching server on, 458
sudo command
accessing resources, 664
command-line administration, 662–663
Password Server log and, 671–672
serveradmin command, 676–677
switching shells, 663
tab completion, 650
viewing contents of personal chats, 623
viewing Messages archive, 635
sudo killall mDNSResponder command, DNS, 65

system configuration, System Image Utility, 427
System Image Utility
- creating customized NetInstall image, 437–438
- creating images, 426–427
- using NetInstall, 428–430
- using NetRestore, 430–431

System keychain
- configuring trust, 141
- inspecting certificates, 127–129
- issuing new SSL certificate, 542

System Preferences
- client computer networking, 48–50
- client computer trusting certificate, 153
- Computer Name, 28–29, 48
- File Sharing, 346
- Local Admin account, 25–26
- network interfaces, 29–32
- starting VPN connection without opening, 496–497
- Time Machine, 180–181
- updating software, 32–33, 52–53
- Users & Groups preferences in. See Users & Groups preferences
- verifying OS X Server, 4–5

System Roots keychain, 115, 116
system user (root), 640

T

tab completion
- in command line, 648
- file paths with, 665
- overview of, 649–650

tape, back up to, 174
Target Disk Mode, using NetRestore, 430
TCP (Transmission Control Protocol), VPN service, 487
templates
- creating user, 255–256
- creating user and group, 227–228
- creating user from, 256–257
- importing users from delimited text file, 259

Terminal
- accessing command line, 640–641
- clean up DNS permissions, 80–81
- clearing screen, 666
- configuring recursive lookup restrictions, 78
- confirming restricted access to DNS, 80
- customizing command line with preferences, 665
- inspecting public key fingerprint, 668–669
- removing Open Directory domain, 213

terminology, Profile Manager, 278–279
testing
- alerts, 168–170
- Caching service, 461–464

text
- adding blog to wiki, 591
- converting certificate into file with, 124
- editing wiki, 589–590
- messages. See Messages service

text editor, vi command, 660–661
TextEdit, 124
TFTP (Trivial File Transfer Protocol), NetInstall, 425
third-party products
- accessing FTP service with read/write capabilities, 358
- troubleshooting server installations, 19–20
- web proxy in Server 5 impacting, 521
- working with Calendar service, 595

ticket-granting ticket (TGT), Kerberos, 244, 245–246
Ticket Viewer, Kerberos, 245–247, 249
tickets, Kerberos
- basics, 244
- examining with Ticket Viewer, 245–247
- obtaining on Mac, 245
- troubleshooting, 249

tier-one replica, 195
tier-two replica, 195
tilde (~) character, command line, 649, 672
Time Machine backup
- client browsing for, 10
- configuring, 180–181
- with external disk as destination, 178
- inspecting files, 181–186
- with internal volume as destination, 179–180
- network and local home folders, 351
- Open Directory archive and, 202–203
- overview of, 175–177
- promoting Open Directory replica to master, 196
- restoring Open Directory info from, 211–217

Time Machine network backup
- clean up, 481
- configuring, 472–474
- configuring client computer to use destination, 477–479
- configuring/using Time Machine service, 475–477
- inspecting status of, 479–481
- overview of, 471

timestamps, backup log, 186
tips and tricks, command line, 665–666
TLD (top-level domain) server, DNS lookups, 58
Tools menu, Server app, 100, 426
touch command, 657
Transmission Control Protocol (TCP), VPNs, 487
Trivial File Transfer Protocol (TFTP), NetInstall, 425
troubleshooting
- access to Open Directory log files, 209
- Caching service, 461–464
- Calendar service, 598
- client computers with NetInstall, 423
- Contacts service, 610–611
- DHCP, 511–513
- DNS service in OS X Server, 64–65
- File Sharing service, 355, 375–376
- imported users, 248
- Mail service, 563–564
- Messages service, 624
- NetInstall service, 433
- Open Directory services, 209–211
- OS X Server, 19–20
- Server app, 102
- Software Update service, 467–468
- SSL certificates, 142
- using Ticket Viewer in Kerberos, 245
- VPN service, 490–491
- web services, 529
- Wiki service, 584

trust profile
- configuring iOS devices/OS X computers, 116
- creating customized NetInstall image, 438–441
- downloading, 436–437

trusted certificates
- binding server to another OD service, 207
- configuring, 138–142
- configuring client computer for, 152–156
- for default self-signed certificates, 144
- following certificate chain, 133–138
- getting from widely trusted CAs, 121–123
- inspecting certificates, 127–129
- inspecting OD certificates, 150
- for Profile Manager, 279
- self-signed certificates as, 117
- signed by widely trusted CAs, 115–116

U

UDP (User Datagram Protocol), VPNs, 487
UIDs (user IDs), POSIX and ACLs, 395–396
umask variable, POSIX permissions, 385

unenrollment, from Profile Manager, 332
uninterruptible power supply (UPS), availability, 7
universally unique ID (UUID), 385, 395–396
UNIX-style permissions. See POSIX (Portable Operating System Interface) permissions
Up Arrow keys, command-line tips, 666
updates
  ACL inheritance rules for folder, 393
  client computer software, 52–53
  OS X Server, 19
  of passwords for imported users, 261–262
  using NetInstall for multiple workstation, 422
upgrades
  OS X Server, 17–18
  Sharing settings inherited on, 86
uploading documents, editing wiki text, 589–590
URL (uniform resource locator)
  managing websites, 525
  updating configuration profile for wikis, 588
Usage section, Caching server, 456
Use as Default Boot Image, default NetInstall image, 445
User Datagram Protocol (UDP), VPNs, 487
user ID (UID) attribute, user account advanced options, 227
user IDs (UIDs), POSIX and ACLs, 395–396
user name
  authentication/authorization, 220–222
  saved VPN configuration profile, 490
  VPN service, 487
user portal
  administering Profile Manager, 278
  remotely locking/wiping device via, 300–301
users
  adding group to group, 255
  adding in System Image Utility, 427
  configuring in Messages, 620–621
  configuring in Server app, 342
  creating from template, 256–257
  creating group, 251
  creating new, 252–253
  creating new folder for home folders, 249–250
  creating user template, 255–256
  default access rules restricting, 92
  disconnecting File Sharing, 368
  editing, 253–255
  inspecting group Workgroup, 250–251
  preferences, 301–304
  restricting Messages app, 631–632
  restricting Messages service, 630–631
  settings for, 296
  troubleshooting file-sharing service, 355
Users & Groups preferences
  administering local users and groups, 222
  binding OS X to OD service, 209
  binding server to another OD service, 207
  binding to another directory server, 199
  default share points created in, 346
  in Profile Manager, 323–324, 329
  services access for accounts created with, 238
  specifying user as administrator, 231
  troubleshooting directory services, 211
  using Directory Utility remotely, 208
users, managing
  authentication/authorization, 220–222
  configuring accounts, 230–236
  configuring authentication, 239–242
  configuring password policies, 265–269
  creating accounts, 223–228
  creating and administering, overview, 222
  creating/editing accounts, 249–257
  disabling account, 240
  importing account, 228–230, 257–265
  overview of, 219–220
  server access, 269–273
  services access, 236–239
  troubleshooting, 247–249
  troubleshooting importing, 248
  troubleshooting Kerberos, 249
  troubleshooting services access, 248
  using single sign-on and Kerberos, 242–247
Users pane, Server app
  Accounts section, 96
  configuring password policies, 265–266
  confirming removal of Open Directory domain, 214
  creating new user, 252–253
  creating user group, 251
  importing users from delimited text file, 258–260
  importing users from exported formatted file, 260–261
  inspecting access to services, 270–271
  inspecting Workgroup group, 250–251
  managing access to files and services, 238–239
  restricting Messages users, 630
  setting global password policies, 241–242
  users hidden from view, 239
UTC (Coordinated Universal Time) standard, 186
UUID (universally unique ID), 385, 395–396

V

var folder, Time Machine backup files, 183
Verify Your Identity dialog, iOS device, 54
vi command, text editor, 660–661
video conference, Messages service, 619
View Alert, 160
views
  File Sharing users, 368
  hidden items at command line, 650–651
  Messages service/chat logs, 633–636
  of permissions, 413–417
Virtual Network Computing (VNC), 84
virtual private networks. See VPNs (virtual private networks)
viruses
  confirming Mail scanned for, 576–577
  downloading definitions with Mail service, 564–565
  scanning incoming email for, 561
visudo command, 665
VNC (Virtual Network Computing), 84
Volume Purchase Program. See VPP (Volume Purchase Program)
volume(s)
  configuring Caching service, 455–456
  configuring Time Machine network backup, 472–474
  configuring Time Machine to stop offering server, 481
  creating NetInstall images from mounted, 429
  defined, 8
  installing OS X on RAID, 10
  installing OS X Server on, 8
  moving Caching Service data, 464
  navigating to other, 651
Volumes folder, 651
VPNs (virtual private networks)
  advanced options, 488–490
  clean up, 498–499
  copying VPN profile to client computer, 494–495
  describing, 483–484
  examining logs, 498
  installing/using VPN profile, 495–497

- overview of, 491–492
- saving configuration profile, 490
- with Server app, 484–487
- and starting, 492–494
- troubleshooting, 490–491

VPP (Volume Purchase Program)
- acquiring apps for multiple computers, 422
- clean up, 293
- managing apps, 297–298
- using groups for enrollment in, 287
- using with Profile Manager, 281–283

W

web clips, updating configuration profile for wiki, 588

web hosting services. See websites, hosting

web link, delivering profiles via, 298

web proxy, Server 5, 521

web services
- basic website structure, 522–523
- monitoring, 528, 549–551
- turning on, 529–532
- turning on and off, 524–525

WebDAV (Web-based Distributed Authoring and Versioning)
- adding/removing share points, 347–349
- comparing file-sharing protocols, 340–341
- enabling file sharing, 337–338
- enabling personal folders for iOS, 353
- file/folder ownership and permissions, 384
- iOS device users accessing wiki files, 584
- reviewing file-sharing logs, 344
- for share points in iOS device, 338–339
- sharing folders over different protocols simultaneously, 339

websites
- basic structure of, 522–523
- turning on and off, 523–525

websites, hosting
- basic structure, 522–523
- creating new website, 540–545
- identifying web service software, 521–522
- managing websites, 525–527
- modifying default websites, 533–539
- monitoring web services, 528, 549–551
- removing website, 545–547
- restricting access to website, 547–549
- specifying certificates for hosted sites, 133
- troubleshooting web services, 529
- turning on web services, 529–532
- turning websites on and off, 523–525

Websites service, 152–155, 156

Welcome screen, 22

which command, file management, 652

whitelist IP address of server, alerts, 159

who -m command, 661–662

Wi-Fi
- configuring client computer to trust certificate, 153
- configuring OS X before OS X Server install, 22
- for learning/testing scenarios only, 6
- NetInstall unsupported over, 435
- network interface settings for, 30
- setting up client iOS device, 55

widely trusted CA
- archive certificate signed by, 130
- decision to use, 117
- renewing certificate signed by, 131
- using certificate signed by, 115–116

Wiki service
- configuring/managing, 581–584
- editing wikis, 589–592
- overview of, 581–582
- setting up wikis, 526
- troubleshooting, 584
- turning on, 585–588
- viewing wikis as anonymous user, 592

wildcard characters (globs), 654–655

workflow, customizing NetInstall image, 440–441

Workgroup
- using Calendar service, 602–603
- using configuration profile for Mail, 569–572
- using Messages service, 626–627

Workgroup group, 250–251

working directory, command-line prompt and, 641–642

Write set of permissions, ACEs, 391

_www user or group, 523, 529

X

XML (Extensible Markup Language), profiles in, 298

Y

Yosemite
- checking if computer can run, 4–5
- hardware for OS X Server install, 4
- installing Server app on another computer, 158
- sending alerts to any Mac, 160
- supporting Gigabit Ethernet, 6
- upgrading/migrating to OS X Server, 17–18

Z

zero-configuration networking, 10, 12

zone files, DNS, 59

zone transfer, DNS, 59

Server 5.0
ntials
s, Numbers
Keynote
OS X Support Essentials 10.11
Supporting and Troubleshooting OS X El Capitan
Kevin M. White and Gordon Davisson
Logic Pro X 10.1
Professional Music Production
David Nahmani
Final Cut Pro X 10.2
Professional Post-Production
Brendan Boykin
Apple Pro Training Series