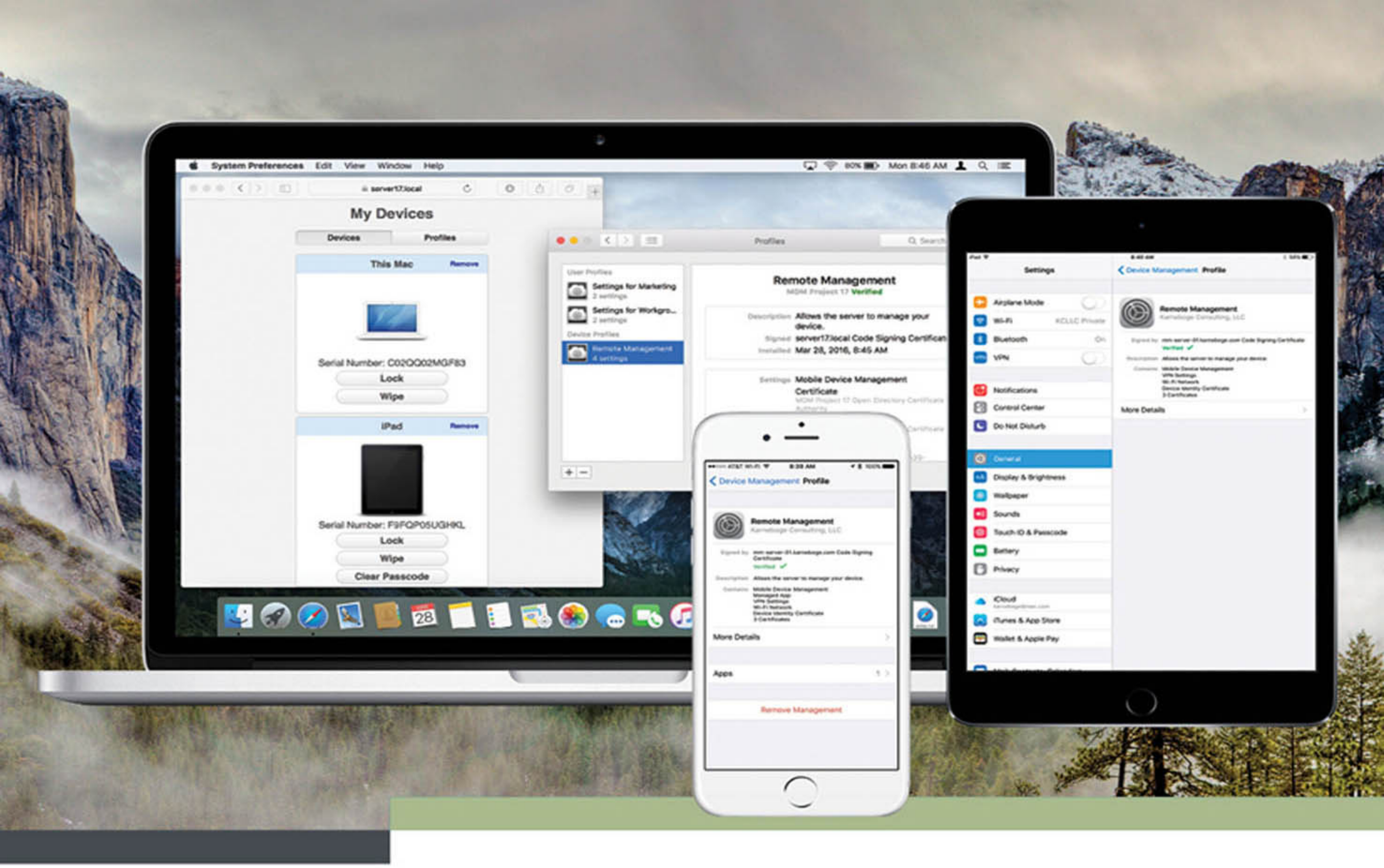


Managing Apple Devices

THIRD EDITION

DEPLOYING AND MAINTAINING
iOS 9 AND OS X EL CAPITAN DEVICES

AREK DREYER | ADAM KARNEBOGE

FREE SAMPLE CHAPTER

Managing Apple Devices

THIRD EDITION

Arek Dreyer and Adam Karneboge

Managing Apple Devices, Third Edition
Arek Dreyer and Adam Karneboge

Peachpit Press
www.peachpit.com

To report errors, please send a note to errata@peachpit.com.
Peachpit Press is a division of Pearson Education.

Executive Editors: Lisa McClain and Nancy Davis
Production Editor: Maureen Forys, Happenstance Type-O-Rama
Project Editor and Copy Editor: Kim Wimpsett
Technical Editor: Craig Cohen
Proofreader: Darren Meiss
Compositor: Cody Gates, Happenstance Type-O-Rama
Indexer: Jack Lewis
Cover Production: Happenstance Type-O-Rama
Cover Design: Mimi Heft

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.

ISBN-13: 978-0-13-430185-3
ISBN-10: 0-13-430185-4

9 8 7 6 5 4 3 2 1

Thanks to Heather Jagman for her love, support, and encouragement.

—Arek Dreyer

Thanks to Dr. Nasser Hanna and the amazing staff at Indiana University Health. I would have never been able to embark on this journey without them.

This book is dedicated to my parents, Monica and Brian Karneboge.

—Adam Karneboge

Acknowledgments Thanks to you, dear reader, for staying on top of what's new, while keeping your users' needs as the root of what you do.

Thank you to Tim Cook and everyone at Apple for always innovating.

Thanks to Craig Cohen for insightful technical editing.

Thanks to Schoun Regan for his help and guidance, and to his team for setting an example of great documentation.

Thank you to the amazingly capable Nancy Davis and Lisa McClain for gently making sure these materials made it into your hands, and to Kim Wimpsett, Darren Meiss, and Maureen Forys and her team at Happenstance Type-O-Rama for working their editorial and production magic.

Thank you to the following people. Without your help, guidance, suggestions, and feedback, this guide would be much less than what it is.

Jeremy Agostino

Mike Boylan

Weldon Dodd

Josh Durham

Charles Edge

John Filardo

Patrick Gallagher

Erik Gomez

Richard Goon

Christopher Holmes

Andrew MacKenzie

Keith Mitnick

John Poynor

Owen Pragel

Maurits Sanders

Sal Soghoian

Sam Valencia

Kevin White

Joan Work

Table of Contents

Lesson 4

OS X Server 5 on El Capitan

OS X Server 5 helps your users collaborate, communicate, share information, and access the resources they need to get their work done. While OS X Server indeed provides a variety of services, the aim of this guide is to focus on the services that facilitate the management of Apple devices.

This lesson begins with a brief introduction of OS X Server before moving into the requirements and initial setup of OS X Server. This lesson also covers selecting and configuring Secure Sockets Layer (SSL) certificates required for Apple device management.

GOALS

- Perform the initial installation and configuration of OS X Server
- Consider TLS/SSL certificate requirements and best practices

NOTE ▶ Although you can install OS X Server 5.0 on OS X Yosemite, the version available from the Mac App Store at the time of this writing is OS X Server 5.1, which requires OS X El Capitan 10.11.4. Server 5.1 provides additional support for new features in iOS 9.3.

Reference 4.1
OS X Server Benefits

Other solutions are capable of providing management for Apple devices, but at only $19.99 (US), not many of them are as inexpensive as OS X Server. Also, despite the price, because Apple develops OS X Server, it’s often the first management solution that supports the latest Apple management features and operating systems.

Further, even if you intend to use a third-party Mobile Device Management (MDM) solution, other services in OS X Server are still clearly the best solution. For example, the Caching service has no supported alternative. The NetInstall service that provides network system disk access for OS X computers is available from other servers, but the implementation in OS X Server is supported by Apple.

Services Covered in This Guide

Again, this guide focuses on the OS X services that are most responsible for helping administrators manage their Apple deployments:

- Caching service—As introduced previously, the Caching service greatly reduces Internet bandwidth used for the installation of Apple-sourced software and media. Lesson 5, "Caching Service," focuses on the architecture, setup, and troubleshooting of this service.

  NOTE ► OS X Server 5 still offers the legacy Software Update service. However, this older service is limited to providing updates for OS X system software and Apple software installed from outside the Mac App Store. Because of this service's limited use in contemporary Apple deployments, it's not covered in this guide.

- Profile Manager—This is the name given to the MDM service provided by OS X Server. The vast majority of material in this guide deals directly with or is designed around MDM management workflows. Both Lesson 6, "Configuration and Profiles," and Lesson 7, "Mobile Device Management," cover Profile Manager specifically. In addition, nearly all lessons that follow these two deal with topics related to MDM services.
- NetInstall—This service makes OS X systems available for startup via a network connection. NetInstall is often used as a platform for installing or re-imaging Mac computers en masse. Coverage of this service is beyond the scope of this guide, but you can find out more from *Apple Pro Training Series: OS X Server 5.0 Essentials on El Capitan* (Peachpit Press, 2016).
- File Sharing—The local file-sharing service provided by OS X Server supports both iOS and OS X devices. The new option in Server 5, "Create personal folders when users connect on iOS," is available for supported iOS apps (at the time of this writing: Keynote, Numbers, and Pages) with Server 5 on El Capitan (not available with Server 5 on Yosemite). Additionally, in the File Sharing pane, you can configure each shared folder to support WebDAV, and some iOS apps support WebDAV.
- Wiki—The OS X Server Wiki service not only provides a browser-based interface for collaborative document creation but serves as an alternative for local file sharing.

  MORE INFO ► For more detailed coverage of OS X Server setup and services outside the scope of this guide, check out *Apple Pro Training Series: OS X Server 5.0 Essentials on El Capitan* (Peachpit Press, 2016).

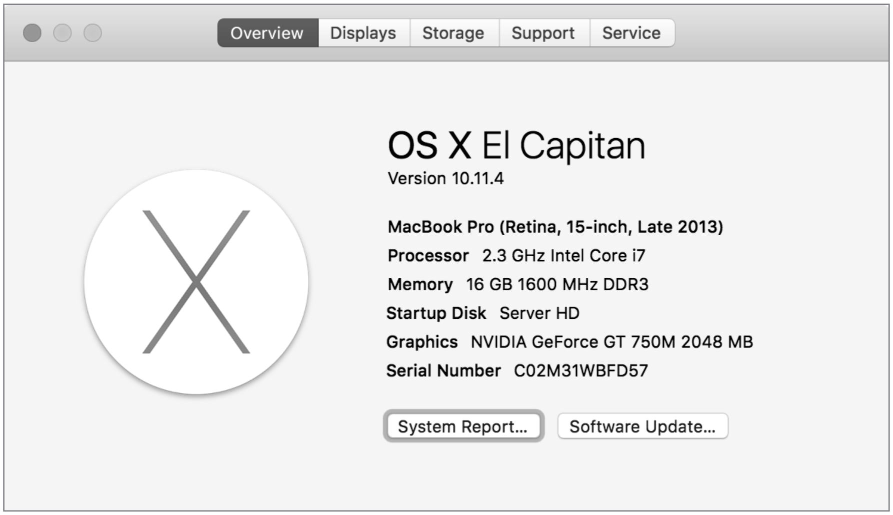
Reference 4.2
OS X Server Setup

This section outlines the system requirements for OS X Server and presents suggestions for scoping server hardware. It also gives recommendations for network configuration of an OS X Server.

MORE INFO ▶ You'll find more detailed step-by-step instructions for installing and configuring OS X Server in the exercises later in this lesson.

Verifying Server Hardware Requirements

OS X Server 5.1 is an app that runs on any Mac running El Capitan 10.11.4 with 10 GB of free disk space. Before you install OS X Server, confirm that your system meets at least the minimum hardware requirements. You can find this information on the label attached to the box of every Mac sold, or you can find it with the About This Mac and System Information applications.



OS X El Capitan
Version 10.11.4

MacBook Pro (Retina, 15-inch, Late 2013)
Processor 2.3 GHz Intel Core i7
Memory 16 GB 1600 MHz DDR3
Startup Disk Server HD
Graphics NVIDIA GeForce GT 750M 2048 MB
Serial Number C02M31WBFD57

To run El Capitan, your Mac must be one of the following models or later:

- iMac (mid-2007 or later)
- MacBook (13-inch Aluminum, late 2008; 13-inch, early 2009 or later)
- MacBook Pro (13-inch, mid-2009 or later; 15-inch or 17-inch, mid/late 2007 or later)

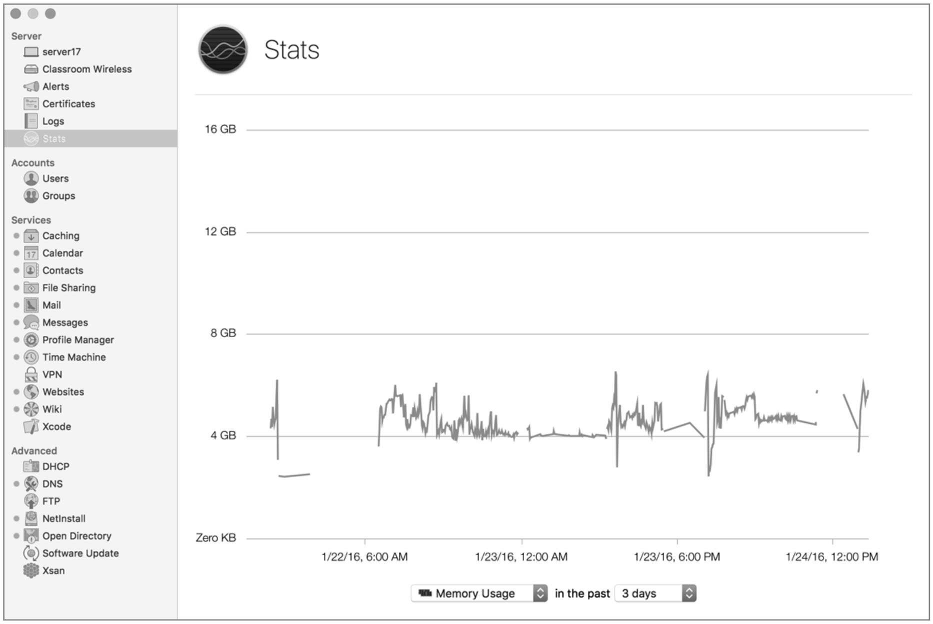
- MacBook Air (late 2008 or later)
- Mac mini (early 2009 or later)
- Mac Pro (early 2008 or later)
- Xserve (early 2009)

Some features of OS X Server require an Apple ID, and some features require a compatible Internet service provider.

Server Hardware Considerations

For the purposes of the exercises in this guide or any other deployment testing, you can run OS X Server on just about any contemporary Mac. In practice, however, consider the size of your Apple deployment and select hardware appropriate for your production needs:

- Memory—In general, more system memory results in better system performance, but exactly how much memory is ideal for your situation is impossible for this guide to prescribe. You can, however, get a good idea of system memory usage for an existing server from the Memory Usage and Memory Pressure statistics available in the Stats pane of the Server app. Obviously, if you observe extremely high memory usage, upgrading the Mac computer's system memory is a good idea.



- Storage—Be sure you have enough disk space to hold the data for the services you plan to offer. If the services you plan to offer are disk intensive (for example, the Wiki service with a high volume of user content), consider using a faster physical disk or even an external disk system. An external disk is especially useful for the Caching service since it can potentially fill an entire disk, and the more items that are cached, the more effective the service.
- Backup—You cannot re-create a lost MDM database because of the security architecture of the MDM service. Thus, if the data store for Profile Manager is lost, you will lose the ability to manage your Apple devices. The devices will retain existing management settings but will accept new management only when enrolled into a new MDM service. In short, you really need to back up your management server. OS X Server is fully supported by the Time Machine backup built in to OS X.
- Network interfaces—Be sure to consider the speed of the network interface when making a server hardware decision. Most Mac computers support Gigabit Ethernet. All Mac computers capable of running OS X Yosemite or El Capitan that include built-in Ethernet interfaces support Gigabit Ethernet. If your Mac is equipped with Thunderbolt interfaces, you can use Apple Thunderbolt to Gigabit Ethernet adapters to add Ethernet interfaces. All services, except for Caching and NetInstall, can operate from the Mac system's Wi-Fi interface. But for performance reasons, it's not recommended that you provide services via a Wi-Fi interface.
- Availability—To help ensure that OS X Server stays up and running, you can turn on the Energy Saver system preference "Start up automatically after a power failure" (not available on all Mac systems). It's also recommended that you use an uninterruptible power supply (UPS) for your server, including any external volumes, to keep your server up and running in the case of a brief power outage.

Server Network Considerations

Again, for the purposes of completing exercises in this guide or for general testing, you can configure your server using whatever Internet Protocol (IP) address was set via Dynamic Host Control Protocol (DHCP) and even use the computer's local Bonjour name. However, some services may be negatively affected if the server's IP address or host name is changed.

TIP If you absolutely must change the name of your server, do so only via the server Overview settings in the Server app. On a computer running OS X Server, you should never change the name via Sharing preferences.

For example, your MDM service must be resolvable on all managed devices to a single Domain Name System (DNS) host name. Managed devices communicate with the MDM service only via the single host name used during enrollment. In other words, if you want to change the DNS host name clients use to resolve the MDM service, you will have to reenroll all your devices with the new host name.

Given that changes to a server configuration can dramatically affect device management, it's obviously best to select network settings that will remain appropriate throughout the duration of your deployment. Consider the following factors when configuring network access for your management server:

- IP address—Configuring a static IP address for your production OS X Server is highly recommended. The primary reason for this is to prevent accidental changes that would prevent the DNS host name of the server to become unreachable.
- Subnets—With the exception of two specific issues, most OS X Server services aren't affected by subnet settings. First, if you don't use a DNS host name and instead rely on the Bonjour local host name (often defined as something like computername.local), only devices on the local subnet will recognize your server's local host name. Obviously, this issue can be resolved by configuring a "real" DNS host name. Second, the NetInstall discovery service broadcast doesn't travel beyond the local subnet by default. Resolving this issue is detailed in Apple Support article PH15509, "Set up NetInstall service across subnets."
- Computer name—The server's computer name affects access to the server only from the local subnet. The computer name is often used to define the Bonjour local host name, which again is resolvable only on the server's local subnet. For any server that needs to be reachable beyond the local subnet (that is, most servers), the computer name doesn't really matter.
- DNS host name—A server's DNS host name is how most clients will resolve access to almost all the services hosted on your server. You must coordinate with your DNS network administrator to make sure the server's DNS host name is properly configured. Remember that OS X Server requires both a forward and reverse DNS host name record for proper setup.
- Network ports—The variety of services offered by your server use a range of both User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) network ports. A properly configured firewall should allow traffic only for the necessary network ports. Thus, newly configured services often require changes to established network firewalls. You will likely have to work with the network firewall administrator

to open additional ports for managing Apple devices. Throughout this guide, when a specific service's architecture is detailed, the required network ports will be included with the documentation.

MORE INFO ▶ Apple maintains a list of all the well-known network ports used by Apple products in Apple Support article HT202944, "TCP and UDP ports used by Apple software products."

- Simple Mail Transfer Protocol (SMTP) relay—A variety of services in OS X Server will send email messages as part of their function. If your organization relies on an SMTP relay service for sending email messages, then you need to configure OS X Server to take advantage of this service.

  MORE INFO ▶ For information about configuring OS X Server to use an SMTP relay, see Apple Support article HT202962, "OS X Server: Sending email invitations, notifications and alerts when an SMTP relay is required."

External Access and Reachability Testing

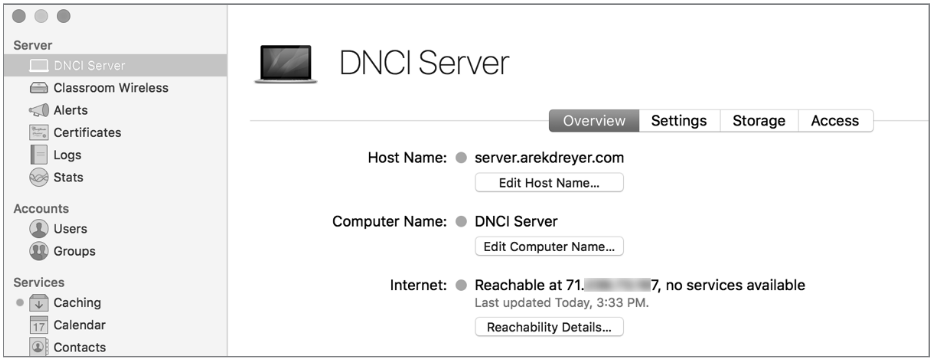
Managed devices can receive management changes only if they can access your MDM service. Thus, if you require that devices are able to receive management changes when they are outside your network or on the Internet, your network infrastructure will have to be properly configured to allow connections from outside your network to reach your server.

If your server is on an internal network that uses private IP addresses, as is the most common case, your network routing will need to be configured so that it forwards traffic from a public Internet IP address to your server. If this is the case, only the required specific TCP ports will likely be forwarded to your server. Obviously, coordinating with a network administrator will be required to properly configure network routing and firewall rules.

Another consideration if your server is to be accessed from the Internet is that the DNS host name must be resolvable to any host on the Internet. As covered previously, in most of these cases, your server will be accessible via an external public IP address that forwards to an internal private IP address. This type of IP forwarding also requires a DNS configuration—commonly known as *split DNS*—where a single host name resolves to the proper IP address both externally and internally.

In other words, even though your server uses a single DNS host name, devices in your network will resolve this host name to a private IP address; devices outside your network will resolve the same host name to a public IP address. Again, coordinating with a network administrator is required to properly set up this type of DNS configuration.

Properly testing external service reachability can be tricky because it requires that you have access to a test external network. Fortunately, reachability testing will help you determine whether your server is accessible to Internet clients. This testing service is turned on by default, and you can find the results in the server Overview tab in the Server app.



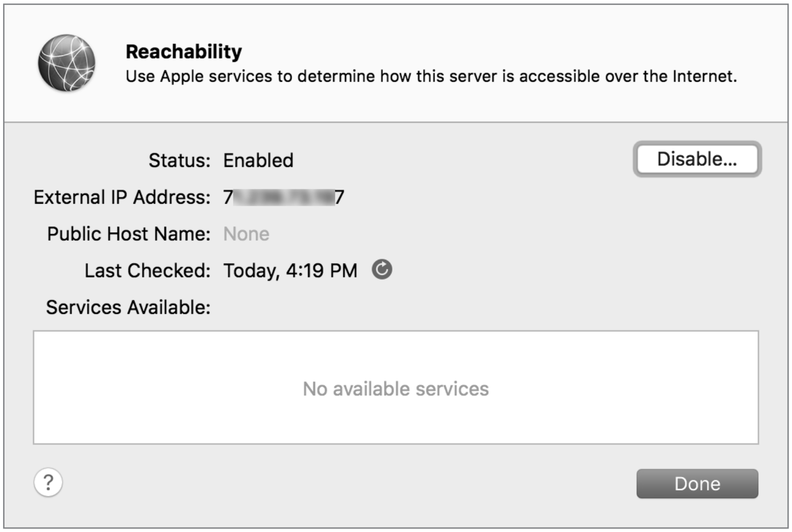
DNCI Server

Host Name: ● server.arekdreyer.com

Computer Name: ● DNCI Server

Internet: ● Reachable at 71.[redacted]7, no services available
Last updated Today, 3:33 PM.

You can further verify reachability for specific services by clicking the Details button to the right of the reachability information. The reachability service works by instructing automated servers at Apple to try to contact your server. In the reachability detailed view, you can see what external IP address, public host name, and specific services are available. This information will be valuable for any network administrator who is trying to help you facilitate external access for your server.



Reachability
Use Apple services to determine how this server is accessible over the Internet.

Status: Enabled
External IP Address: 7[redacted]7
Public Host Name: None
Last Checked: Today, 4:19 PM
Services Available:
No available services

Reference 4.3
TLS/SSL Certificates

Transport Layer Security (TLS) and its predecessor, SSL, are protocols for the secure transmission of data between hosts. More specifically, TLS/SSL technology is used to prove your server's identity to client devices and to encrypt communication between your server and client devices. This encryption isn't just recommended to secure OS X Server services; it's required for any MDM service including Profile Manager. This section starts with the basics of TLS/SSL certificates and then provides recommendations for certificate best practices in regard to managing Apple devices.

Understanding Certificates

To enable TLS/SSL communications, you must configure your server with a TLS/SSL certificate (also referred to as simply a *certificate*). A certificate is a file that identifies the certificate holder. A certificate specifies the permitted use of the certificate and has an expiration date. This is why certificates must be renewed on a regular basis (most often annually).

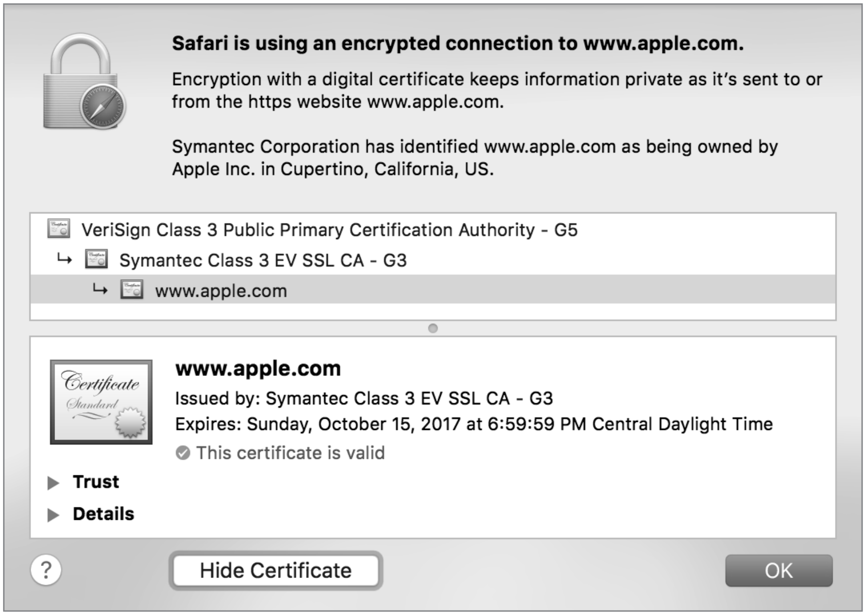
Importantly, a TLS/SSL certificate also includes a public key infrastructure (PKI) public key. This public key is mathematically tied to a private key that is securely stored on the server. Data encrypted with one key can be decrypted only by using the other key. Thus, if you can decrypt data with one key, it proves that the data was encrypted with the other key.

To initiate secure TLS/SSL connections, client devices download the certificate (containing the public key) from your server. If a client can successfully verify the identity of the server from the certificate, it will use the public key to begin secure communications with the server. This raises the question, how exactly does a client device verify, or trust, a certificate?

The answer is that a certificate is verified by its digital signature. A certificate is either self-signed or signed by a certification authority (also known as a certificate authority or, more simply, a CA). A self-signed certificate, as the name implies, doesn't require the involvement of other CAs; thus, OS X Server will automatically create a self-signed certificate during the setup process. You can use a self-signed certificate for most TLS/SSL services, but self-signed certificates created by OS X Server (and most other servers) are not trusted by Apple devices for MDM services.

In other words, if you need to manage Apple devices, you will need to configure a certificate that has been signed by a verifiable CA. Certificates used by servers are most often signed by an intermediate CA, which is a CA whose certificate is signed by another CA.

The PKI infrastructure allows for a hierarchical chain of certificates, commonly known as a *chain of trust*. For example, the following figure shows the chain of trust for https://www.apple.com, which can be revealed in Safari by clicking the lock to the left of a web address:



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.

Symantec Corporation has identified www.apple.com as being owned by Apple Inc. in Cupertino, California, US.

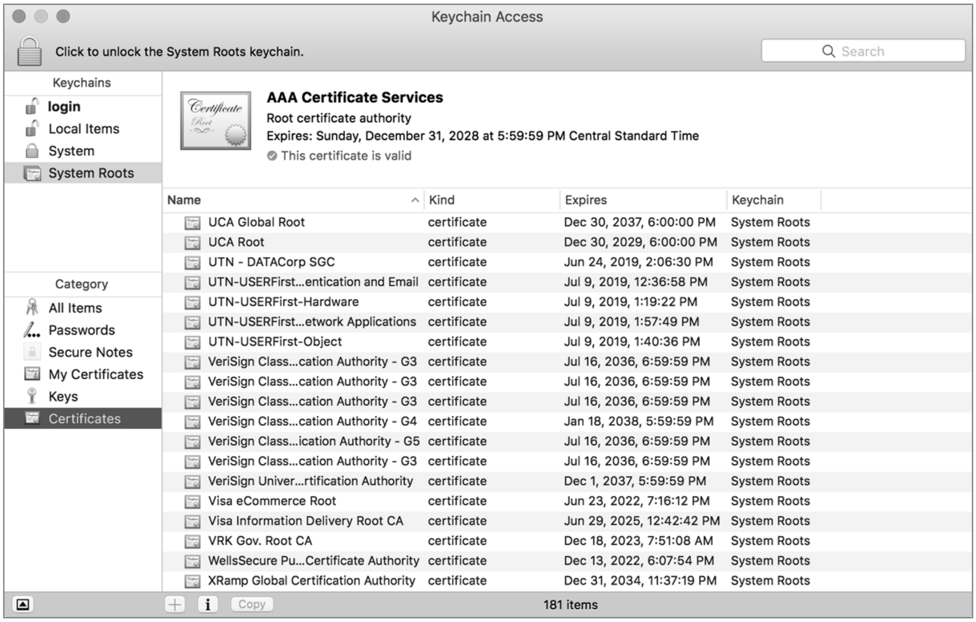
VeriSign Class 3 Public Primary Certification Authority - G5
↳ Symantec Class 3 EV SSL CA - G3
↳ www.apple.com

www.apple.com
Issued by: Symantec Class 3 EV SSL CA - G3
Expires: Sunday, October 15, 2017 at 6:59:59 PM Central Daylight Time
This certificate is valid

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 VeriSign 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*. But how does a device know whether it can trust a CA?

The answer is that trust has to start somewhere. iOS and OS X include a collection of root and intermediate CAs that Apple has determined are worthy of trust out of the box. By extension, your Apple devices also trust any certificate or intermediate CA whose certificate chain ends with one of these CAs.

Although you can't directly inspect the list of root certificates included on iOS devices, you can on an OS X computer from the Keychain Access application. Open Keychain Access (in the Utilities folder). In the upper-left Keychains column, select System Roots. Note that in the following figure the bottom of the window states that, at the time of this writing, there are more than 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	Expires	Keychain
UCA Global Root	certificate	Dec 30, 2037, 6:00:00 PM	System Roots
UCA Root	certificate	Dec 30, 2029, 6:00:00 PM	System Roots
UTN - DATACorp SGC	certificate	Jun 24, 2019, 2:06:30 PM	System Roots
UTN-USERFirst...entication and Email	certificate	Jul 9, 2019, 12:36:58 PM	System Roots
UTN-USERFirst-Hardware	certificate	Jul 9, 2019, 1:19:22 PM	System Roots
UTN-USERFirst...etwork Applications	certificate	Jul 9, 2019, 1:57:49 PM	System Roots
UTN-USERFirst-Object	certificate	Jul 9, 2019, 1:40:36 PM	System Roots
VeriSign Class...cation Authority - G3	certificate	Jul 16, 2036, 6:59:59 PM	System Roots
VeriSign Class...cation Authority - G3	certificate	Jul 16, 2036, 6:59:59 PM	System Roots
VeriSign Class...cation Authority - G3	certificate	Jul 16, 2036, 6:59:59 PM	System Roots
VeriSign Class...cation Authority - G4	certificate	Jan 18, 2038, 5:59:59 PM	System Roots
VeriSign Class...ication Authority - G5	certificate	Jul 16, 2036, 6:59:59 PM	System Roots
VeriSign Class...cation Authority - G3	certificate	Jul 16, 2036, 6:59:59 PM	System Roots
VeriSign Univer...rtification Authority	certificate	Dec 1, 2037, 5:59:59 PM	System Roots
Visa eCommerce Root	certificate	Jun 23, 2022, 7:16:12 PM	System Roots
Visa Information Delivery Root CA	certificate	Jun 29, 2025, 12:42:42 PM	System Roots
VRK Gov. Root CA	certificate	Dec 18, 2023, 7:51:08 AM	System Roots
WellsSecure Pu...Certificate Authority	certificate	Dec 13, 2022, 6:07:54 PM	System Roots
XRamp Global Certification Authority	certificate	Dec 31, 2034, 11:37:19 PM	System Roots

MORE INFO ▸ The Apple PKI website (https://www.apple.com/certificateauthority/) contains more information about the root certificates included with Apple devices. You can also find a complete list of trusted root certificates for iOS in Apple Support article HT204132, "Lists of available trusted root certificates in iOS," and for OS X in article HT202858, "Lists of available trusted root certificates in OS X."

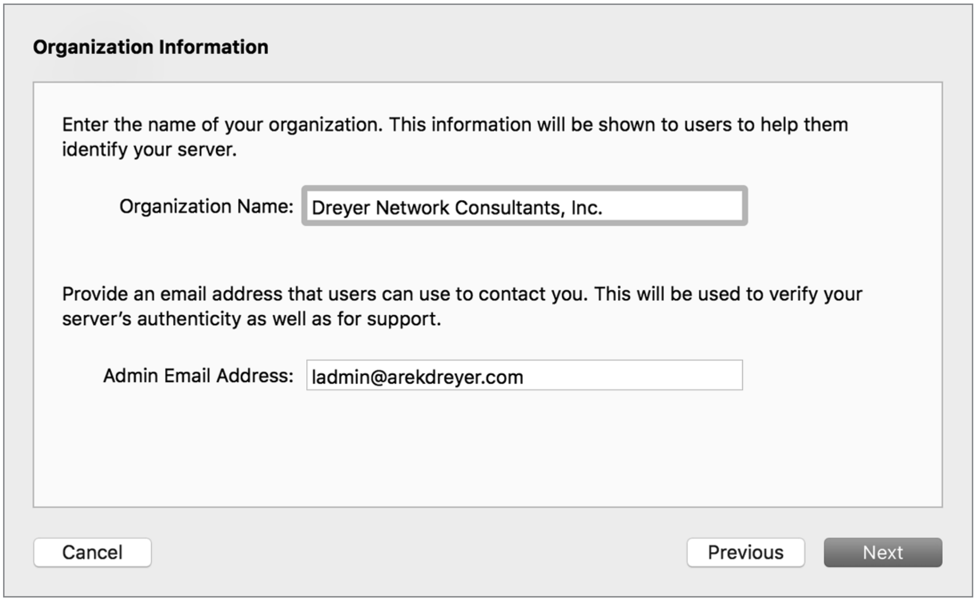
Certificate Signed by an Open Directory CA

Again, any MDM service must use a TLS/SSL certificate signed by a trusted CA. This limits you to one of two choices if using Profile Manager as your MDM service: a certificate signed by a widely trusted CA (as covered in the next section) or a certificate signed by your own local Open Directory CA. Fortunately, OS X Server makes this latter choice an easy option by automatically creating an Open Directory CA and signing your server's TLS/SSL certificate during the creation of an Open Directory master.

NOTE ▸ Creating an Open Directory master is required to enable device management for Profile Manager. In other words, you're probably going to end up with an Open Directory CA even if you don't use it to sign the server's certificate.

NOTE ▸ Make sure your server's host name is properly configured prior to creating an Open Directory master. The Open Directory CA will only automatically sign the certificate with a name that matches the host name of the server.

When creating an Open Directory master from the Server app, Setup Assistant will guide you through several screens. One of the setup screens allows you to enter organizational information. This information will be used to create an Open Directory CA that will then be used to sign an intermediate CA, which is then used to sign your server's TLS/SSL certificate. This process will also create a code-signing certificate that will come in handy for verifying profiles, as covered in Lesson 6, "Configuration and Profiles."



Organization Information

Enter the name of your organization. This information will be shown to users to help them identify your server.

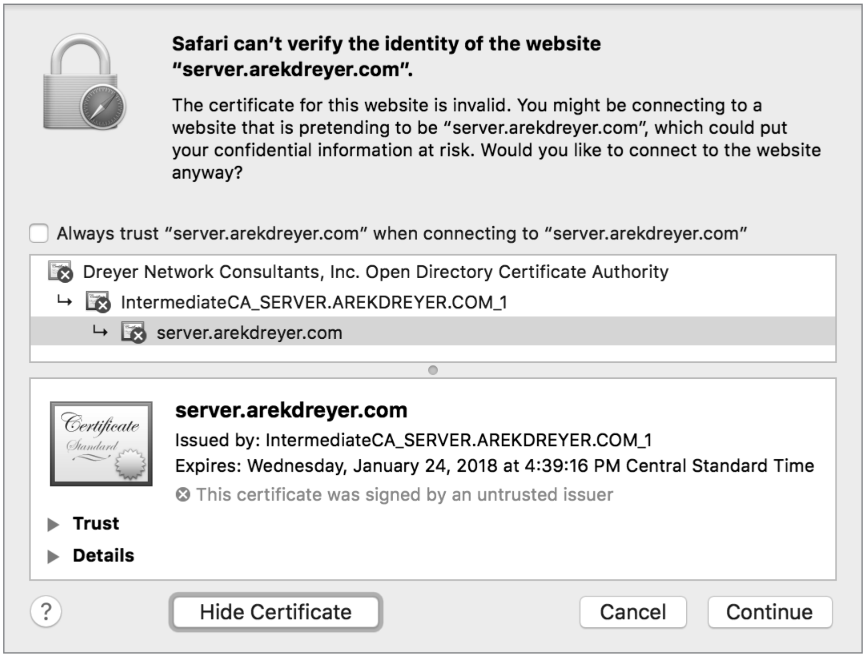
Organization Name: Dreyer Network Consultants, Inc.

Provide an email address that users can use to contact you. This will be used to verify your server's authenticity as well as for support.

Admin Email Address: ladmin@arekdreyer.com

MORE INFO ▸ You can find detailed step-by-step instructions for creating an Open Directory master in the exercises later in this lesson.

Assuming you completed the Open Directory master creation before acquiring other certificates, the Server app will automatically configure all supported services to use the certificate signed by the Open Directory CA. You can verify this by simply navigating to your server's default secure website, https://hostname, where "hostname" is the name of your server. You will still see a default web services page and can inspect the certificate used to protect the site (as of this writing, configuring your server as an Open Directory master starts the Websites service).



Safari can't verify the identity of the website "server.arekdreyer.com".

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

□ Always trust "server.arekdreyer.com" when connecting to "server.arekdreyer.com"

Dreyer Network Consultants, Inc. Open Directory Certificate Authority
↳ IntermediateCA_SERVER.AREKDREYER.COM_1
↳ server.arekdreyer.com

server.arekdreyer.com
Issued by: IntermediateCA_SERVER.AREKDREYER.COM_1
Expires: Wednesday, January 24, 2018 at 4:39:16 PM Central Standard Time
☒ This certificate was signed by an untrusted issuer

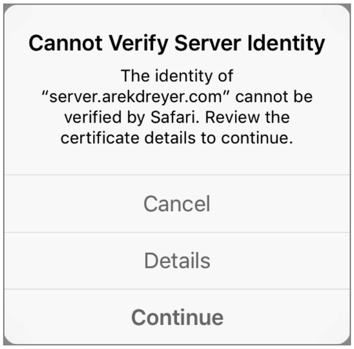
You'll note that even though a chain of trust has been created, you still have the fundamental problem that Apple devices, by default, do not trust your server's Open Directory CA. In a managed environment, you can easily solve this problem by using a trust profile, also covered in Lesson 6, "Configuration and Profiles."

In fact, deploying a trust profile is required for the enrollment of most MDM services, including Profile Manager. Thus, if you or your staff is going to be directly responsible for managing the enrollment of Apple devices, using a certificate signed by the Open Directory CA is a perfectly acceptable solution for most deployments.

Issues with an Untrusted Certificate

In some environments, using a certificate signed by an Open Directory CA is not the recommended solution. For example, your organization may require that all TLS/SSL services use certificates that meet a certain specification or are provided by a specific vendor.

Alternately, if your environment relies upon users self-enrolling their own devices, you don't want the first user experience of your management solution to be a warning message. The following warning message appears on an unmanaged iOS device when connecting for the first time to an MDM service using a certificate signed by an untrusted Open Directory CA:



Cannot Verify Server Identity

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

Not only does this type of warning message make your management solution look sketchy, it means that you (and your users) can't trust any connection made to your management server. In other words, when connecting from an unmanaged device, you will have no way of identifying a legitimate connection to your server from an illegitimate server acting as your server or a server that is attempting a man-in-the-middle attack.

Further, you don't want to establish that it's OK for your users to click Continue when presented with this warning. Quite to the contrary, you should be instructing them that accepting connections to unverified servers is extremely dangerous.

NOTE ▶ You can use a configuration profile to prevent the user of an iOS device from trusting an untrusted TLS certificate.

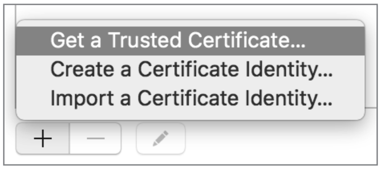
Certificate Signed by a Widely Trusted CA

If you determine that your server needs a certificate signed by a widely trusted CA, the Certificates pane of the Server app provides two main methods for configuration: getting a trusted certificate by generating a certificate-signing request (CSR) or importing an existing certificate identity.

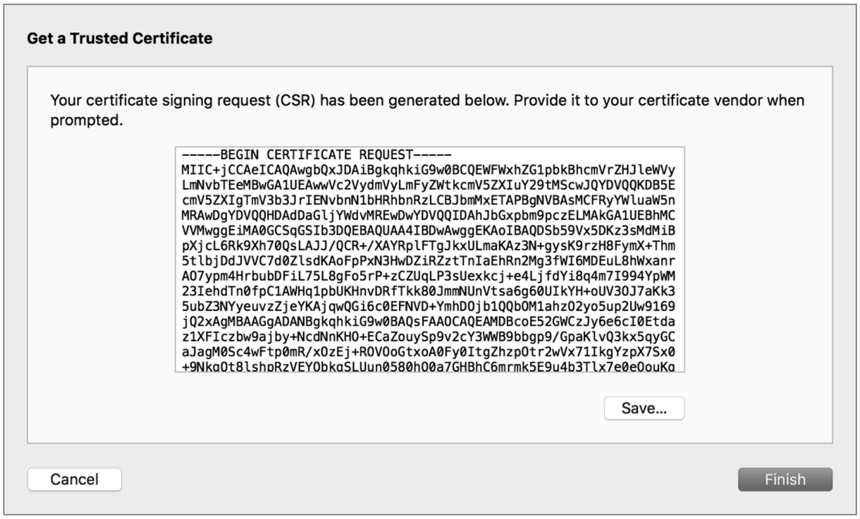
NOTE ▶ At this point, when configuring OS X Server for managing Apple devices, you only need to acquire a standard TLS/SSL certificate, the kind that is commonly used to protect websites. Although a code-signing certificate can be used with an MDM service, it is not required to set up and use the service.

Get a Trusted Certificate

It all starts in the Certificates pane of the Server app; the Add (+) button reveals a pop-up menu.


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

The Get a Trusted Certificate assistant will create a new certificate identity consisting of an unsigned certificate and a private/public key pair. After you enter contact information for the certificate, the system will present a CSR. You will need to copy and paste (or save to a text file) the CSR content. The act of providing a CSR to a CA vendor is the most common method for acquiring a certificate signed by a widely trusted CA.



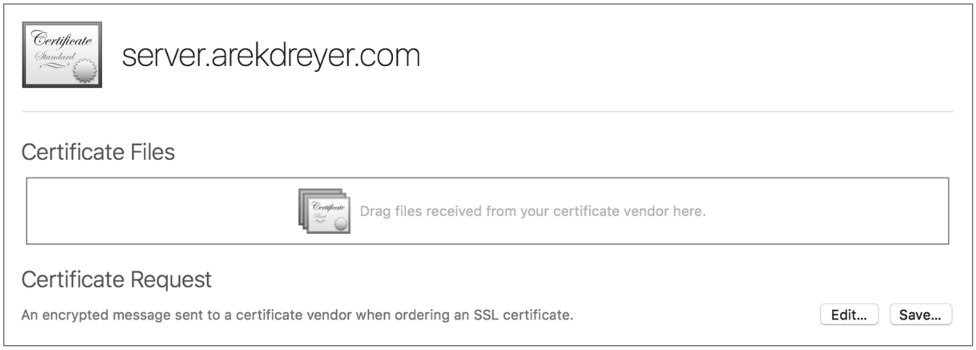
Get a Trusted Certificate

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC+jCCAeICAQAwgbQxJDAiBgkqhkiG9w0BCQEWFWxhZG1pbkBhcmVrZHJleWVy
LmNvbTEeMBwGA1UEAwwVc2VydmVyLmFyZWtkcmV5ZXIuY29tMScwJQYDVQQKDB5E
cmV5ZXIgTmV3b3JrIENvbnN1bHRhbnRzLCBJbmMxETAPBgNVBAsMCFRyYWluaW5n
MRAwDgYDVQQHDAdDaGljYWdvMREwDwYDVQQIDAhJbGxpbm9pczELMAkGA1UEBhMC
VVMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDSb59Vx5DKz3sMdMiB
pXjcL6Rk9Xh70QsLAJJ/QCR+/XAYRplFTgJkxULmaKAz3N+gysK9rzH8FymX+Thm
5tlbjDdJVVC7d0ZlsdKAoFpPxN3HwDZiRZztTnIaEhRn2Mg3fWI6MDEuL8hWxanr
AO7ypm4HrbubDFiL75L8gFo5rP+zCZUqLP3sUexkcj+e4LjfdYi8q4m7I994YpWM
23IehdTn0fpC1AWHq1pbUKHnvDRfTkk80JmmNUnVtsa6g60UIkYH+oUV3OJ7aKk3
5ubZ3NYyeuvzZjeYKAjqwQGi6c0EFNVD+YmhDOjb1QQbOM1ahzO2yo5up2Uw9169
jQ2xAgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEAMDBcoE52GWCzJy6e6cI0Etda
z1XFIczbw9ajby+NcdNnKHO+ECaZouySp9v2cY3WWB9bbgp9/GpaKlvQ3kx5qyGC
aJagM0Sc4wFtp0mR/xOzEj+ROVOoGtxoA0Fy0ItgZhzpOtr2wVx71IkgYzpX7Sx0
+9NkgOt8lshpRzVEYObkgSLUun0580hO0a7GHBhC6mrmk5E9u4b3Tlx7e0eOouKg
```

At this point, you will need to identify a CA vendor. Your organization may already work with a CA vendor, so that will likely be your first choice. Otherwise, the only recommendation is choosing a CA vendor that works with Apple devices. When selecting a CA vendor, an obvious quick test is that an Apple device can establish a secure connection to the vendor's website.

After acquiring a TLS/SSL certificate subscription from a CA vendor, you will need to give the vendor your server's CSR. Most CA vendors will accept the CSR content via a simple paste into a website. After the CA vendor has validated and signed your certificate, the vendor will return it to you as a download. The download will often include the CA vendor's intermediate and root certificates. Double-click the pending certificate in the Server app, and drag all certificates provided by the CA vendor into the appropriate area.



server.arekdreyer.com

Certificate Files

Drag files received from your certificate vendor here.

Certificate Request

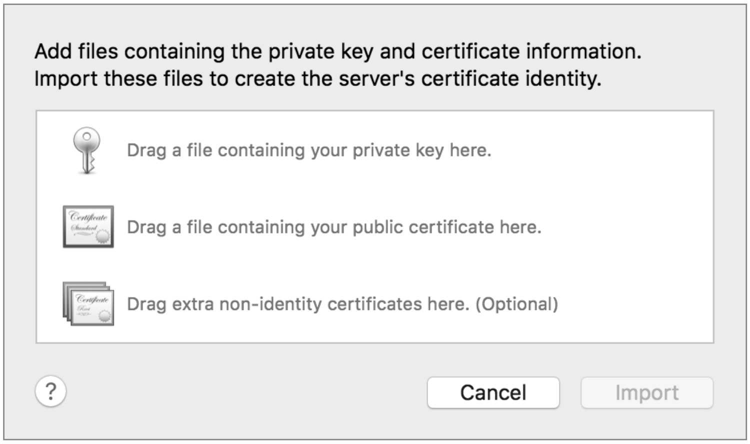
An encrypted message sent to a certificate vendor when ordering an SSL certificate.

Import a Certificate Identity

The Add (+) button reveals a pop-up menu. From this menu, you can select the option to import a certificate identity. This option assumes you already have a valid certificate identity consisting of a signed certificate and a private/public key pair. This is often the case if your organization uses a centralized certificate repository or if your organization has a wildcard certificate that can be used for multiple services. The term *wildcard* means the certificate can be used with any host name inside a specific domain.

If this is the case, someone else has already done all the hard work for you and will provide you with the appropriate certificates and private/public key pair. Transporting a private key in the clear is dangerous, so the key is often stored in an encrypted document. Further, to make certificate identities easier to transport, this encrypted document will also contain all the appropriate certificates. The most common file types are .pfx and .p12, both of which share a similar encrypted format.

The person providing you with the certificate identity will also have to provide you with the encryption key used to protect the document containing the private key. Once you have all the certificate identity documents, simply drag them to the certificate import window in the Server app and then provide the encryption key.



Add files containing the private key and certificate information.
Import these files to create the server's certificate identity.

Drag a file containing your private key here.

Drag a file containing your public certificate here.

Drag extra non-identity certificates here. (Optional)

Exercise 4.1
Prepare Your Mac to Install OS X Server for El Capitan

Prerequisites

- You'll need a Mac computer that is qualified to run OS X Server, that has OS X El Capitan on its startup volume, and that does not yet have OS X Server installed and configured on its startup volume.
- Your own administrator Apple ID or the administrator Apple ID from Exercise 2.2, "Create Apple IDs."
- Even though best practice calls for a PTR DNS record (reverse DNS record) to exist for the IPv4 address of your server computer, the exercises in this guide are written for use in a test network with Bonjour .local names, so there should be no PTR record for the primary IPv4 address of your server.

In this exercise, you will configure your server computer in preparation to install OS X Server on it.

You'll use one of two options to configure a local administrator account, depending on whether you are performing these exercises independently or are in an instructor-led environment with a Mac computer that has already been set up.

In both situations, you'll use System Preferences to configure Network and Sharing preferences. You will also download the student materials that you'll use throughout this class. Finally, you will apply any necessary system software updates.

Challenge

Set up your server computer with a unique computer name. Download the student materials.

Considerations

The exercises in this guide are written so that the individual reader and the student in the instructor-led environment have a similar experience.

In a production environment, it is best practice to use your server's fully qualified domain name. However, to make the exercises possible for those who cannot provide appropriate DNS records to computers and devices on their test network, the exercises in this guide use your server's Bonjour .local name instead of a fully qualified domain name.

Solution

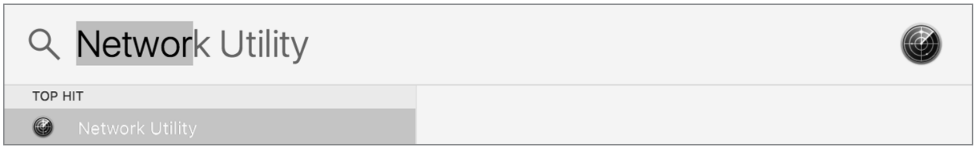
Use Your Client Computer to Confirm Lack of PTR Records

Before you configure your server Mac, use your client Mac to confirm that your DNS service does not provide a PTR record defining a host name for the primary IPv4 address your server will use.

1 On your client Mac, press Command–Space bar (or click the Spotlight icon in the upper-right corner of the screen) to reveal the Spotlight Search field.

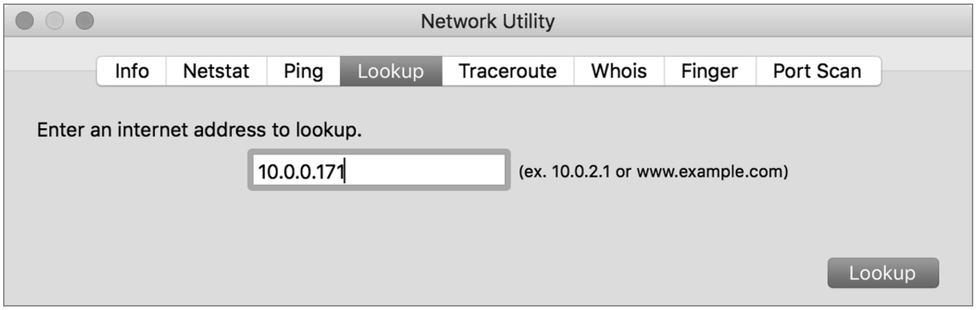
2 In the Spotlight Search field, enter Network Utility.

3 Confirm that Network Utility is listed in the Top Hit section of the search results, and then press Return to open it.



4 Click the Lookup tab.

5 In the “Enter an internet address to lookup” field, enter 10.0.0.*n*1 (where *n* is your student number; for example, student1 uses 10.0.0.11, student 6 uses 10.0.0.61, and student 15 uses 10.0.0.151).

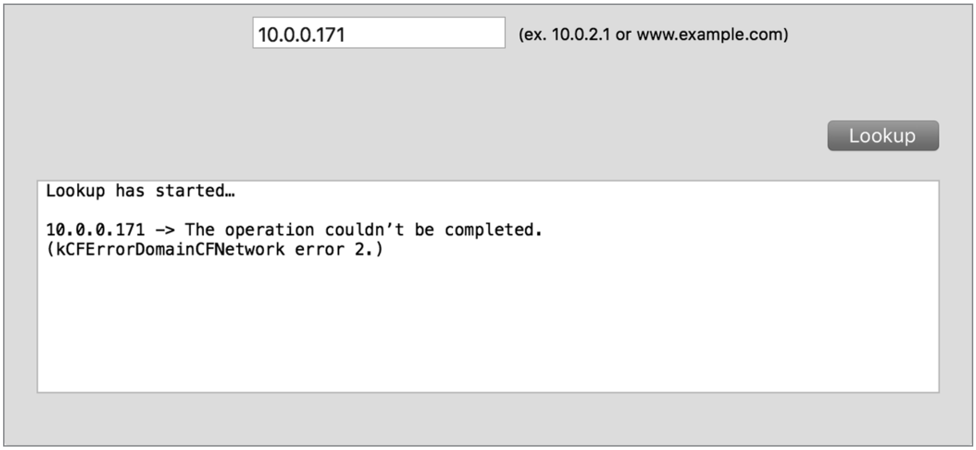


Enter an internet address to lookup.

10.0.0.171 (ex. 10.0.2.1 or www.example.com)

6 Click Lookup.

7 If the result field contains the text “The operation couldn’t be completed,” there is no PTR record for your server’s primary IPv4 address. You can continue with the next section, “Configure OS X on Your Server Computer.”

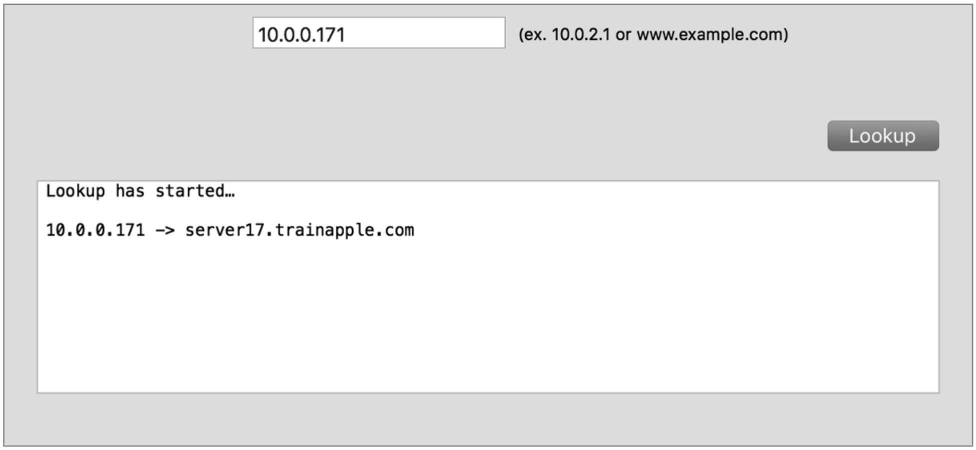


10.0.0.171 (ex. 10.0.2.1 or www.example.com)

```
Lookup has started…

10.0.0.171 -> The operation couldn’t be completed.
(kCFErrorDomainCFNetwork error 2.)
```

8 If the result field contains a DNS name such as "server*n*.trainapple.com" (where *n* is your student number), the DNS server that you are using provides PTR records for your server's primary IPv4 address. In an instructor-led environment, check with your instructor. If you are performing these exercises independently, check your DNS server entries.



```
Lookup has started…

10.0.0.171 -> server17.trainapple.com
```

For best results when you perform the exercises on your test network, the DNS service for your server computer, your client computer, and your iOS device should not provide a PTR record for your server's primary IPv4 address. If the DNS service does provide a PTR record for your server's primary IPv4 address, here are two options you might try before continuing with the exercises in this guide:

- Configure your internal DNS server to not offer a PTR record for your server's primary IPv4 address.

- Configure your test network's DHCP service to use an external DNS service that does not offer a PTR record for your server's primary IPv4 addresses.

After you make one of the suggested changes, perform the previous step 5 again.

If you cannot perform either of the previous options, perform the following to configure your server to use a .local Bonjour name even though there is a PTR record available for its primary IPv4 address:

- After you install OS X Server, select your server in the Server app sidebar, click the Overview tab, click Edit next to the Host Name field, click Next to start Change Host Name Assistant, and select Local Network in the Accessing Your Server pane. Click Next, enter server*n*.local in the Host Name field, and then click Finish.

For experienced administrators, if you must use your server's fully qualified domain name instead of its Bonjour .local name, replace every instance of a Bonjour .local name with your server's fully qualified domain name throughout all the exercises in this guide.

Configure OS X on Your Server Computer

Starting with a fresh installation of OS X is most convenient. If your Mac is at the Welcome pane when you turn it on, you can use the Option 1 section that follows. If you need to use an existing OS X system, skip to Option 2 so your Mac will be configured as expected for the rest of the exercises.

Option 1: Configure OS X on Your Server Computer with Setup Assistant

This option is necessary if your server computer has not already been set up, which is the situation in an instructor-led environment. If you are using a Mac with existing accounts, perform the steps in "Option 2: Configure an Existing OS X System for Your Server Computer" instead.

Ensure that you have OS X El Capitan installed on your server computer. If it isn't already installed, install it now using the App Store, the Recovery HD, or a method specified by your instructor, and then continue when you reach the Welcome pane.

In this section, you'll step through the OS X Setup Assistant for the initial system configuration of your server computer.

1. Ensure that your computer is connected to a valid network connection, unless you plan to use Wi-Fi as your primary network connection.

2. If necessary, turn on the Mac that will run OS X Server.

3. At the Welcome screen, select the appropriate region, and click Continue.

4. Select the appropriate keyboard layout, and click Continue.

   Setup Assistant evaluates your network environment and tries to determine whether you are connected to the Internet. This can take a few moments.

5. If you plan to use Ethernet for your primary network connection and are not asked about your Internet connection, your computer's network settings have already been configured via DHCP, and you may skip to step 8.

If you plan to use Wi-Fi for your primary network connection and are at the Select Your Wi-Fi Network screen, select an appropriate Wi-Fi network, provide the Wi-Fi network's password if necessary, click Continue, and skip to step 8.

6 If you are at the How Do You Connect screen, select Local network (Ethernet), and click Continue.

7 If you are at the Your Internet Connection screen, leave the settings at their defaults, and click Continue.

NOTE ► If no DHCP service is available or your network is not connected to the Internet, you will see the warning message "Your Mac isn't connected to the internet." In this case, click Try Again, configure your router to provide DHCP service, and make sure your network is connected to the Internet. Then click Continue in the Your Internet Connection pane. For advanced users on a network without DHCP, you can set your TCP/IP connection type to Manually, configure settings appropriate for your network, and then click Continue in the Your Internet Connection pane.

8 When asked about transferring information to this Mac, select "Don't transfer any information now," and click Continue.

9 If the Enable Location Services screen appears, select "Enable Location Services on this Mac," and click Continue.

10 At the Sign in with Your Apple ID screen, select "Don't sign in," click Continue, and then click Skip to confirm that you want to skip signing in with an Apple ID.

Note that if you do provide Apple ID credentials, some figures in upcoming exercises may look slightly different, and there may be extra steps. In an instructor-led environment, entering an Apple ID at this time is not recommended.

11 At the Terms and Conditions screen, read the terms and conditions, and click Agree; then in the dialog to confirm that you have read and agree to the OS X software license agreement, click Agree.

Create your local administrator account.

NOTE ► Make sure you create this account as specified here. If you do not, future exercises may not work as written. Highlighted text is used throughout this guide to indicate text you should enter exactly as shown.

1 At the Create Your Computer Account screen, enter the following information:

- Full Name: Local Admin
- Account Name: ladmin
- Password: ladminpw
- (verify field): ladminpw
- Hint: Leave blank.
- Deselect the checkbox “Set time zone based on current location.”

If you are performing the exercises independently and if your server is accessible from the Internet, you can select a more secure password for the Local Admin account. Be sure to remember the password you have chosen because you will need to reenter it periodically as you use this computer.

If you are performing the exercises independently, you may provide a password hint if you want.

If you entered your Apple ID, you can select or deselect the checkbox “Allow my Apple ID to reset this user’s password”; it does not have a major effect on the exercises.

NOTE ▶ In a production environment, always use a strong password.

2 Click Continue to create the local administrator account.

3 At the Select Time Zone screen, click your time zone in the map or choose the nearest location in the Closest City pop-up menu, and then click Continue.

4 At the Diagnostics & Usage screen, leave selected “Send diagnostics & usage data to Apple” and “Share crash data with app developers,” and then click Continue.

Please skip the Option 2 section, and continue at the section “Set the Computer Name.”

Option 2: Configure an Existing OS X System for Your Server Computer

This option is designed only for those who are performing the exercises independently and who have a computer that is already set up with an existing administrator account.

NOTE ▶ You may not use a Mac whose startup volume has already had OS X Server installed.

If your computer has not been set up (that is, if the initial administrator account has not been created), perform the steps in “Option 1: Configure OS X on Your Server Computer with Setup Assistant” instead.

Create a new administrator account in System Preferences.

1. If necessary, log in with your existing administrator account.

2. Open System Preferences.

3. In System Preferences, open Users & Groups.

4. In the lower-left corner, click the lock icon.

5. In the dialog that appears, enter the password for your existing administrator account, and then click Unlock.

6. Click the Add (+) button under the user list.

7. In the dialog that appears, use the following settings:

   NOTE ▶ Make sure you create this account as specified here. If you do not, future exercises may not work as written. If you already have an account named Local Admin or ladmin, you will have to use a different name here and then remember to use your substitute name throughout the rest of the exercises. Highlighted text is used throughout this guide to indicate text you should enter exactly as shown.

- New Account: Choose Administrator.
- Full Name: Local Admin
- Account Name: ladmin

8. If necessary, select “Use separate password.”

9. If your server is not accessible from the Internet, enter ladminpw in the Password and Verify fields.

   If you are performing the exercises independently, you can select a more secure password for the Local Admin account. Be sure to remember the password you have chosen because you will need to reenter it periodically as you use this computer.

   You may provide a password hint if you want.

If you entered your Apple ID, you can select or deselect the checkbox "Allow my Apple ID to reset this user's password"; it does not have a major effect on the exercises.

NOTE ▶ In a production environment, always use a strong password.

10 Click Create User.

11 At the bottom of the user list, click Login Options.

12 If an account is selected for Automatic Login, use the pop-up menu to switch it to Off.

13 Quit System Preferences, and log out.

14 At the login screen, select the Local Admin account, and enter its password (ladminpw, or whatever you specified earlier).

15 Press Return to log in.

This is the end of Option 2; everyone should continue with the next section.

Set the Computer Name

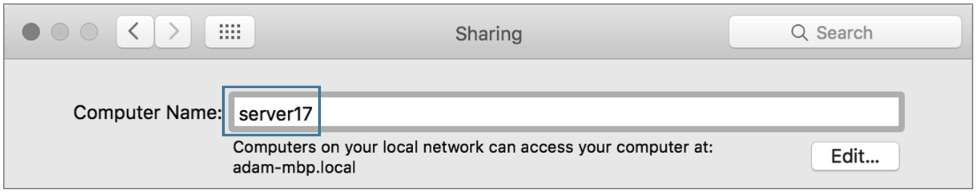
You will specify a computer name associated with your student number. If you are performing the exercises independently, you can choose to skip this section.

1 Open System Preferences.

2 Open Sharing.

3 Set Computer Name to *servern*, replacing *n* with your student number.

For example, if your student number is 17, the computer name should be server17 (all lowercase and no spaces).



Computer Name: server17

Computers on your local network can access your computer at:
adam-mbp.local

4 Press Return.

Notice that the name listed under the Computer Name field, which is the local host name, updates to match your new computer name.

Turn On Remote Management

Enable Remote Management, which will allow the instructor to observe your computer, control your keyboard and mouse, gather information, copy items to your computer, and otherwise help you if necessary.

NOTE ► Even though you know administrator credentials for other students' computers and have the technical ability to remotely control their computers, please do not use that ability to interfere with their classroom experience.

1. Click somewhere over the phrase "Remote Management," but don't select the checkbox yet.

2. For "Allow Access for," select "Only these users."

3. Click the Add (+) button, select Local Admin, and click Select.

4. In the dialog that appears, hold down the Option key while selecting the Observe checkbox, which selects all the checkboxes.

5. Click OK.

6. Select the checkbox Remote Management.

7. Confirm that the Sharing pane displays the text "Remote Management: On" and displays a green status indicator next to the text.

8. Click Show All (looks like a grid) to return to the main System Preferences pane.

Configure Network Interfaces

It is best practice to configure your network settings before you initially install and configure OS X Server. To keep the setup as simple as possible for all situations, for this course your Apple devices will access your server's services via Bonjour, rather than via DNS names.

NOTE ► The exercises are written for only one network interface to be active, but using multiple network interfaces will not significantly impact your ability to complete the exercises.

1 In System Preferences, click Network.

2 In the instructor-led environment, configure your Mac computer's built-in Ethernet port (or its Thunderbolt to Ethernet adapter port) to be the only active network service.

If you are performing the exercises independently, you may leave additional interfaces active, but be aware that this may cause differences between the way the exercises describe the windows and what you actually see.

In the list of network interfaces, select each network interface that you will not use in the exercise (which should be all interfaces except one Ethernet port), click the Action (gear icon) pop-up menu, and choose Make Service Inactive.

3 If you will use multiple network interfaces, click the Action (gear icon) pop-up menu, choose Set Service Order, drag the services to an appropriate order so that your primary interface is at the top of the list, and click OK.

4 Select the network interface you chose earlier in this exercise.

5 Click Advanced.

6 Click the TCP/IP tab.

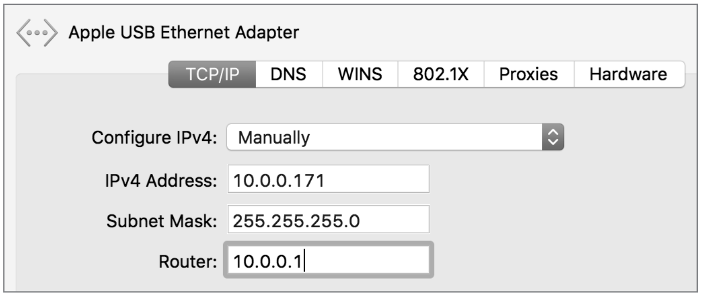
7 In the Configure IPv4 pop-up menu, choose Manually.

8 In the instructor-led environment, enter the following information to manually configure the Ethernet interface (IPv4) for the classroom environment:

IP Address: 10.0.0.*n*1 (where *n* is your student number; for example, student1 uses 10.0.0.11, student 6 uses 10.0.0.61, and student 15 uses 10.0.0.151)

Subnet Mask: 255.255.255.0

Router: 10.0.0.1



Configure IPv4: Manually

IPv4 Address: 10.0.0.171

Subnet Mask: 255.255.255.0

Router: 10.0.0.1

If you are performing the exercises independently and choose to use different network settings, see the "Exercise Setup" section in Lesson 1.

9 Click the DNS tab.

Even though you just switched Configure IPv4 from DHCP to Manually, you did not yet apply the change. Values assigned by DHCP are listed, but once you click Apply, those values will not remain unless you deliberately add them.

10 In the DNS Servers field, click Add (+).

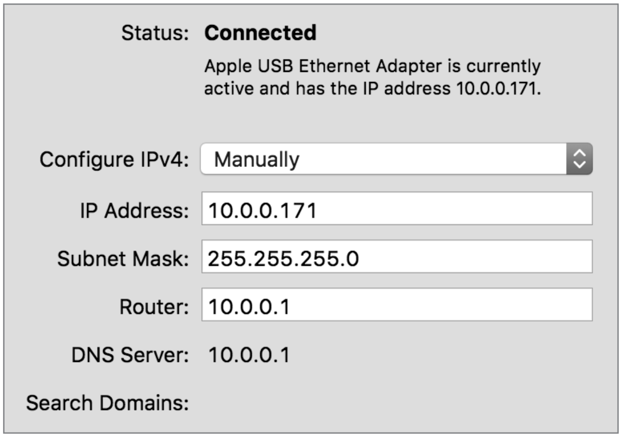
11 In the instructor-led environment, enter 10.0.0.1.

If you are performing the exercises independently, enter the value or values appropriate for your environment.

12 If there are any other values in the DNS Servers field, select another value, and then click Delete (-) to delete the value; do this until 10.0.0.1 (or your desired values if you are performing the exercises independently) is the only value in the DNS Servers field.

13 Click OK to save the change and return to the list of network interfaces.

14 Review the settings, and then click Apply to accept the network configuration.



Status: **Connected**
Apple USB Ethernet Adapter is currently active and has the IP address 10.0.0.171.

Configure IPv4: Manually
IP Address: 10.0.0.171
Subnet Mask: 255.255.255.0
Router: 10.0.0.1
DNS Server: 10.0.0.1
Search Domains:

15 Click Show All (looks like a grid) to return to the main System Preferences pane.

Update Software

To take advantage of possible fixes and improvements, be sure that you're running the most recent version of OS X. If a local Caching service is available, your Mac will automatically use it.

1 While still in System Preferences, open App Store preferences.

2 Select the checkbox "Install app updates."

3 Select the checkbox "Install OS X updates."

4 If the button at the bottom of the window is Check Now, click Check Now.

If the button at the bottom of the window is Show Updates, click Show Updates.

5 If you are in an instructor-led environment, ask your instructor what updates are appropriate to install; otherwise, if there are any updates, click Update All.

If there are no updates available, press Command-Q to quit the App Store, quit System Preferences, skip the rest of this section, and continue with the section "Download the Student Materials."

6 If the "Some updates need to finish downloading before they are installed" dialog appears, click Download & Restart.

If the Restarting Your Computer notification appears, click Restart; after your Mac restarts, you will be automatically logged back in.

7 Quit the App Store.

8 Quit System Preferences.

Download the Student Materials

Some files are necessary for the completion of some of the exercises. You have already downloaded them to your client computer, but you should also have them available on your server computer. If you are in an instructor-led environment, you can use the Option 1 section that follows. Otherwise, skip to Option 2.

Option 1: Download the Student Materials in the Instructor-Led Environment

If you are performing the exercises independently, skip to "Option 2: Download the Student Materials for the Independent Reader."

If you are in an instructor-led environment, you will connect to the classroom server and download the student materials used for the course. To copy the files, you'll drag the folder to your Documents folder.

1 In the Finder, choose File > New Finder Window (or press Command-N).

2 In the Finder window sidebar, click mainserver.

  If Mainserver does not appear in the Finder sidebar, in the Shared list, click All, and then double-click the mainserver icon in the Finder window.

  Because mainserver allows guest access, your client computer logs in automatically as Guest and displays the available share points.

3 Open the Public folder.

4 Drag the StudentMaterials folder to the Documents folder in the sidebar.

5 Once the copy is complete, disconnect from mainserver by clicking Eject next to the Mainserver listing.

Skip the Option 2 section that follows, and resume with the section "Install the Server App."

Option 2: Download the Student Materials for the Independent Reader

If you are in the instructor-led environment, skip this section.

If you are performing the exercises independently, copy the student materials from your client or download the materials from Peachpit's site, and place them in your Documents folder.

If both of your Mac systems have AirDrop enabled, you can use AirDrop to copy the StudentMaterials folder from your client to your server computer. Click AirDrop in a Finder window on each Mac. On your client computer, open a new Finder window, open your Documents folder, drag the StudentMaterials folder to the picture for your server computer in the AirDrop window, and then click Send. On your server computer, click Save. When the transfer has completed, open the Downloads folder, and drag StudentMaterials to your Documents folder in the Finder window sidebar. Finally, close the AirDrop window on your client computer and on your server computer.

Another option is to use a removable disk. If you have a USB, FireWire, or Thunderbolt disk, you can connect it to your client, copy the StudentMaterials folder from your local administrator's Documents folder to the volume, eject the volume, connect the volume to your server computer, and drag the StudentMaterials folder to your Documents folder in the Finder window sidebar.

Alternatively, you can download the files from Peachpit again using the following steps:

> **NOTE ▶** You registered this guide for the lesson files in Exercise 2.1, "Configure Your Client Mac." If you have not already done so, see the section "Option 2: Download the Student Materials for the Independent Reader" in that exercise for details.

1. Using Safari, open www.peachpit.com, and click the Account link or Account Sign In link at the top right of the home page to access your Peachpit account.

2. Click the Registered Products tab and locate Managing Apple Devices: Deploying and Maintaining iOS 9 and OS X El Capitan Devices.

3. Click the Access Bonus Content link to access the student materials.

4. Click the Student Materials link to download the appropriate files to the Downloads folder (or whichever location you have selected in Safari Preferences) on your computer.

5. In the Finder, choose File > New Finder Window (or press Command-N).

6. Choose Go > Downloads.

7. Double-click the StudentMaterials.zip file to decompress the file.

8. Drag the StudentMaterials folder from your Downloads folder to your Documents folder in the Finder window sidebar. If you want, you can also place StudentMaterials in your Dock for easy access.

9. Drag the StudentMaterials.zip file from your Downloads folder to the Trash in the Dock if necessary.

In this exercise, you used System Preferences and the Finder to configure OS X on your server computer in preparation to install OS X Server.

Exercise 4.2
Install OS X Server for El Capitan

Prerequisite

- Exercise 4.1, "Prepare Your Mac to Install OS X Server for El Capitan"

Challenge

Now that you have OS X configured on your server computer, install OS X Server on your server computer and configure it so you can administer it remotely.

Considerations

Your server computer isn't a server until you run and configure the Server app.

If you are a member of the Mac Developer Program or iOS Developer Program (available at https://developer.apple.com), you may obtain a free redemption code for OS X Server.

Solution

Install Server

In a production environment, it's recommended to download the latest version of OS X Server from the App Store.

> **TIP** If you've already purchased OS X Server, you must use the same Apple ID used for the original purchase to avoid being charged again.

If you are in an instructor-led environment, use the Option 1 section that follows. Otherwise, you should skip to Option 2.

Option 1: In the Instructor-Led Environment, Copy Server

In the instructor-led environment, the classroom server has the Server app available in the StudentMaterials folder; move the Server app to the Applications folder on your server computer with the following steps:

1. In the Finder on your server computer, open a new Finder window, click Documents in the sidebar, open the StudentMaterials folder you downloaded, and then open the Lesson4 folder.

2. Drag the Server app into the Applications folder in the sidebar.

Please skip the Option 2 section, and continue at the “Open Server” section that follows.

Option 2: For the Independent Reader, Download or Purchase Server in the App Store

If you are performing the exercises independently, use your own administrator Apple ID or the administrator Apple ID from Exercise 2.2, “Create Apple IDs,” to purchase or redeem a code for OS X Server from the App Store. This automatically places the Server app in your Applications folder. If you have already purchased the Server app, download it again from the Purchased tab in the App Store. If you have the Server app available on a removable volume, drag the Server app from your removable volume into your Applications folder.

Open Server

Once you have the Server app installed in the Applications folder, open the Server app.

1. In your Dock, click Launchpad.

2. You may need to swipe to the next page in Launchpad to see the Server app (hold down the Command key and press the Right Arrow key, or if you have a trackpad, swipe to the left with two fingers to get to the next page in Launchpad).

3. Click Server to open the Server app.

4. Keep the Server app in the Dock. Click and hold Server in the Dock, and then choose Options > Keep in Dock from the menu that appears.

5 In the “To set up OS X Server on this Mac, click Continue” pane, click Continue.

6 Read and agree to the terms of the software license agreement.

7 Ensure that “Use Apple services to determine this server’s Internet reachability” is selected, and click Agree.

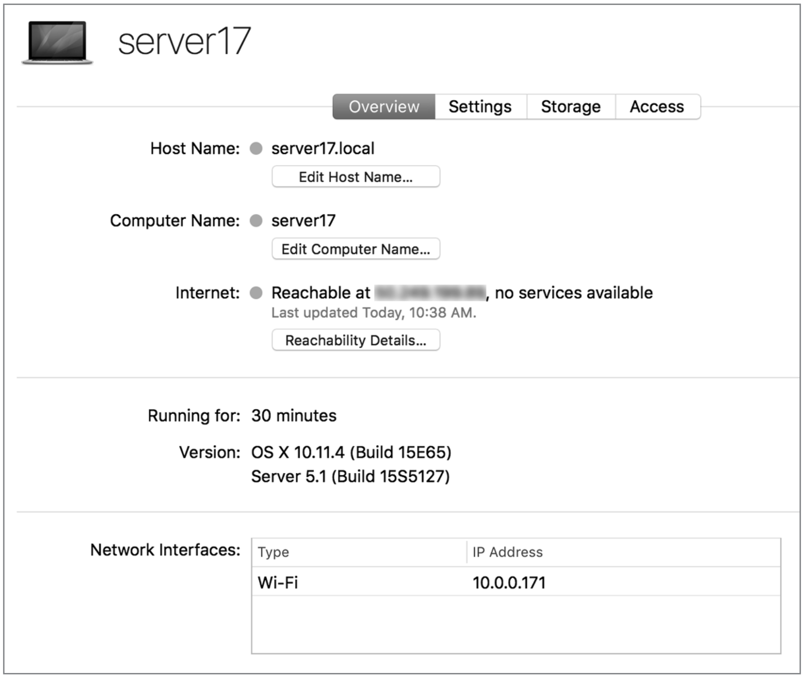
8 Provide local administrator credentials (User Name: Local Admin, Administrator Password: ladminpw), and click Allow.

9 Wait while OS X Server for El Capitan configures itself.

10 Close the Server Tutorials window.

After its initial installation, the Server app displays the Overview tab in the Server pane.

NOTE ► The public IPv4 address in the following figure is obscured intentionally.



Host Name: ● server17.local

Computer Name: ● server17

Internet: ● Reachable at [redacted], no services available
Last updated Today, 10:38 AM.

Running for: 30 minutes

Version: OS X 10.11.4 (Build 15E65)
Server 5.1 (Build 15S5127)

Network Interfaces:

Type	IP Address
Wi-Fi	10.0.0.171

You have successfully installed OS X Server.

Configure Your Server to Allow Remote Access via the Server App

Configure your server so that you can administer it with the Server app on your client computer.

1 In the Server app, click the Settings tab.

2 Select the checkbox "Using Server app on a remote Mac."

It's recommended that you administer your server with only one instance of the Server app at a time; if you have the Server app open while logged in on your server, quit the Server app before opening the Server app on your client computer.

In this exercise, you used the Server app to configure your server with OS X Server, and you turned on remote access using the Server app.

Exercise 4.3
Configure OS X Server for El Capitan

Prerequisites

- Exercise 4.2, "Install OS X Server for El Capitan"
- Text files from the student materials, which you obtained as part of Exercise 4.1, "Prepare Your Mac to Install OS X Server for El Capitan"

Challenge

Configure Apple Push Notifications. Configure and start services you will use for the rest of the course:

- Open Directory, including importing users and groups
- Mail
- Calendar
- Contacts
- Wiki

Considerations

In the Server app's list of services, Open Directory is hidden by default in a section of advanced services. The downloadable student materials contain user import files with eight users and a group import file with two groups.

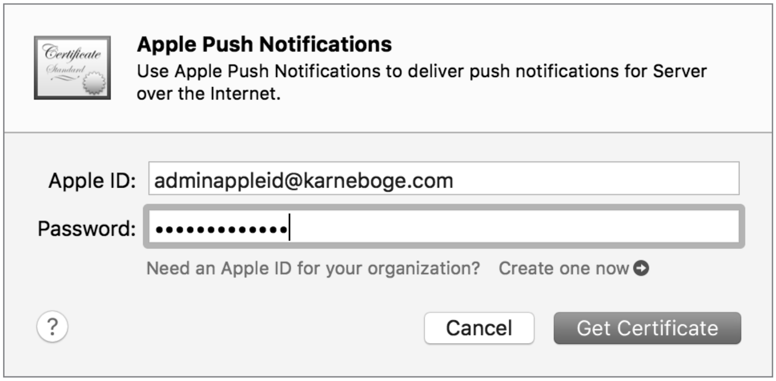
Solution

Enable Apple Push Notifications

1 If necessary, open the Server app, authenticate to your server, select your server in the Server app sidebar, and then click the Settings tab.

2 If the Apple Push Notifications (APN) checkbox is not already selected, select it now.

3 Enter your administrator Apple ID credentials.

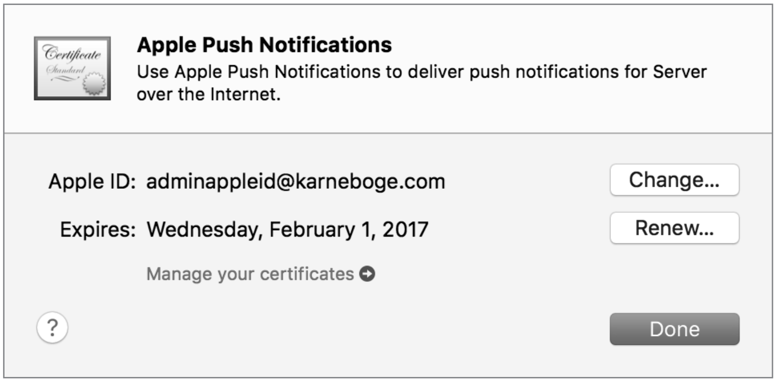


Apple Push Notifications
Use Apple Push Notifications to deliver push notifications for Server over the Internet.

Apple ID: adminappleid@karneboge.com
Password: •••••••••••••

4 Click Get Certificate.

5 After the Server app successfully creates and processes the Apple Push Notification service certificates and displays their shared expiration date, click Done.



Apple Push Notifications
Use Apple Push Notifications to deliver push notifications for Server over the Internet.

Apple ID: adminappleid@karneboge.com

Expires: Wednesday, February 1, 2017

Configure Your Server as an Open Directory Master

In a production environment, you would definitely confirm or verify DNS records before configuring your server as an Open Directory master. However, because this environment uses Bonjour names, you can skip the usual DNS verification step.

1 If the Server app does not display the list of advanced services, hover the pointer above "Advanced" in the sidebar, and then click Show.

2 Click Open Directory.

3 Click the On/Off switch to turn on the Open Directory service.

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

5 Configure a password; you can leave the "Remember this password in my keychain" option selected.

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

Of course, in a production environment, you should use a secure password.

6 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: MDM Project *n* (where *n* is your student number)
- Admin Email Address: ladmin@server*n*.local (where *n* is your student number)

7 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.

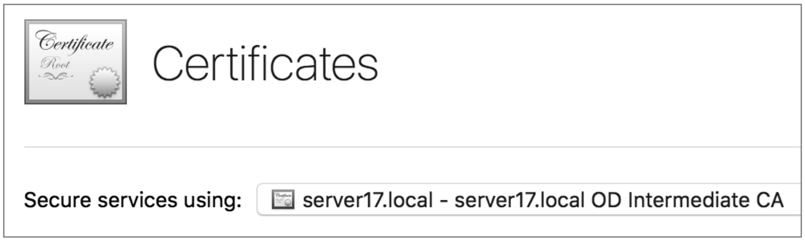
When the configuration is complete, the Server app displays the Servers section of the Open Directory pane, with your server listed as the master. It also displays any additional IPv4 addresses your Mac has in addition to your server's primary IPv4 address (such as Wi-Fi).

Inspect the SSL Configuration

One of the benefits of configuring your server to be an Open Directory master is that it automatically creates a code-signing certificate for Profile Manager to use. Use the following steps to inspect your server's Secure Sockets Layer configuration:

1 In the Server app sidebar, select Certificates.

Note that all the services are set to use the same certificate: server*n*.local certificate (where *n* is your student number), which is signed by your server's OD intermediate CA.



Certificates

Secure services using: server17.local - server17.local OD Intermediate CA

2 Double-click the server*n*.local certificate (where *n* is your student number).

3 Inspect the details of the certificate.

4 Scroll to the end of the certificate information, and note that Purpose is Server Authentication.

Note the Renew button for the certificate. When the renewal date approaches, the Server app automatically generates an expiration alert for the certificate, and the alert offers a Renew button. You don't have to wait for the alert; you can use this button to renew the certificate at any time.

5 Click OK to return to the list of certificates.

6 Double-click Code Signing Certificate.

7 Scroll to the end of the certificate information, and note that Purpose is Code Signing.

8 Click OK to return to the list of certificates.

Import Users into Your Server's Shared Directory Node

To expedite the exercise, in the StudentMaterials folder is a text file with user accounts. This import file defines these users with a "net" password. Of course, in a production environment, each user should have a unique password or passphrase that is secret and secure.

Import the accounts into your server's shared directory node.

1 In the Server app sidebar, select Users.

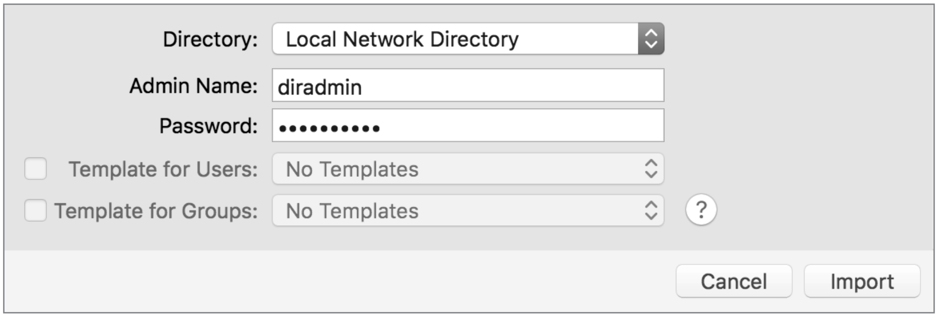
2 Click the Action (gear icon) pop-up menu, and choose Import Users.

3 In the sidebar, click Documents. Open StudentMaterials, and then open the Lesson4 folder.

4 Select the users.txt file.

5 Click the Directory pop-up menu, and choose Local Network Directory.

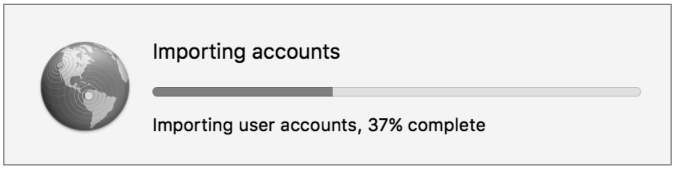
6 If directory administrator credentials are not automatically provided thanks to the keychain item, provide directory administrator credentials in the Admin Name and Password fields.



Directory: Local Network Directory
Admin Name: diradmin
Password: •••••••••••
□ Template for Users: No Templates
□ Template for Groups: No Templates

7 Click Import.

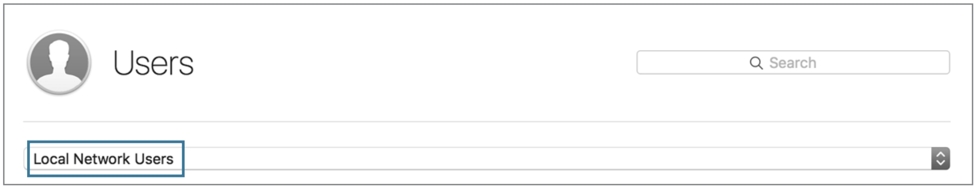
8 At the “Importing users and groups may take several minutes. Are you sure you want to continue?” dialog, click Continue.



Importing accounts

Importing user accounts, 37% complete

9 After the import has completed, select Local Network Users from the pop-up menu, and confirm that there are eight new local network users.



NOTE ▶ If any of the users are listed as Limited or No Access, after the import has completed, choose View > Refresh.

You now have added eight local network user accounts.

Import Groups into Your Server’s Shared Directory Node

To expedite the exercise, you have two import files: one that defines some of the imported users as members of the Marketing group and another that defines users as members of the Engineering group.

1 In the Server app sidebar, select Groups.

2 Click the Action (gear icon) pop-up menu, and choose Import Groups.

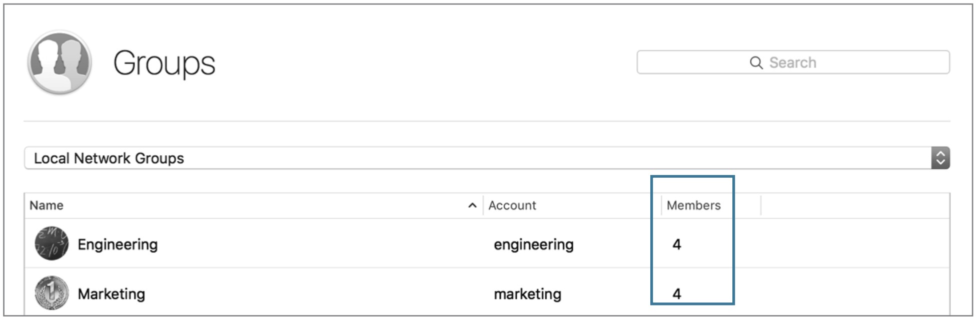
3 If necessary, in the sidebar, click Documents. Open StudentMaterials, and then open the Lesson4 folder.

4 If necessary, select Local Network Directory from the Directory pop-up menu, and provide directory administrator credentials in the Admin Name and Password fields.

5 Double-click the groups.txt file to start importing the file.

6 At the “Importing users and groups may take several minutes. Are you sure you want to continue?” dialog, click Continue.

7 After the import has completed, select Local Network Groups from the pop-up menu, and confirm that there are two new local network groups, each containing four members.



Groups

Search

Local Network Groups

Name	Account	Members
Engineering	engineering	4
Marketing	marketing	4

You now have two new local network groups populated with the local network users you previously imported.

Configure and Start the Mail Service

Once you’ve configured the Mail service, you can use it in other parts of this guide for configuration profile examples and to mail VPP notification invitations. This is not a production server, so to expedite the setup, you will disable virus and junk mail filtering.

1 In the Server app sidebar, select Mail.

2 Click Filtering Settings.

3 Deselect the “Enable virus filtering” checkbox.

4 Deselect the “Enable junk mail filtering” checkbox.

5 Click OK to close the Mail Filtering pane.

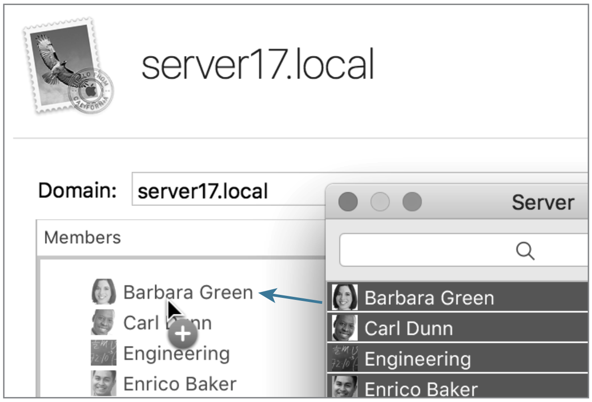
6 Under the Domains field, click the Add (+) button.

7 In the Domain field, enter server*n*.local (where *n* is your student number).

8 Press Command-B to display the accounts browser window.

9 Select an account in the accounts browser, and then press Command-A to select all users and groups.

10 Drag the accounts to the field that lists the Members and Email columns.



server17.local

Domain: server17.local

Members

Barbara Green
Carl Dunn
Engineering
Enrico Baker

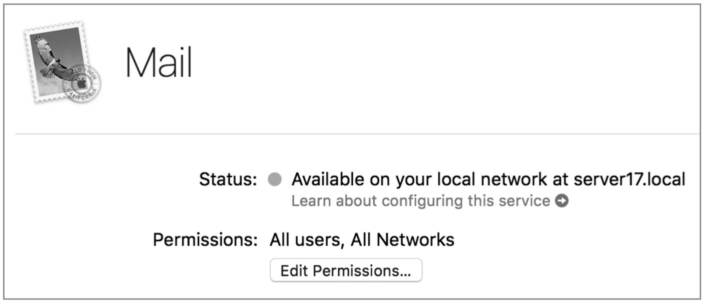
Barbara Green
Carl Dunn
Engineering
Enrico Baker

11 Press Command-B to hide the accounts browser window.

12 Click Create.

13 Click the On/Off switch to start the Mail service.

14 Wait for the Mail service to become available (green status indicator in the Status field).



Mail

Status: ● Available on your local network at server17.local
Learn about configuring this service

Permissions: All users, All Networks

Verify the Mail Service

1 Open Mail on either your server Mac or your client Mac.

2 In the "Choose a Mail account provider" pane, select Other Mail Account, and click Continue.

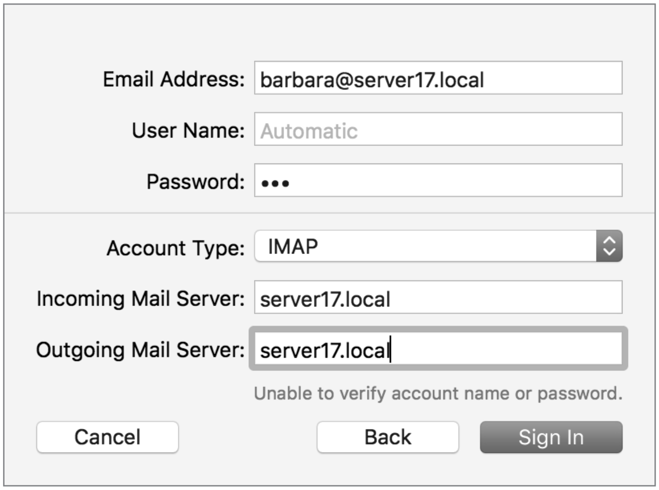
3 In the Add a Mail Account pane, confirm that the import file includes an email address for your server, for example:

- Name: Barbara Green
- Email Address: barbara@server*n*.local (where *n* is your student number)
- Password: net

4 Click Sign In. The pane will display the message "Unable to verify account name or password."

5 In the Incoming Mail Server and Outgoing Mail Server fields, enter server*n*.local (where *n* is your student number).

The User Name and Password fields should already be populated.



Email Address: barbara@server17.local

User Name: Automatic

Password: •••

Account Type: IMAP

Incoming Mail Server: server17.local

Outgoing Mail Server: server17.local

Unable to verify account name or password.

6 Click Sign In.

7 If you see the Verify Certificate window, click Show Certificate, select the "Always trust" checkbox, and click Connect.

8 If necessary, enter the local administrator credentials, and then click Update Settings.

9 In the "Select the apps you want to use with this account" pane, deselect Notes, and click Done.

Send and Receive a Test Message

1. Choose File > New Message.

2. In the To field, enter barbara@server*n*.local (where *n* is your student number).

3. Enter Test Message in the Subject field.

4. Enter some text in the main body field.

5. Click the Send button in the upper-left corner of the message.

6. Confirm that the message is delivered. If necessary, choose Window > Message Viewer.

7. Quit Mail.

Turn On the Calendar Service

To have another service available for the Settings for Everyone configuration profile, you can turn on the Calendar service.

1. In the Server app sidebar, select Calendar.

2. Click the On/Off switch to start the service.

   You can leave all the settings at their defaults.

Turn On the Contacts Service

Using the Contacts service allows you to quickly look up information, such as email addresses, for the users hosted by your server.

1. In the Server app sidebar, select Contacts.

2. Select the checkbox "Allow users to search the directory using the Contacts application."

3. Click the On/Off switch to start the service.

   You can leave all the other settings at their defaults.

Turn On the Wiki Service

By default, the Wiki service allows iOS users to edit files on the wiki using iWork.

1. In the Server app sidebar, select Wiki.
2. Click the On/Off switch to start the service.

   You can leave all the other settings at their defaults.
3. Quit Server.

In this exercise, you turned on Apple Push Notifications on your server computer, configured the server as an Open Directory master, imported users and groups, and turned on a few key services.

Exercise 4.4
Configure Server on Your Client Computer (Optional)

Prerequisites

- Exercise 4.3, "Configure OS X Server for El Capitan"
- Text files from the student materials, which you obtained as part of Exercise 4.1, "Prepare Your Mac to Install OS X Server for El Capitan"

Challenge

Install the Server app on your client computer, and prepare it to remotely administer your server computer.

Considerations

Your server does not allow remote administration by default.

If you attempt to remotely administer your server, you will get a message that your client computer does not trust the identity of the SSL certificate used by the server.

Solution

Install the Server App

On your server computer, you ran the Server app to configure your server computer as a server. However, on your client computer, you can run the Server app to remotely administer your server.

Option 1: In the Instructor-Led Environment, Copy the Server App

In the instructor-led environment, the classroom server has the Server app available in the StudentMaterials folder; move the Server app to the Applications folder on your client Mac with the following steps:

1. In the Finder on your client Mac, open a new Finder window, click Documents in the sidebar, open the StudentMaterials folder you downloaded, and then open the Lesson4 folder.
2. Drag the Server app into the Applications folder in the Finder window sidebar.

Option 2: For the Independent Reader, Download or Purchase OS X Server in the App Store

If you are performing the exercises independently, you should have already purchased OS X Server by the time you completed Exercise 4.1. If this is the case, open the App Store from the Dock or from Recent Items under the Apple menu, sign in with the Apple ID you used to purchase OS X Server, and download OS X Server, which automatically places the Server app in your Applications folder. If you have already purchased the Server app and have it available on a removable volume, drag the Server app from your removable volume into your Applications folder.

Use the Server App to Administer Your Server

Using your client computer, open the Server app, connect to your server, and accept its SSL certificate.

1. On your client computer, open the Server app.

   NOTE ► Do not click Continue; otherwise, you will configure your client Mac to be a server.

2 Click and hold Server in the Dock, and then choose Options > Keep in Dock from the menu that appears.

3 Click Other Mac.

4 In the Choose a Mac window, select your server, and click Continue.

5 Provide the administrator credentials (Administrator Name: ladmin, Administrator Password: ladminpw).

6 Select the "Remember this password in my keychain" checkbox so the credentials you provide will be saved in your keychain (a secure store of passwords) and so you will not need to provide credentials again.

7 Click Connect.

Because your server is using a self-signed SSL certificate that has not been signed by a certificate authority your client computer is configured to trust, you'll see a warning message that you are connecting to a server whose identity certificate is not verified.

NOTE ► In a production environment, you might want to address this situation as soon as possible by using Keychain Access on your server computer to configure your server to use a valid SSL certificate for the com.apple.servermgrd identity, which is used to communicate with a remote instance of the Server app. This is outside the scope of this guide.

8 Click Show Certificate.

9 Select the checkbox to always trust com.apple.servermgrd when connecting to your server.

10 Click Continue.

11 You must provide your login credentials to modify your keychain.

Enter your password (ladminpw), and click Update Settings.

After you click Update Settings, the Server app connects to your server.

12 Quit Server.

In this optional exercise, you configured your client computer to remotely configure your server with the Server app.

This page intentionally left blank

Index