Apple Device Management

A Unified Theory of Managing Macs, iPads, iPhones, and Apple TVs

Second Edition

Charles Edge
Rich Trouton

Apress®

Apple Device Management

A Unified Theory of Managing Macs, iPads, iPhones, and Apple TVs

Second Edition

Charles Edge
Rich Trouton

Apress®

Apple Device Management: A Unified Theory of Managing Macs, iPads, iPhones, and Apple TVs

Charles Edge
Minneapolis, MN, USA

Rich Trouton
Middletown, MD, USA

ISBN-13 (pbk): 978-1-4842-9155-9
ISBN-13 (electronic): 978-1-4842-9156-6
https://doi.org/10.1007/978-1-4842-9156-6

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: James Markham
Coordinating Editor: Jessica Vakili

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 NY Plaza, New York, NY 10004. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on the Github repository: https://github.com/Apress/Apple-Device-Management. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

Table of Contents

About the Authors

Charles Edge is the Chief Technology Officer of venture capital firm Bootstrappers.mn. He holds 30 years of experience as a developer, administrator, network architect, product manager, and CTO. He built the team that developed an Apple-focused MDM and has code-level experience with security and cryptography on the Apple platforms. He is the author of 20+ books and more than 6000 blog posts on technology and has served as an editor and author for many publications. Charles also serves on the board of multiple companies and conferences and frequently speaks at industry conferences around the world, including DefCon, BlackHat, LinuxWorld, the Apple Worldwide Developers Conference, and a number of Apple-focused conferences. Charles is also the author of krypted.com and a cohost of the Mac Admins Podcast and the History of Computing Podcast.

Rich Trouton has been doing Macintosh system and server administration for 20 years and has supported Macs in a number of different environments, including university, government, medical research, advertising, and enterprise software development. His current position is at SAP, where he works with the rest of the Apple CoE team to support SAP's Apple community.

About the Technical Reviewer

Ahmed Bakir is a career iOS developer, entrepreneur, and educator. He is the author of three books on iOS development, including *Program the Internet of Things with Swift for iOS*, which ranked #3 on Amazon. In 2009, he started his consulting business, devAtelier, where he worked on mobile apps for a wide range of clients ranging from startups to Fortune 500 companies. He has been a senior or lead developer on over 20 apps, including ones for major brands like UNIQLO and KFC. In 2015, he developed and taught a mobile programming certificate program for the University of California San Diego's extension program. Ahmed is currently building cool stuff in Tokyo! You can find him online at `www.devatelier.com`.

Preface

Apple distributed 25 releases of the Mac operating system across 35 years. Then came iPhone, iPad, Apple TV, a watch, and a HomePod. The success of the iPhone and the unique challenges to manage mobile devices mean that new paradigms in device management had to be established. This meant the world of managing Apple devices had to change. That evolution was inevitable, from the second the iPhone sales doubled those of the Mac, and has only gotten more and more clear.

That evolution in device management is now undeniable and irreversible. The end result of that evolution is a fate not yet determined. But change is afoot. This book is meant to codify those changes and identify best practices.

Who This Book Is For

Simply put, this book is for administrators of organizations that want to integrate with the new Apple. Many organizations have started building what's next. And many complain about aspects of how they have to build out infrastructure and services. But the world's most valuable company has shown no desire to allow exceptions.

This book outlines what organizations need to achieve work effectively with the Apple platform and includes not only infrastructure but a mode of thinking that you have to adopt to find success, a mode of thinking that forces you to leave 30 years of IT dogma at the door. And you can feel free to complain, but the faster you embrace, the faster you find success with the platform.

This book is here to help you embrace the new style of management. Because it's not going anywhere.

Chapters at a Glance

This book provides guidance. This guidance is split up into a number of chapters that provide insights for each larger theme of Apple device management. Most will go through the philosophy and design of the Apple device management story. Unless specified in the title, we work to unify that management story across the operating systems, covering iOS, macOS, and tvOS, noting the differences within each chapter.

Chapter 1: The Evolution of Apple Device Management

How did we get here? It helps to understand the history of how Apple management has evolved in the past 20+ years. Understanding where we have come from should make you more accepting of Apple's choices and help you better understand where Apple, third-party software vendors, and the IT community are taking us. Chapter 1 provides the background to get us started.

Chapter 2: Agent-Based Management

There is no such thing as an agentless management solution. In this chapter, we'll look at management agents that do not include MDM, as well as when you will need to use an agent as opposed to when to use other options.

Chapter 3: Profiles

A profile is a file that can be used to configure settings on a Mac or iOS device. Once you install a management solution, you can deploy those profiles on a device, or you can deploy profiles on Macs using scripts. We'll cover how to craft profiles and install them so you can get most necessary settings on devices.

Chapter 4: MDM Internals

What is Mobile Device Management and how does it work under the hood? By understanding how MDM works, you will understand what needs to happen on your networks in order to allow for MDM, as well as the best way to give the least amount of access to the servers or services that are necessary.

Chapter 5: iOS Provisioning

This chapter covers how to prepare iOS, tvOS, and iPadOS devices for deployment, including working with profiles, MDM, Apple Configurator, the App Store, and other tools to set up these devices.

Chapter 6: Mac Provisioning

Setting up Macs has been a bit of a moving target, starting with the end of traditional imaging and the rise of zero-touch deployments using DEP. This chapter covers how to provision Macs for deployment using a variety of methods, including tools from both Apple and third parties.

Chapter 7: Endpoint Encryption

Now that the Mac or iOS device has been set up, folks will start adding data to them which needs to be protected. Encryption provides that protection, and this chapter covers how it works, how to enable it, and how to manage it for all of your Apple devices.

Chapter 8: Securing Your Fleet

An administrator can lock down devices so they're completely secure by turning them off and smashing them with a hammer. Security is table stakes in order to grow your device population. Every organization has their own security posture, and so once you get settings and apps on devices, we will take you through applying your security posture to customize the settings on Apple devices.

Chapter 9: A Culture of Automation and Continuous Testing

Deploying settings on devices without first testing those settings can cause your coworkers to have no idea where things are on their devices, get kicked off of networks, or many other things that will cause you to get coal during your office Secret Santa. As you deploy more and more iterations of systems, settings configurations, and software loads, you won't be able to manually test everything. In this chapter, we'll work on getting standard QA environments built out, so you can test without having to manually test everything.

Chapter 10: Directory Services

Active Directory was once the bane of many Mac Admins' existence. But in recent years, the problem of binding and existing in an Active Directory environment has been mostly a nonissue. In fact, these days, the biggest concern isn't how but why, given that there is now a bevy of options for dealing with directory services. In this chapter, we go through how to get Macs to work with Active Directory and function as a first-class citizen on predominantly Windows networks.

Chapter 11: Customize the User Experience

You can't cover device management without discussing one of the main reasons why people actually want to manage devices: to make the lives of their coworkers better. The book has thus far been about deployment and the finer technical details. We'll look at techniques and tools to leverage some of the things you've learned how to do in order to deliver world class support and enablement workflows.

Chapter 12: Identity and Device Trust

Federated identities are important as they keep us from putting our passwords over networks. This allows us to more easily access resources on networks and be more secure at the same time. What can be better? In this chapter, we cover common federated identity solutions and how to leverage them in new ways.

Chapter 13: The Future of Apple Device Management

By this point, you've likely stopped caring and just want the authors to wrap it up already. We get that. But in case you're still reading, you'll find a little prognostication for things to consider future-proofing your deployments.

Think Different

How cliché can we be? Obviously very much so. But there's an important concept that needs to be addressed, and that's attitude. Apple is forging their own path in IT. They trade spots with Amazon, Google, and Microsoft as the wealthiest company to ever exist. And they will not be constrained by 30 or more years of dogma in the IT industry. Or at least that's the way they often portray their perspective on the industry (which is real, but also a little spin).

As you'll see in Chapter 1, Apple is actually going about mass device management in much the same way it has since the 1980s. The screens look similar, the options look similar, sometimes with the same words. But due to the private data on systems and the ease of identity theft, there's much more of a focus on end-user privacy. Still, Apple devices aren't Windows devices. But they are increasingly sharing a code base made simpler by shared Swift and SwiftUI frameworks, and this has led to more similar management techniques than ever before.

The most important thing to consider is whether you want to try to shoehorn Apple devices into outdated modes of device management or whether you are ready to embrace Apple's stance on management. If you aren't ready to embrace the Apple way, then you might not be ready to manage Apple devices.

CHAPTER 1

The Evolution of Apple Device Management

Once upon a time, in a land far, far away, the Mac existed in a vacuum. Unmanaged and left behind in the grand scheme of the corporate enterprise, it was at best overlooked by Windows-centric IT departments and, at worst, marked for retirement and removal. In those times, it was common to see a network of Macs run as a silo, often with a dedicated cable modem for Internet access and sometimes even with a dedicated mail server to support the creatives. And yes, the Mac was almost exclusively used by teams of creatives like graphic designers and video editors.

The Mac platform seemed close to death in the late 1990s, as Apple's sales slumped and Microsoft's offerings dominated the consumer and enterprise markets. Microsoft embraced corporate and large-scale use and they released a number of tools like Active Directory and policies that a generation of administrators began to consider synonymous with enterprise management. Meanwhile, Apple released a few tools to help manage devices, but nothing with as granular options to control devices en masse as Microsoft had. Gradually, deployments of Apple equipment shrank to small workgroups with one exception: education.

C. Edge and R. Trouton, *Apple Device Management*,
https://doi.org/10.1007/978-1-4842-9156-6_1

Schools around the world continued to embrace the Apple platform throughout the tough times at Apple. During those times, anyone with large-scale Apple management experience almost certainly worked at a school or for a school district. But everything started to change with the advent of the iPhone. Suddenly, enterprises looked to education for guidance on how to deploy large numbers of Apple devices, CIOs asked their IT departments why IT wouldn't support the CEO's new MacBook Air, staff at some schools started to get jobs at large companies, and some of the requirements we faced started to change as corporate compliance became a new challenge.

> *The more things change, the more they stay the same, but not exactly. When Apple asked me to take over updating the Directory Services course and book, we used Mac OS X Server to keep management, identity, and authorization settings in the same place: Open Directory. But most wanted to leverage identity and authorization stored in another directory (LDAP or Active Directory). Then it seemed like no one cared about Directory Services any more and the focus was on moving from directory-based management (Workgroup Manager) to MDM. Now we're learning more about integrating MDM solutions with various 3rd party Identity Providers (IdPs). The fun part of this job is trying to figure out... What's next?*
>
> —Arek Dreyer, Dreyer Network Consultants and the author of several books on macOS and macOS Server

There are about as many reasons for this change as there are Apple fans. But the change is undeniable. The rise of Apple in the enterprise and the growth led to a number of innovations from Apple. The management story completely changed when Mac OS X was released and slowly evolved into what we now call macOS. But it started long before that.

In this chapter, we'll look at this management story – beginning in the dark ages, through the Renaissance that was the emergence of Mac OS X rising like a phoenix from the ashes of NeXT and into the modern era of macOS and iOS management. That story begins with the Apple II.

The Classic Mac Operating Systems

The Apple II was released in June of 1977 and changed the world, long before the Mac. It was one of the first mass-produced and therefore actually accessible computers. Back then, if environments had more than one computer, device management meant someone walked around with floppy disks that were used to boot the computer. Large-scale device management didn't become a thing until much, much later.

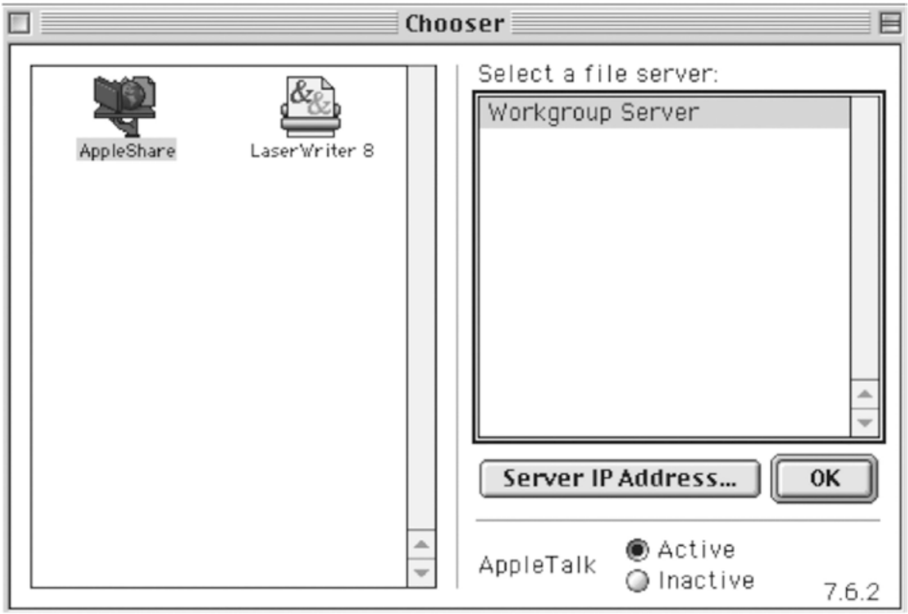
The Macintosh was released in 1984 and marked the first rung of the upward climb to where we are today. Between Apple's System 6 and Mac OS 9 operating systems, Mac management over the network often used the AppleTalk network protocol (which was released in 1985 but only went away in 2009 with Mac OS X Snow Leopard) instead of TCP/IP. In addition to being unsupported by any other platform (although Windows NT Server shipped with a connector and there were third-party tools that could bootstrap a service to host AppleTalk), AppleTalk's methods of network communication were viewed by many as being unnecessarily "chatty," which caused networks to slow down. This reputation, other Apple-specific characteristics, and the difficulty of managing Apple devices using Microsoft management tools led to the opinion that many old-timer IT execs still have today: "Apple devices don't play nice on corporate networks." They always did, just in a different way than Windows.

Network Protocols

Many of those older IT execs still have questions about whether or not Apple devices will cause problems on modern networks. If an Apple device can hurt a network, then the network has problems. It is true that once upon a time, Apple devices could spew AppleTalk traffic on the network that caused packet storms or other problems. But then, so could IPX or NetBIOS, which were initially released in 1983. The developers of these protocols learned a lot about how to network computers in the past 40 years.

Networking capabilities were initially built into the Apple Lisa in 1983 and initially called AppleNet. AppleNet was replaced by AppleTalk in 1985, and Apple finally dropped support for AppleTalk in 2009, although its use had slowed since the introduction of Mac OS X. Apple was able to join TCP/IP networks in 1988 with the release of MacTCP, which provided access to most types of devices that a Mac would connect with provided there was an agent that could decipher typically socket-based communications for each protocol.

Before Mac OS X, the Chooser was a tool used to connect to network file servers and printers. Shown in Figure 1-1, the Chooser would scan the network for AppleTalk devices and display them, which allowed users to "choose" a device to mount. Those mounts were synonymous with drive letter maps to network shares in Windows and mounted NFS shares for Unix and Linux. Because networks grew and discovery protocols didn't always find devices on the network, users could also enter a custom IP address to connect to if the host didn't show up in the list. The custom IP could also be used to connect to other LANs or over a WAN, provided port 548 was open on a host.



AppleTalk ● Active ○ Inactive

Figure 1-1. *The 1990s era Chooser*

With the advent of Mac OS X in 2001, the Chooser was replaced with the Connect to Server option (Figure 1-2), which had everything required to connect to file servers, WebDAV, and FTP servers available in most standard TCP/IP environments. Apple added Rendezvous to Mac OS X beginning in 2002, which allowed Macs to find devices and services over TCP/IP. Renamed to Bonjour in 2005, this zero-configuration technology uses mDNS (multicast Domain Name System) to allow users to locate (or browse) and connect to devices or services on networks with the same level of convenience that AppleTalk offered but with built-in support for the traditional Windows SMB (Server Message Block)services.

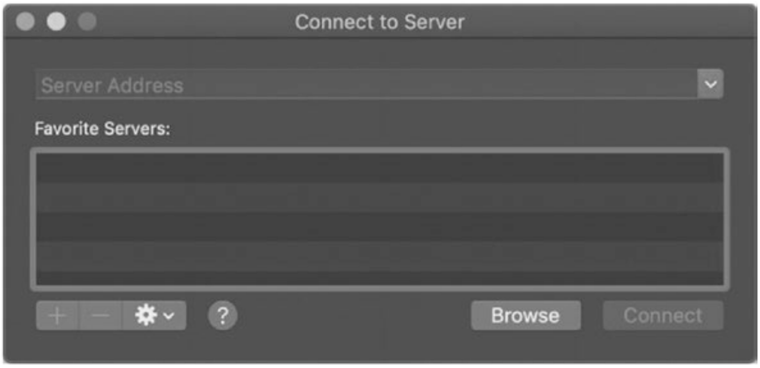


Figure 1-2. *The Connect to Server dialog*

The concerns about Apple on corporate networks were valid at times. During the massive rollouts of Windows 95 and then Windows 98, many environments used Novell networks or left IPX/SPX enabled on computers. NetBIOS, and later NetBEUI, were often enabled as well, causing a lot of traffic going over older hubs. When you added AppleTalk into that mix, there could legitimately be just too much traffic for the network equipment of that era. Luckily, AppleTalk is long behind us. Additionally, many switching environments started to ship with Spanning Tree Protocol (STP) enabled during the 2000s. Macs could have issues with Spanning Tree Protocol, especially if AppleTalk had not been disabled. However, Mac OS X slowly phased AppleTalk out in favor of newer protocols like Apple Filing Protocol (AFP) and later SMB. Even AFP became a “legacy” protocol as Apple transitioned the default protocols to SMB over time, and by the mid-2000s, AppleTalk was only there for backward compatibility with old hardware and software.

Once file services (and print services as AppleTalk gave way to standard LPR and other types of printers) were more compatible with other vendors, Apple could turn their attention to more important services. Larger environments naturally looked toward how they could manage devices over that same network connection used for files and printers.

Early Device Management

Devices weren't managed as intricately initially as they are today. Not only were the network protocols different, but the technology stack was wildly different; there weren't nearly as many devices being managed from a central location, and we didn't have 30–40 years of IT wisdom on how to make the lives better for our coworkers, students, or even ourselves. There also wasn't the expectation of privacy that there is today, which is a key element for managing Apple devices, as we'll cover over the next few hundred pages. Maybe administrators managed extensions (as Desk Accessories) with Font/DA Mover or launchers. This allowed a school or other environments to install fonts and things like screensavers – but Apple-provided tools for centralized management of Macintosh settings by and large weren't available reliably until the 1990s.

Apple's At Ease was an alternative desktop environment released for System 7 in 1991, which provided a simplified desktop environment for multiple users to use and share files, functionality not otherwise supported in the Mac at that time. As At Ease evolved, Apple also released At Ease for Workgroups, which provided client configuration options and a restricted Finder mode. It also allowed for home folders that could be stored on an AppleShare IP Server and with eMate the ability to hand in homework for classes (Figure 1-3). That restricted Finder mode later evolved into a (mostly) multiuser operating system environment in Mac OS 9 and the Simple Finder, which is still around today in modern macOS.