Apple Pro Training Series

Mac in the Enterprise

Second Edition

An Executive Guide to Integrating and Deploying Mac Systems

Ryan Faas, Ed.

Apple Certified

Contents at a Glance

SAMPLE PAGES

Table of Contents

Executive Summary

Mac in the Enterprise

You may be familiar with the impressive performance of the Mac, as well as its ease of use, and its wide range of applications. Yet with more Mac computers moving into medium and large organizations, many executives are asking the same question: How does the Mac fit in? The purpose of this book is to communicate the simplicity, high quality, and wide range of options available to IT teams as they deploy Mac systems. Simply stated, Macs integrate into the enterprise in the following ways:

- Apple offers tools and support for organizations ready to evaluate and deploy Mac systems (Chapter 1).
- The Mac comes standard with robust tools to manage users, groups, and systems according to your business needs (Chapters 2 and 3).
- The Mac integrates seamlessly into Active Directory environments (Chapter 4).
- The Mac has a wide range of built-in security features that work to provide and maintain system security (Chapter 5).
- Along with running OS X, the Mac runs Microsoft Windows and Linux operating systems using Boot Camp and virtualization technologies (Chapter 6).

- The Mac enables high-quality collaboration in the enterprise including interoperability with Microsoft Exchange, Lync, and SharePoint (Chapter 7).
- The cost of supporting the Mac in your enterprise can be the same or less than other PCs (Chapter 8).
- Apple offers a range of award-winning enterprise support options to serve your users where and when they need it (Chapter 9).

It is important to know the information presented here is aimed toward an IT decision maker or IT manager who has little to no technical Mac knowledge.

In addition, please note Apple has taken a very aggressive stance on supporting open standards and protocols, making it easy to integrate the Mac into existing environments with minimal effort.

This guide also makes a concerted effort to present configuration options that require little (or preferably no) change to your existing infrastructure or IT processes, yet will not dilute or inhibit your users' overall computing experience.

While this book will not cover step-by-step details, it will guide you through the technical options. As you consider an initial Mac deployment, or look at integrating larger numbers of Macs, feel free to contact your Apple Authorized Reseller or Apple account team to answer your Mac deployment questions.

1

Deploying the Mac in Your Enterprise

Most executives are familiar with the superior user experience of the Mac as well as its powerful productivity and wide range of applications. Yet as more and more employees are requesting the Mac at work, many IT decision makers are asking the same question: How does OS X fit in?

The simple answer is the Mac can integrate seamlessly into enterprise environments. And these integration options allow your employees to take advantage of all the well-known benefits of OS X. This chapter provides a brief overview of how the Mac fits into the enterprise. It, outlines the four key steps for implementing a successful evaluation and deployment of Mac systems in business, government, and non-profit organizations. It provides a sample timeline for testing and deploying Macs. Also included are typical stumbling blocks to avoid, and IT technical and training resources available to your teams as they test and deploy the Mac.

It's Simple—the Mac Fits In

Mac clients are designed to integrate smoothly into existing enterprise directory systems. Your employees can log in using Active Directory credentials the same way they do with their Windows clients. OS X supports industry-standard Lightweight Directory Access Protocol (LDAP) services and Kerberos authentication. It also fully supports Microsoft Active Directory authentication policies, replication, and failover.

Mac systems are also designed to work with common enterprise technologies such as Microsoft Exchange, virtual private networks (VPN), and RADIUS authentication. Likewise Mac systems can use many enterprise applications. Whether you have Mac or PC systems in your environment, you can set up a single user identity that can authenticate and grant access to client devices and network resources in the same manner regardless of platform. This enables your organization to leverage existing management processes and teams.

OS X comes standard with robust tools that allow your organization's IT staff to centrally manage and support Mac client systems. These resources provide proactive upgrade, patch, and security services while keeping costs and overhead low. Many proven third-party device management solutions for OS X are also available.

When it comes to security, OS X has been designed from the ground up with an eye toward helping protect data, services, and applications. The Apple approach focuses on providing security at each layer of the operating system and a commitment to making security features as automatic and easy to use as possible.

Microsoft Office and many other popular third-party applications are available for the Mac and run natively on it. When users need to run Microsoft Windows (or other operating systems) applications, OS X virtualization options enable users to run Windows and Windows applications.

The Mac enables high-quality collaboration within enterprise environments. Mac systems come standard with a suite of collaboration tools based on open standards and popular technologies. These tools enable you to immediately and easily integrate OS X into your enterprise collaboration environment.

Apple offers a range of enterprise support options. Whether you have occasional questions or you need daily assistance, Apple has a plan

2

Planning Mac Deployments

This chapter describes seven components—each based on real-world examples of Mac deployments commonly used by large organizations with hundreds or thousands of Mac systems—common to deploying and managing Mac systems. Depending on your organization's needs, you can use these components, and their associated levels of management, to determine the best deployment plan for your organization.

Keep in mind that this list is not absolutely objective. Some of the higher levels of management for a specific component may not fit the needs of your organization. As such, these categories do not represent a grade or value judgment; they simply describe a style of management that can be achieved or enforced. Mac systems can, and do, function effectively at varying levels of client management in different organizations. There is no single correct way to manage Mac systems. Every IT department must balance costs, benefits, and risks to determine the options that best suit the needs of its users and the overall organization.

The seven common components of client deployment and management are:

- **Preparation**—Are new systems deployed from monolithic disk images or via thin imaging workflows? If you are implementing a BYOD program, Mac system preparation can be similar to a thin

imaging workflow, as described in Chapter 3. Depending on the answer, there are different preparations to make.

- **Deployment**—How do you plan to deploy Mac systems? Both network-based and local options are available.

  NOTE ► Disk images and related deployment solutions are covered in the next chapter.

- **Directory services**—If your organization uses directory services such as Active Directory, what information will they provide to Mac systems? (See Chapter 4 for details on Mac directory service integration options.)
- **Policies**—Have user and client management policies been determined and/or implemented?
- **Maintenance**—How easy is it to update the OS X and/or installed applications?
- **Help desk**—How easily and effectively can IT staff support the Mac and assist users?
- **Security**—How secure is the Mac configuration?

Preparation

There are three basic levels of complexity for creating a software, or system, image:

- **None**—At the most basic level, you can simply hand out Mac computers as they came from the factory. This style of deployment can work well with BYOD programs. In such cases, Mac deployment takes on the characteristics common in iOS deployments.
- **Basic**—Preparation for basic Mac deployment revolves around the creation of disk images. These images can be traditional monolithic builds containing all the file and configuration states

3

Deploying and Managing OS X

Whether your IT team is upgrading dozens or thousands of Mac computers, OS X is delivered electronically via the Mac App Store.

Although this new method of software distribution may seem counter to the deployment needs of large institutions, it actually allows for existing deployment workflows to remain in place. More importantly it can serve as a catalyst for change when considering Mac deployment and management options.

In an ideal environment, deployment and management of OS X involves the following steps:

- **Deploy**—When a new Mac is deployed, it needs to be configured so that it meets the requirements of a particular organization. When an existing Mac needs to be upgraded to OS X Mountain Lion, there are additional criteria to consider. How can IT provide the new OS without removing or altering user data? More importantly how can OS X be deployed with a minimal amount of IT effort?
- **Manage**—Major aspects of client management include controlling what activities users are allowed to perform and what installed software they are allowed to run; providing easy access to resources; and monitoring the state and use of computers.
- **Maintain**—After Mac systems have been deployed, it is critical to keep the operating system and applications up to date on each system. A capable patch management mechanism can ensure that updates are deployed in a timely manner.

Deploy

Using a combination of Apple NetInstall, Configuration Profiles, and Installer packages, Mac computers can be deployed in a time efficient way and without the need for traditional imaging workflows.

Creating Software Packages

Over the years computer deployment has been focused on the creation and deployment of block copy disk images. While Apple enables this traditional image-based workflow with its native deployment tools, the state of the art in computer deployment is changing.

Along with the rise of consumerization in IT has come the realization that simply installing additional software and configurations is all that is needed to deploy workstations. This enables IT organizations to focus on the software and configuration additions needed for their environment rather than on recreating and deploying complete system images with base OS and standard apps.

The best way to install software on a Mac system is to use the standard Apple Installer package format. A fully package-based installation offers the following advantages:

- Packages use a standard format.
- Packages can be installed using a variety of client management products.
- Packages can run scripts.
- Packages can be audited.
- The Recovery HD function of OS X Mountain Lion is preserved.

Packages can be created with many different tools, such as PackageMaker from Apple, which is included with the Xcode IDE and related development tools. When it's time to install your

4

Directory Integration and Policy Management

Directory services are a core component of enterprise computing environments that allow organizations to centralize information about users, groups, and computing resources. In addition to consolidating resources and simplifying system management, directory services also provide benefits to users by enabling them to access enterprise resources from anywhere on the network with a single set of credentials

A key advantage to this single directory approach is that it allows organizations to centrally manage all user, group, and computer accounts. As a result, a directory services infrastructure offers advantages for both administrators and users.

The Apple implementation of a directory service is Open Directory (OD). Integrated into the foundations of OS X, it is responsible for providing directory and network authentication services for both OS X clients and systems running OS X Server. Open Directory uses open standard protocols such as LDAP, Kerberos, and the Simple Authentication and Security Layer (SASL) to integrate with other common directory systems.

Although Apple provides its own native directory services platform through Open Directory, OS X supports access to a variety of other directory services including Microsoft's Active Directory. Apple has made a concerted and successful effort to enable IT administrators to integrate OS X clients and servers easily into existing Active Directory

environments. Although every Active Directory installation is different, OS X integrates well with the vast majority of them with minimal effort.

OS X systems fully support joining their local Open Directory node, which contains local user accounts, to an Active Directory forest. When a Mac system is joined to Active Directory, maintaining a separate directory or separate user records to support Mac systems isn't necessary. Users can move between different computers regardless of operating system or platform while still adhering to enterprise policies for strong authentication and protected access to network resources.

When fully integrated with Active Directory, OS X offers a managed environment where users:

- Can access any Mac in the integrated environment using the same credentials they would use to access Windows PCs.
- Are subject to Active Directory password and management policies.
- Can leverage single sign-on access to Active Directory–bound network resources via Kerberos.
- Can have network-based home directories, local home directories, or a combination of the two (called Portable Home Directories, which are similar to roaming profiles on Windows).

Apple support for Active Directory extends to OS X Server as well. Integrating a server is just as easy as integrating a client system—in fact, the process is essentially the same. This allows users logged into Windows workstations to take advantage of resources hosted by OS X Server (file sharing, web services such as wikis and blogs, and other services) while using the existing Active Directory infrastructure and their user accounts for identification and authentication. Secure network services (including network home directories) hosted on OS X Server also support single sign-on from both OS X and Windows clients.

5
Security

OS X is designed from the ground up with an eye toward providing and maintaining system security in an automatic and easy to use way. Apple strives to ensure that OS X provides protection to systems, software, and data without the need for advanced configuration or specialized tools. As your organization considers security strategy, it's important to find the mix of technologies that best protects against unauthorized use or access and that also meets the needs of your business.

The Mac is designed to provide a resilient defense against security threats through a series of protective systems and approaches to identify potential threats and proactively protect against them. These defenses manage access to system resources at a granular level; mitigate advanced runtime attacks; protect against network-borne threats; validate the integrity and authenticity of software; and quarantine unknown files.

Apple also implements many security features designed to protect the confidentiality of both user and corporate data. Some of these features protect data stored on a local or removable volume (data at rest), while others protect data shared on a local network or traveling across the Internet (data in transit). Many of these technologies are inherent in the design of the operating system and are active without

requiring configuration. Others, such as FileVault 2, can be easily enabled and configured by both users and IT departments.

OS X is built on a foundation of open source components that have been through decades of intense scrutiny by Apple, third-party developers, and security experts. Apple participates in the open source community by sharing the development process of many OS X components with third-party developers. This ongoing effort leads to the incorporation of recommended improvements and provides the transparency necessary to validate that many critical components of OS X are as secure as possible.

Apple also collaborates with the broader information security community, including CERT, FIRST, the FreeBSD security team, and government security experts. These efforts have led to a joint review and validation of technology implementations and have also resulted in ongoing security guidance. A thorough and granular discussion of methods to refine the security configuration of OS X systems is publicly available in the form of Apple Security Configuration Guides (www.apple.com/support/security). You can also find them on the NSA Information Assurance website (www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml).

Service and App Protection

OS X provides a range of technologies that work to ensure the security of Mac systems. One of the most critical is the use of digital signatures to certify applications are safe and haven't been tampered with by an individual, malware, or file damage. Sandboxing of applications and services ensures that a compromised app or process can have only limited impact. Mandatory access controls work with other security technologies to help ensure system, application, and data security.

6

Boot Camp and Virtualization

In many medium and large business environments, users occasionally need to run Windows (or other operating systems) or Windows applications to accomplish specific tasks. Mac systems can run Windows natively using the Apple Boot Camp feature. The Mac can also run a variety of Windows and Windows Server releases along various Linux distributions and other operating systems using virtualization. This chapter will help you understand what is possible using each method as well the deployment options and special considerations for each one.

When using Boot Camp, users have access to all the hardware features of their Mac computers (including built-in cameras, optical drives, networking, and graphics hardware). Boot Camp is included free with every Mac, though running Windows will require an appropriate license from Microsoft.

The second option, virtualization, has been common in many IT departments for many years as a server solution for allowing multiple instances of a server operating system to be run simultaneously on a single server. As a server solution, virtualization can reclaim unused processing power and also help secure discrete instances of the operating system and its resources.

Although this may be one of the primary uses of virtualization in the server room, virtualization on the desktop (particularly on the Mac) is often used to allow access to multiple guest operating systems and

associated applications. For employees who prefer to work on the Mac (or whose job functions are more naturally suited for the Mac) yet who still need to occasionally run a Windows application, virtualization allows them to have equal access to both Mac and Windows tools.

Boot Camp

Boot Camp is a free utility built into OS X. Unlike virtualization solutions, Boot Camp is a dual-boot solution requiring users to reboot their computers to switch between installed operating systems such as OS X and Windows.

> **NOTE ►** For the most current information on Boot Camp support for Windows, see www.apple.com/support/bootcamp/.

Boot Camp Assistant

The Boot Camp Assistant utility helps prepare a Mac to have Windows installed on it. This utility provides a simple GUI for nondestructively editing a single-partition HFS+ journaled disk to add a partition onto which Windows can be installed and booted from. The Boot Camp Assistant also creates a Windows Installer answer file containing basic Windows setup information. The assistant will function only with simple, single-partition disk configurations. If you want to install Windows onto a disk with multiple partitions, or onto a nonroot disk, you will need to configure the system by hand. This simple task is covered in the "Deployment" section of this chapter.

In addition to preparing a Mac for Windows installation, the Boot Camp Assistant creates a CD containing a set of Windows device drivers for all of the Mac system's Apple hardware. Once Windows has been installed using Boot Camp, this CD will provide Windows access to all Apple hardware.

7
Collaboration in the Enterprise

Information is the lifeblood of the knowledge worker, and optimizing the sharing, storage, and retrieval of institutional knowledge is one of the great challenges for IT. This chapter looks at the tools and technologies Apple leverages to integrate into an organization's existing collaboration solutions and also explores the powerful native options that OS X offers.

Mail, Calendar, and Contacts

Email, personal and shared calendaring, and personal and shared contacts are some of the most basic and important tools in medium and large business environments. OS X ships with out-of-the-box support for the most common enterprise messaging and calendaring platforms and technologies, including solutions based on open standards such as LDAP, CalDAV, and CardDAV as well as commercial solutions such as Microsoft Exchange.

One difference between Windows systems and OS X is Windows users are used to a single application, most commonly Outlook, to supply all of their messaging, contacts, and calendar needs. While OS X supports the same functionality, it does so with these tasks broken down into three separate but integrated applications: Mail, Calendar, and Contacts.

NOTE ► As an alternative to the Apple tools, Microsoft does offer a version of Outlook for Mac that centralizes these features into a single app as on Windows PCs. Outlook is included as part of Office for Mac 2011.

Using Mail, Calendar, and Contacts with Microsoft Exchange

OS X has built-in support for Microsoft Exchange 2007 and 2010, without the installation of additional software or the cost of a Client Access License (CAL) for Microsoft Outlook. Mac users can use Mail, Calendar, and Contacts to access Exchange services including email, calendar invitations along with free/busy scheduling options, and an organization's Global Address List.

OS X uses the auto-discover services built into Microsoft Exchange 2007 and Exchange 2010, making the entire setup process as easy as typing in a user's email address and password. Mac clients can then use the same Exchange-based data that is available to Windows clients running Outlook. The Mail application, for example, has support for out-of-office messages with separate replies for recipients inside and outside of an organization. Additionally, reminder follow-up flags set in Outlook on the PC are preserved in Mail.

OS X integrates Apple technology in Mail, which provides features unique to the Mac when working with Exchange data. Two examples are Spotlight for quick and easy searches and Quick Look to preview attachments in Mail without needing to launch additional applications. Another is the data detection feature in Mail, which automatically detects dates, addresses, and other common formatted information and offers users a series of options based on the context of the detected data such as creating a calendar event or adding a contact without leaving the Mail application.

8

Supporting Users: The Self-Service Model

The previous chapters describe a number of best practices for how IT departments can manage, support, secure, and control Mac computers within large organizations. Implementing many of these technologies and approaches can enable organizations to spend less time supporting Mac systems and thus can free up valuable IT team time and resources.

This chapter explores some additional methods IT departments can use to reduce costs while increasing user satisfaction with IT staff, policies, and processes. More and more IT departments in large organizations are investigating a variety of innovative approaches that empowers users with the ability to support themselves.

The consumerization of IT and bring your own device (BYOD) trends are becoming mainstays of many businesses and enterprises. These changes potentially bring many benefits to medium and large organizations including increased user engagement and productivity because users can work with the tools they find most efficient. These trends can also provide an increase in overall job satisfaction, boost employee satisfaction with IT experiences, and potentially reduce both hardware and software costs. In fact, a self-servicing philosophy can be a very powerful catalyst to empower users while potentially lowering costs.

These new self-service approaches are being explored in a wide range of companies across virtually every industry. Although these practices may not be right for every organization, they are well worth

considering as organizations plan and allocate resources. Keep in mind that implementing all aspects of these approaches isn't necessary in order to increase user satisfaction and reduce costs. And with every offering, it's important to strike a balance so that users who prefer a self-service approach, as well as users who prefer a centralized IT support approach, are both satisfied.

A Sample Scenario

Although it isn't necessary to implement all the elements outlined here in order to see increases in employee satisfaction and productivity, as well as cost reductions, this sample scenario illustrates what is possible when the consumerization and BYOD trends are taken beyond the mobile device level and applied throughout an organization.

Imagine the following scenario. As a new employee joins the organization, she is given a computer acquisition budget and directed to a website where a variety of systems are offered. All of the machines are portable computers, but some are more powerful than others. Some have longer battery life, and others are more lightweight. She picks the system she is most comfortable with and provides a personal credit card if the price of the system is over the allotted budget.

The computer is shipped overnight directly to the user's desk with no special build or operating system on the computer. She is given a one-page instruction sheet that tells her how to log in to a SSL VPN with a username and password. The system uses either a public Internet connection or the wide-open wireless network in the office.

Once connected using the VPN, she looks over a number of applications from an internal application store and chooses the applications that fit what she will be doing on a daily basis. Self-help videos and screencasts walk her through configuring email and calendar clients. A variety of automated systems allow her to pick from a collection of local printers.

9
Support Options

AppleCare offers a wide range of service and support options for commercial and government customers to support Apple hardware and software products. This chapter provides details about the various support options available to your organization as you begin to test and deploy Apple technologies, including options covering hardware, desktop OS and software, and comprehensive IT and network support.

Annual Support Agreements

Apple offers a complete range of annual support agreements for enterprise customers that can help your IT staff ensure the best possible user experience at all times.

AppleCare OS Support

Get the IT department-level support you need when deploying OS X, OS X Server, or iOS in your organization. AppleCare OS Support delivers phone and email support for integration, migration, and advanced server operation issues. Whether you have occasional questions or you need assistance on a regular basis, Apple has a plan to fit your requirements. Each plan provides one year of coverage.

AppleCare OS Support plans provide enterprise-level incident support—defined as support for system components; network configuration and administration; integration into heterogeneous

environments; professional software applications; web applications and services; and technical issues requiring the use of the command-line tools for resolution.

Customers may choose from three levels of support:

- **Select**—Covers up to 10 enterprise-level incidents and provides four-hour response for priority 1 issues (server down), 12 hours a day, 7 days a week (12/7). Unused incident support expires after one year. Additional support for incidents can be purchased as needed.
- **Preferred**—Covers an unlimited number of enterprise-level incidents, provides two-hour response for priority 1 issues, 12/7, and assigns a technical account manager to your organization.
- **Alliance**—Covers an unlimited number of enterprise-level incidents across multiple locations and provides one-hour response for priority 1 issues, 24/7. This plan includes an onsite review by an Apple technical support engineer.

Every AppleCare OS Support plan also includes AppleCare Help Desk Support, an annual technical support plan that covers an unlimited number of support incidents for software installation, launch, and use; hardware and software diagnosis and troubleshooting; and issue isolation for Apple-based solutions.

> **MORE INFO ►** For more information on AppleCare OS Support, see www.apple.com/support/products/enterprise/ossupport.html.

AppleCare Help Desk Support

Whether deploying iOS in the enterprise or supporting Mac systems, AppleCare Help Desk Support provides the backup expertise that frontline technology staff requires. This plan provides priority access to Apple senior technical support staff by telephone 12 hours a day, 7 days a week. It also includes a suite of tools that enable users to

Apple Certified

Apple Pro Training Series: Mac in the Enterprise, Second Edition

Many IT departments are familiar with the Mac's powerful performance, ease of use, and wide range of applications. Yet with more Mac computers being deployed in medium and large organizations, many executives are asking: How does the Mac fit in? The purpose of this book is to communicate the simplicity, high quality, and range of solutions available to integrate the Mac into an existing IT network.

Mac in the Enterprise provides an overview of how to evaluate, deploy, and manage the Mac; explains several options for adding Mac systems to an Active Directory environment; and explores running Windows and Linux on a Mac. Additionally, it reviews the built-in security as well as the collaboration features in OS X and outlines support options offered by Apple. This book also discusses Apple's robust support for open standards and protocols making it easy to integrate the Mac into existing IT environments with minimal effort and changes to existing infrastructure.

The Apple Pro Training Series is both a self-paced learning tool and the official curriculum of the Apple Training and Certification Program. To find an Apple Authorized Training Center near you, please visit www.apple.com/training.

Check out these other Apple Pro Training Series books:

- OS X Mountain Lion Support Essentials
- OS X Mountain Lion Server Essentials

To see all our titles, visit www.peachpit.com/appleprotraining

Peachpit Press
www.peachpit.com

Book Level Advanced
For Computers Using OS X Mountain Lion

US $18.99

ISBN-13: 978-0-321-88516-6
ISBN-10: 0-321-88516-3