OS X Deployment Technical Reference

OS X Yosemite 10.10

December 2014

Mac Business Solutions

www.mbsdirect.com

Contents

Introduction

This guide is for IT decision makers, implementers, and administrators in commercial organizations who want to support Mac computers with OS X Yosemite on their networks. It provides information about deploying and supporting Mac in medium to large-scale organizations. It explains how OS X provides comprehensive security and integration with your existing infrastructures, and powerful tools for deployment.

Understanding the key technologies supported in OS X will help you implement a deployment strategy that delivers an optimal experience for users. The below sections serve as a technical reference when deploying OS X throughout your organization:

Deployment models. There are several ways to deploy Mac in your organization. Regardless of the deployment model you choose, it's helpful to consider the steps needed to ensure that your deployment goes as smoothly as possible. While this guide encompasses all aspects of an OS X deployment, organizations may approach their deployments differently.

It should be noted that in the past, computer deployment depended heavily on tools for imaging and software distribution. While OS X already offers many such tools, the trend in Mac IT has been to focus on configuration rather than imaging. Every Mac comes with a built-in recovery feature that allows it to repair, or even reinstall, OS X directly from Apple with no in-house infrastructure needed at all.

This allows IT staff to focus on only the parts of the experience that make a Mac unique to your organization. These configuration changes are easily made with your mobile device management (MDM) solution.

Infrastructure and integration. OS X has built-in support for a wide range of network infrastructures. In this section, you'll learn about the technologies supported in OS X and best practices for integrating with Active Directory, Microsoft Exchange, Wi-Fi, VPNs (virtual private networks), and other standard services.

Internet services. Apple has built a robust set of services to help users get the most out of their Mac. These services include iMessage, FaceTime[1], iCloud[2], and iCloud Keychain. Details about how to set up and manage Apple IDs is also covered in this section.

Security. OS X is designed to securely access corporate services and protect important data. It provides strong encryption for data in transmission, proven authentication methods for accessing corporate services, and full-disk encryption for all data at rest. Read this section to learn more about the security features of OS X.

Configuration and management. OS X supports advanced tools and technologies to ensure Mac can be set up easily, configured to meet your requirements, and managed efficiently in a large-scale environment. This section describes the different tools available for deployment including an overview of MDM and the Device Enrollment Program.

App and book distribution. There are a number of ways to deploy apps and content throughout your organization. Programs from Apple, including the Volume Purchase Program and the Mac Developer Program, enable your organization to buy, build, and deploy apps and books for internal users. Use this section to get an in-depth understanding of these programs and learn how to deploy apps and books purchased or built for internal use.

Planning for support. Apple provides a variety of programs and support options for OS X users. Before deploying Mac computers, find out which options are available for your organization and plan for any support you'll need.

Deployment Models

Explore the possibilities before you get started. First think about how you'll distribute and set up Mac. There are several options, from preconfiguration to user self-service setup. Your particular deployment models will determine the tools and processes you use to deploy.

For medium and large organizations, there are several ways to deploy OS X. Whether you choose to deploy company-owned devices or institute a bring-your-own-device (BYOD) policy, it's helpful to consider the steps needed to ensure your deployment goes as smoothly as possible.

After your deployment models are identified, your team can explore Apple's deployment and management tools and programs in detail. They are covered extensively within this resource and should be reviewed with the key stakeholders within your organization.

Enterprise Deployment Models

Mac computers can transform business. They can significantly boost productivity and give your employees the freedom and flexibility to work in new ways, whether in the office or on the go.

Embracing this new way of working leads to benefits across the entire organization. With Mac, users have access to high performance, flexible tools, and solid security so they feel empowered and are able to creatively solve challenges. By supporting OS X, IT departments are viewed as shaping the business strategy and solving real-world problems, rather than fixing technology and cutting costs. Ultimately everyone benefits, with a reinvigorated workforce and new business opportunities everywhere.

Whether you're a large or small organization, there are many easy ways to deploy and manage Mac.

Start by identifying the best deployment models for your organization. Apple provides different deployment and management tools, depending on the model you choose.

Deployment models

Below are common models for deploying OS X in the enterprise:

- Corporate-Owned Deployment
- Personalized Mac—Corporate-Owned
- Personalized Mac—BYOD
- Shared Mac—Corporate-Owned

While most organizations have a preferred model, you may encounter multiple models within your organization.

For example, a retail organization may deploy a personalized-device (BYOD) strategy by allowing employees to set up their personal Mac computers while keeping corporate resources separate from the user's personal data and apps. However, their retail stores may also deploy a non-personalized-device (shared Mac) strategy, allowing Mac computers to be shared by several employees in order to process transactions for customers.

Exploring these models in more detail will help you identify the best approach for your unique environment.

Corporate-Owned Deployment

In many cases, companies choose to purchase computers and assign them for individual employees to use. In this model, each user is assigned a Mac that's configured and managed by your organization. An MDM solution can simplify and automate this process. If the computers are purchased directly from Apple, your organization can use the Device Enrollment Program (DEP) to automate enrollment in MDM, so a Mac can be handed directly to a user.

Once users receive their DEP-enabled Mac, they follow a streamlined process using Setup Assistant, are automatically enrolled in MDM, and can further personalize their Mac within the constraints set by your organization. Users may also receive an invitation to download specific licensed content, such as apps and books purchased through the Volume Purchase Program (VPP). Your organization can deliver, update, or revoke these resources at any time. And with Caching Server, most of these downloads can come from the local network rather than the Internet.

Personalized Mac—Corporate-Owned

The most common enterprise OS X deployment scenario is a Mac that is owned by your organization, but set up for an individual user. You can configure a Mac with corporate settings and enroll it with an MDM solution before giving it to a user. This approach is the least amount of work for employees, but is more labor intensive for IT.

Alternatively, users can enroll their computers with an MDM solution that provides settings and apps over the network. This approach allows a new Mac to be shipped directly to a user. And the workload can be further reduced by leveraging DEP to automate the MDM enrollment settings.

The following tables list the responsibilities of both the administrator and users for a corporate-owned personalized Mac deployment.

Prepare	
Administrator:	**Users:**
Evaluate your existing infrastructure including Wi-Fi, VPN, directory service, and mail and calendar servers.	Create an Apple ID as well as iTunes Store and iCloud accounts, if applicable.
Investigate, procure, and deploy an MDM solution.	
Enroll in the Device Enrollment Program and the Volume Purchase Program.	

Set up and configure	
Administrator:	**Users:**
From the DEP website, link your virtual servers to your MDM solution.	The user is provided a Mac. If IT has preconfigured it, no further action is needed.
Streamline enrollment through the DEP by assigning devices to your virtual MDM servers by order number or by serial number.	Enter enterprise credentials in Setup Assistant for DEP (optional).
Assign Mac computers in DEP for streamlined enrollment in MDM.	Personalize your Mac with Setup Assistant and enter a personal Apple ID.
Configure and install accounts, settings, and restrictions with MDM.	If DEP isn't used, enroll in MDM. Device settings and configurations are automatically received from MDM.

Distribute apps and books	
Administrator:	**Users:**
Download your token from the VPP Store and link it to your MDM solution.	Accept the invitation to VPP.
Purchase apps and books using VPP and assign them to users with MDM.	Download and install apps and books assigned by the organization.
Send VPP invitations to users.	
Install Caching Server to speed content delivery over the local network.	
Distribute in-house apps, non-VPP apps, and in-house books by hosting them on a web server or using your MDM solution.	

Ongoing management	
Administrator:	**Users:**
Revoke and reassign apps to other users as needed with MDM.	If a Mac is lost or stolen, the user can locate, lock, or perform a remote wipe using Find My Mac.
With MDM, an administrator can query managed computers to monitor compliance, or trigger alerts if users add unapproved apps or content.	Apply software updates from the Mac App Store as they become available.
MDM can also lock computers or reset system passwords, remotely wipe any managed accounts or data, and wipe a Mac entirely.	
A Mac may be easily wiped and then redeployed using the OS X Recovery feature or a local NetInstall server.	

Additional resources

Volume Purchase Program

Mobile Device Management

Device Enrollment Program

Apple ID

Caching Server

Personalized Mac—BYOD

With a bring-your-own-device deployment, users set up their personal Mac using their own Apple ID. In order to access corporate resources, users can configure settings manually, install a configuration profile, or more commonly, enroll the computer with your organization's MDM solution.

An advantage of using MDM to enroll personal computers is that you can enforce settings, monitor corporate compliance, and remove corporate data and apps, while leaving personal data and apps on each user's system.

Other than ownership, the main differences between BYOD and corporate-owned deployments is the ability to use DEP for automated MDM enrollment.

The following tables list the responsibilities of both the administrator and users for a personalized BYOD Mac deployment.

Prepare	
Administrator:	**Users:**
Evaluate your existing infrastructure including Wi-Fi, VPN, directory service, and mail and calendar servers.	Bring a Mac from home or purchase a new Mac to use at work.
Investigate, procure, and deploy an MDM solution.	Create an Apple ID as well as iTunes Store and iCloud accounts, if applicable.
Enroll in the Volume Purchase Program.	

Set up and configure	
Administrator:	**Users:**
Enroll devices and configure accounts, settings, and restrictions wirelessly using MDM based on user/group policies defined by the organization.	Enroll in MDM.
Alternatively, organizations can provide settings for individual accounts to users, and policies can be pushed with Exchange or installed using a configuration profile.	Corporate settings, configurations, and accounts are automatically received from MDM. Alternatively, users can install configuration profiles manually or configure settings provided by IT.

Distribute apps and books	
Administrator:	**Users:**
Download your token from the VPP Store and link it to your MDM solution.	Accept the invitation to VPP.
Purchase apps and books using VPP and assign them to users with MDM.	Download and install apps and books assigned by the organization.
Send VPP invitations to users.	
Install Caching Server to speed content delivery over the local network.	
Distribute in-house apps, non-VPP apps, and in-house books by hosting them on a web server or your MDM solution.	

Ongoing management	
Administrator:	**Users:**
Revoke and reassign apps to other users as needed with MDM.	If a Mac is lost or stolen, the user can locate, lock, or perform a remote wipe using Find My Mac.
With MDM, an administrator can query managed computers to monitor compliance, or trigger alerts if users add unapproved apps or content.	Apply software updates from the Mac App Store as they become available.
MDM can also lock computers or reset system passwords, remotely wipe any managed accounts or data, and wipe a Mac entirely.	When the MDM relationship is removed, managed accounts, settings, and apps are disabled. The user's personal apps, books, data, and content are untouched.

Additional resources

Volume Purchase Program

Mobile Device Management

Apple ID

Caching Server

Shared Mac—Corporate-Owned

Although it isn't as common, there are use cases for Mac as a shared computer. These scenarios normally revolve around kiosk and point-of-sale deployments or shared work areas such as reception desks or lab workstations.

OS X fully supports a multiuser environment and seamlessly works with directory services such as Active Directory and LDAP. (See the Infrastructure and Integration section for more details.) These abilities can be combined with MDM to provide a secure, low-maintenance environment.

The following tables list the responsibilities of both the administrator and users for a corporate-owned shared Mac deployment.

Prepare	
Administrator:	**Users:**
Evaluate your existing infrastructure including Wi-Fi, VPN, directory service, and mail and calendar servers.	No action needed.
Investigate, procure, and deploy an MDM solution.	
Determine if an Apple ID will be needed for app assignment.	
Enroll in the Device Enrollment Program and the Volume Purchase Program.	

Set up and configure	
Administrator:	**Users:**
From the DEP website, link your virtual servers to your MDM solution.	No action needed.
Streamline enrollment through DEP by assigning computers to your virtual MDM servers by order number or by serial number.	
Assign Mac computers in DEP for streamlined enrollment in MDM.	
Configure and install accounts, settings, and restrictions with MDM.	
Unbox and (optionally) asset tag each Mac.	

Distribute apps and books	
Administrator:	**Users:**
Download your token from the VPP Store and link it to your MDM solution.	No action needed.
Purchase apps and books using VPP and assign them to users with MDM.	
Enroll the created Apple IDs in VPP, if needed.	
Install Caching Server to speed content delivery over the local network.	
Push VPP apps to Mac computers.	
Distribute in-house apps, non-VPP apps, and in-house books by hosting them on a web server or your MDM solution.	

Ongoing management	
Administrator:	**Users:**
With MDM, an administrator can query managed computers to monitor compliance, or trigger alerts if users add unapproved apps or content.	No action needed.
MDM can also lock computers or reset system passwords, remotely wipe any managed accounts or data, or wipe a Mac entirely.	
A Mac may be easily wiped and then redeployed using the OS X Recovery feature or a local NetInstall server.	

Additional resources

Volume Purchase Program

Mobile Device Management

Apple ID

Caching Server

Infrastructure and Integration

OS X supports a wide range of network infrastructures, including the following:

- Standard Wi-Fi protocols for data transmission and encryption
- Local networking using Bonjour
- Wireless connections to Apple TV using AirPlay
- Digital certificates to authenticate users and secure communications
- Single sign on to streamline authentication to networked apps and services
- Standards-based mail, directory, calendar, and other systems
- Popular third-party systems like Microsoft Exchange and Active Directory
- VPN including per app VPN and always-on VPN

This support is built into OS X, so your IT department only needs to configure a few settings to integrate Mac into your existing infrastructure. Read on to learn more about OS X-supported technologies and guidelines for businesses and educational institutions.

Wi-Fi

Out of the box, OS X can securely connect to corporate or guest Wi-Fi networks, making it quick and simple for users to join available wireless networks whether they're on campus or on the road.

Note: OS X must have access to your wireless network and Internet services for setup and configuration. You may need to configure your web proxy or firewall ports if Mac computers are unable to access Apple's activation servers, iCloud, or the iTunes Store. For a list of ports used by Apple products, refer to this Apple Support article.

Wi-Fi throughput

As you plan to deploy OS X throughout your organization, make sure your Wi-Fi network and supporting infrastructure are robust and up to date. Consistent and dependable access to a strong network is critical for setting up and configuring a Mac. In addition, being able to support multiple systems with simultaneous connections from all your employees, students, or teachers is important to the success of your program.

Joining Wi-Fi

Users and IT departments can set OS X to automatically join available Wi-Fi networks. Built-in captive portal support means that Wi-Fi networks that require login credentials or other information can be quickly accessed without opening a separate browser session, from Network Preferences in System Settings or within apps such as Mail. And low-power, persistent Wi-Fi connectivity allows apps to use Wi-Fi networks to deliver push notifications.

WPA2 Enterprise

OS X supports industry-standard wireless network protocols, including WPA2 Enterprise, ensuring corporate wireless networks can be accessed securely from a Mac. WPA2 Enterprise uses 128-bit AES encryption, a proven, block-based encryption method. This provides users with the highest level of assurance that their data will remain protected.

With support for 802.1X, OS X can be integrated into a broad range of RADIUS authentication environments. 802.1X authentication methods supported by OS X include EAP-TLS, EAP-TTLS, EAP-FAST, EAP-AKA, PEAPv0, PEAPv1, and LEAP.

Bonjour

Bonjour is Apple's standards-based, zero-configuration network protocol that lets devices find services on a network. OS X uses Bonjour to discover AirPrint-compatible printers and AirPlay-compatible devices such as Apple TV. Some apps also use Bonjour for peer-to-peer collaboration and sharing.

Bonjour works by using multicast traffic to advertise the availability of services. Multicast traffic is usually not routed, so make sure Apple TV devices or AirPrint printers are on the same IP subnet as the Mac that would use them. If your network is larger and utilizes many IP subnets, you may want to consider using a Bonjour gateway such as those offered by various Wi-Fi infrastructure manufactures.

For more information on Bonjour, refer to this Apple web page.

AirPlay

OS X Yosemite supports the ability to stream content from a Mac to Apple TV even if the devices are on different networks or there's no network available. A Mac with OS X uses Bluetooth Low Energy (BTLE) to begin the discovery process of available Apple TV devices and then establishes a connection directly to Apple TV using Wi-Fi.

In OS X, peer-to-peer AirPlay lets employees use AirPlay directly from a supported iOS device or Mac to an Apple TV without first connecting to the infrastructure network. Peer-to-peer AirPlay eliminates the need to join the right network or disclose Wi-Fi passwords, avoids reachability issues in complex network environments, and provides a direct path from the AirPlay sender to AirPlay receiver to optimize performance. Peer-to-peer AirPlay is enabled by default in iOS 8 and OS X Yosemite v10.10, and doesn't require any user configuration.

Peer-to-peer AirPlay requires:

- Apple TV (3rd generation rev A Model A1469 or later) with Apple TV software v7.0
- Mac computers (2012 or later) with OS X Yosemite v10.10
- iOS devices (2012 or later) with iOS 8

To find the model number of an Apple TV, refer to this Apple Support article.

Peer-to-peer discovery is initiated using BTLE when a user selects AirPlay on a Mac with OS X Yosemite v10.10 or a device with iOS 8. This causes the device and the Apple TV to visit Wi-Fi channel 149 in the 5GHz band and Wi-Fi channel 6 in the 2.4GHz band, where the discovery process continues. Once the user selects an Apple TV and AirPlay starts, the Wi-Fi radios timeshare between channel 149 and whichever infrastructure channel each device is currently using. If possible, the AirPlay sender roams to the same infrastructure channel the Apple TV is using. If neither device is currently using an infrastructure network, the devices will utilize Wi-Fi channel 149 only for AirPlay. Peer-to-peer mirroring adheres to 802.11 standards, sharing Wi-Fi bandwidth with other Wi-Fi devices.

When you deploy Apple TV on a large enterprise Wi-Fi network, consider the following guidelines:

- Connect Apple TV via Ethernet whenever possible.
- Don't use Wi-Fi Channel 149 or 153 for your infrastructure network.
- Don't place or mount the Apple TV behind objects that could disrupt the BTLE and Wi-Fi signals.

Note: Bluetooth Low Energy discovery is a distinct subset of peer-to-peer AirPlay.

AirPlay Discovery

For AirPlay that isn't peer-to-peer, Mac computers will continue to discover AirPlay receivers via Bonjour.

Discovered AirPlay receivers appear in the AirPlay menu.

Connectivity

Infrastructure and peer-to-peer are the two supported modes of AirPlay connectivity. If both the AirPlay sender and receiver support peer-to-peer AirPlay, that's the preferred data path regardless of infrastructure availability. Peer-to-peer AirPlay coexists with infrastructure connections, so the AirPlay client or AirPlay sender can maintain Internet connectivity simultaneously with the peer-to-peer connection. The 5GHz band is better for connecting over peer-to-peer AirPlay because it provides a fast, direct connection between the AirPlay sender and AirPlay receiver.

Note: If peer-to-peer AirPlay isn't supported by either the AirPlay sender or receiver, the infrastructure connection is automatically used.

Security

AirPlay uses AES encryption to ensure content remains protected when mirroring or streaming from a Mac or iOS device to an Apple TV.

AirPlay access to an Apple TV can be restricted by setting an onscreen code or password. Only users who enter the onscreen code (per AirPlay attempt) or password on their Mac or iOS device can send AirPlay content to an Apple TV.

Enabling Require Device Verification requires that a Mac with OS X Mavericks v10.9.2 or later, or an iOS device with iOS 7.1 or later, authenticate on the initial AirPlay connection. Require Device Verification is useful when Apple TV is deployed on an open Wi-Fi network. To ensure Mac or iOS devices are securely paired, the user is prompted to enter a one-time onscreen code. Subsequent connections don't require a code, unless Onscreen Code settings are enabled.

Peer-to-peer AirPlay is always secured with Require Device Authentication. This setting isn't configurable by the user, and it prevents any nearby rogue users from accessing an Apple TV.

Note: For devices not on an infrastructure network, Bonjour advertisement of supported Apple TV devices (Model A1469 or later) is triggered by Bluetooth.

Digital Certificates

OS X supports digital certificates, giving your organization secure access to corporate services. A digital certificate is a form of identification that offers streamlined authentication, data integrity, and encryption. It's composed of a public key, information about the user, and the certificate authority that issued the certificate.

Certificates can be used in a variety of ways. Signing data with a digital certificate helps ensure that information cannot be altered. Certificates can be used to guarantee the identity of the author or "signer." They can also be used to encrypt configuration profiles and network communications to further protect confidential or private information.

For example, the Safari browser can check the validity of an X.509 digital certificate and set up a secure session with up to 256-bit AES encryption. This involves verifying that the website's identity is legitimate and that communication with the website is protected to help prevent interception of personal or confidential data.

Use certificates in OS X

Out of the box, OS X includes a number of preinstalled root certificates. You can easily view these certificates by opening the Keychain Access app located in the Utilities folder.

OS X can update certificates wirelessly if any of the preinstalled root certificates become compromised. To disable this, there's a restriction that prevents over-the-air certificate updates. Supported certificate and identity formats are:

- X.509 certificates with RSA keys
- File extensions cer, .crt, .der, .p12, and .pfx

If you're using a root certificate that isn't preinstalled, such as a self-signed root certificate created by your organization, you can distribute it using one of the methods listed below.

Distribute and manually install certificates

Manually distributing certificates to Mac computers is simple. When a certificate is received, users simply double-click it to open Keychain Access and review the contents. If the certificate matches expectations, users can select the desired keychain and click the Add button. Most user certificates need to be installed in the Login Keychain.

When an identity certificate is installed, users are prompted for the password that protects it. If a certificate's authenticity can't be verified, it's shown as untrusted and the user can decide whether to add it to their Mac.

Install certificates via configuration profiles

If configuration profiles are used to distribute settings for corporate services such as S/MIME email, VPN, or Wi-Fi, certificates can be added to the profile to streamline deployment. This includes the ability to distribute certificates via MDM.

Install certificates via enterprise infrastructure

When configured via MDM or configuration profile, OS X can leverage your existing certificate systems. The Mac can obtain certificates via SCEP or an Active Directory Certificate Authority for either the computer or user identity.

Note: In order to obtain certificates from an Active Directory Certificate Authority, you must bind Mac to Active Directory.

Certificate removal and revocation

To manually remove a certificate that's been installed, launch the Keychain Access app, then search for the desired certificate. Simply select the certificate and delete it from the keychain.

If a user removes a certificate that's required for accessing an account or network, the Mac is no longer able to connect to those services.

An MDM server can view all certificates on a device and remove any certificates it has installed at any time.

Additionally, the Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) protocol are supported to check the status of certificates. When an OCSP- or CRL-enabled certificate is used, OS X validates it to make sure it hasn't been revoked.

Single Sign-On (SSO)

OS X has always been able to leverage Kerberos for single sign on (SSO), and OS X Yosemite continues this support. Single sign on can improve the user experience by only requiring users to enter their password once. It also increases the security of daily app use by ensuring passwords are never transmitted over the air.

The Kerberos authentication system used by OS X is the most commonly deployed single sign-on technology in the world. If you have Active Directory, eDirectory, or Open Directory, it's likely to already have a Kerberos system in place.

Supported apps

Any app that supports Kerberos authentication will work with SSO. This includes many of the OS X built-in apps such as Safari, Mail, Calendar, and Messages, as well as services like file sharing, screen sharing, and SSH (secure socket shell). Many third-party apps such as Microsoft Outlook and Microsoft Lync support Kerberos as well.

Configure single sign on

There are two ways to configure OS X to use SSO:

- Bind Mac to your directory service. In the case of Active Directory or Open Directory, the device will be configured to automatically retrieve a Kerberos Ticket-Granting Ticket (TGT) when a user logs in.
- Place a Kerberos configuration file at /Library/Preferences/edu.mit.Kerberos. This is a standard Kerberos configuration file that contains information about your authentication realm. With this configuration, OS X will not request a TGT at login, but rather when a user connects to a service that supports Kerberos.

Standards-Based Services

With support for the IMAP mail protocol, LDAP directory services, CalDAV calendaring, and CardDAV contacts protocols, OS X can integrate with just about any standards-based environment. And if your network environment is configured to require user authentication and SSL, OS X provides a secure approach to accessing standards-based corporate email, calendars, tasks, and contacts. With SSL, OS X supports 128-bit encryption and X.509 root certificates issued by the major certificate authorities.

In a typical deployment, Mac computers establish direct access to IMAP and SMTP mail servers to send and receive mail, set VIP status in message threads, and sync notes with IMAP-based servers. And Mac can connect to your organization's LDAPv3 corporate directories, giving users access to corporate contacts in Mail, Contacts, and Messages apps. CardDAV support lets users maintain a set of contacts synced with your CardDAV server using the vCard format. Synchronization with your CalDAV server lets users do the following:

- Create and accept calendar invitations.
- View an invitee's calendar free/busy information.
- Create private calendar events.
- Configure custom repeating events.
- View the week numbers in Calendar.
- Receive calendar updates.
- Sync tasks with the Reminders app.

All network services and servers can be within a DMZ subnetwork, behind a corporate firewall, or both.

Microsoft Exchange

OS X can communicate directly with your Microsoft Exchange Server via Exchange Web Services (EWS), enabling use of all your email, calendars, contacts, notes, and tasks in one place. In fact, Mail, included with OS X, supports both basic and certificate-based authentication for Exchange.

If your company currently enables EWS, you already have the necessary services in place to support Mac—no additional configuration is required.

Requirements

Mail supports the following versions of Exchange:

- Office 365
- Exchange 2013
- Exchange 2010
- Exchange 2007 Service Pack 1 Update Rollup 4

Microsoft Exchange Autodiscover Service

OS X supports the Autodiscover service in Exchange Server 2007 and later. This means that when you manually configure a Mac, Autodiscover uses the user's email address and password to determine the correct Exchange Server information.

For more information, refer to Autodiscover Service.

Microsoft Exchange Global Address List

OS X will retrieve contact information from your company's Exchange Server corporate directory. You can access the directory while searching in Contacts, and it's automatically accessed for completing email addresses as you type them.

Calendar

OS X supports the following features of Microsoft Exchange:

- Create and accept calendar invitations.
- View an invitee's calendar free/busy information.
- Create private calendar events.
- Configure custom repeating events.
- View the week numbers in Calendar.
- Receive calendar updates.
- Sync tasks with the Reminders app.

SMB3

SMB3 is the new default protocol for sharing files in OS X Yosemite. SMB3 helps protect against tampering and eavesdropping by encrypting and signing data "in flight."

- **Encryption.** SMB3 provides end-to-end encryption to protect data and secure communication on untrusted networks. SMB3 in Yosemite uses AES-CCM for encryption to ensure communications between client and server are private.
- **Signing.** To guard against tampering, SMB3 adds a signature to every packet transmitted over the wire. SMB3 uses AES-CMAC to validate the integrity of the signature, ensuring the packets have not been intercepted, changed, or replayed and that communication between hosts is authenticated and authorized.
- **Power.** Encryption and signing of SMB3 connections are fast and power efficient. Both AES-CCM for encryption and AES-CMAC for signing are dramatically accelerated on modern Intel CPUs with AES instruction support.
- **Authentication.** SMB supports Extended Authentication Security using Kerberos and NTLMv2.
- **Efficient.** SMB features Resource Compounding, allowing multiple requests to be sent in a single request. In addition, SMB can use large reads and writes to make better use of faster networks as well as large MTU support for blazing speeds on 10 Gigabit Ethernet. It aggressively caches file and folder properties and uses opportunistic locking to enable better caching of data. It's even more reliable, thanks to the ability to transparently reconnect to servers in the event of a temporary disconnect.

- **Transparent reconnect.** Yosemite supports Persistent Handles for transparent failover and reconnects to enterprise SMB3 file servers.
- **Compatible.** SMB is automatically used to share files between two Mac computers running OS X Yosemite, or when a Windows computer running Windows 8 connects to your Mac. OS X Yosemite maintains support for AFP SMB2 and SMB network file-sharing protocols, automatically selecting the appropriate protocol as needed.

Virtual Private Network

Secure access to private corporate networks is available in OS X using established industry-standard VPN protocols. Out of the box, OS X supports Cisco IPSec, L2TP over IPSec, and PPTP. If your organization supports one of these protocols, no additional network configuration or third-party apps are required to connect a Mac to your VPN.

Additionally, OS X supports SSL VPN from popular VPN providers. Users simply install the third-party VPN client to get started. Like other VPN protocols supported in OS X, SSL VPN can be configured manually on the computer, or via configuration profiles or MDM.

OS X supports industry-standard technologies such as IPv6, proxy servers, and split-tunneling, providing a rich VPN experience when connecting to corporate networks. And OS X works with a variety of authentication methods including passwords, two-factor tokens, Kerberos, and digital certificates. To streamline VPN connection in environments where certificate-based authentication is used, OS X features VPN On Demand, which initiates a VPN session when it's needed to connect to specified domains.

Starting with OS X v10.9, individual apps can be configured to utilize a VPN connection independent from other apps on the Mac. This ensures that corporate data always flows over a VPN connection, while other data, such as an employee's personal apps from the Mac App Store, do not. For details, see "Per App VPN" later in this section.

Supported protocols and authentication methods

- **SSL VPN.** Supports user authentication by password, two-factor token, and certificates using a third-party VPN client.
- **Cisco IPSec.** Supports user authentication by password, and machine authentication by shared secret and certificates.
- **L2TP over IPSec.** Supports user authentication by MS-CHAP v2 password, two-factor token, certificate, and Kerberos, and machine authentication by shared secret or certificate.
- **PPTP.** Supports user authentication by MS-CHAP v2 password, certificate, Kerberos, and two-factor token.

Per App VPN

OS X enables VPN connections to be established on a per-app basis. This approach allows for more granular control over which data goes through VPN and which doesn't. With device-wide VPN, all VPN data travels through the same private network regardless of its origin. As more and more personally owned devices are used within organizations, per app VPN provides secure networking for internal-use apps while preserving the privacy of personal activity.

Per app VPN allows each app managed by MDM to communicate with the private network via a a secure tunnel, while excluding other unmanaged apps on the computer from using the private network. Additionally, managed apps can be configured with different VPN connections to further safeguard data. For example, a sales quote app could use an entirely different data center than an accounts payable app, while the user's personal web browsing traffic uses the public Internet. This ability to segregate traffic at the app layer provides separation of personal data and data belonging to the organization.

In order to use per app VPN, a Mac must be managed via MDM and use standard networking APIs. After enabling per app VPN for any VPN connection, you need to associate that connection with the apps that will use it to secure the network traffic for those apps. This is done with the App-to-Per-App VPN mapping payload in a configuration profile.

AppLayerVPNMapping

This is an array of dictionaries, with the keys described below, that determine the App-to-VPN mappings in OS X.

- **Identifier.** The app's bundle ID
- **VPNUUID.** The VPNUUID of the per app VPN to use

Per app VPN is configured with an MDM configuration that specifies which apps and Safari domains are allowed to use the settings. For more information on MDM, see the "Configuration and Management" section below.

VPN On Demand

VPN On Demand allows OS X to automatically establish a secure connection without user action. The VPN connection is started on an as-needed basis, based on rules defined in a configuration profile.

In OS X Yosemite, VPN On Demand is configured using the OnDemandRules key in a VPN payload of a configuration profile. Rules are applied in two stages:

- **Network detection stage.** Defines VPN requirements that are applied when the computer's primary network connection changes
- **Connection evaluation stage.** Defines VPN requirements for connection requests to domain names on an as-needed basis

For example, rules can be used to:

- Recognize when a Mac is connected to an internal network and VPN isn't necessary.
- Recognize when an unknown Wi-Fi network is being used and require VPN for all network activity.
- Require VPN when a DNS request for a specified domain name fails.

Stages

Network detection stage

VPN On Demand rules are evaluated when the computer's primary network interface changes, such as when a Mac changes to a different Wi-Fi network or switches to Ethernet from Wi-Fi. If the primary interface is a virtual interface, such as a VPN interface, VPN On Demand rules are ignored.

The matching rules in each set (dictionary) must all match in order for their associated action to be taken. If any one of the rules does not match, evaluation falls through to the next dictionary in the array until the OnDemandRules array is exhausted.

The last dictionary should define a "default" configuration—that is, it should have no matching rules, only an action. This will catch all connections that haven't matched the preceding rules.

Connection evaluation stage

VPN can be triggered, as needed, based on connection requests to certain domains instead of unilaterally disconnecting or connecting VPN based on the network interface.

On demand matching rules

Specify one or more of the following matching rules:

- **InterfaceTypeMatch.** Optional. A string value of Wi-Fi or Ethernet. If specified, this rule will match when the primary interface hardware is of the type specified.
- **SSIDMatch.** Optional. An array of SSIDs to match against the current network. If the network is not a Wi-Fi network or if its SSID doesn't appear in the list, the match will fail. Omit this key and its array to ignore SSID.
- **DNSDomainMatch.** Optional. An array of search domains as strings. If the configured DNS search domain of the current primary network is included in the array, this property will match. Wildcard prefix (*) is supported. For instance *.example.com would match anything.example.com.
- **DNSServerAddressMatch.** Optional. An array of DNS server addresses as strings. If all the DNS server addresses currently configured for the primary interface are in the array, this property will match. Wildcard (*) is supported. For example 1.2.3.* would match any DNS servers with a 1.2.3. prefix.
- **URLStringProbe.** Optional. A server to probe for reachability. Redirection is not supported. The URL should be to a trusted HTTPS server. The computer sends a GET request to verify that the server is reachable.

Action

This key defines VPN behavior for when all specified matching rules evaluate as true. This key is required. Values for the Action key are:

- **Connect.** Unconditionally initiates the VPN connection on the next network connection attempt.
- **Disconnect.** Tears down the VPN connection and doesn't trigger any new connections on demand.
- **Ignore.** Leaves any existing VPN connection up, but doesn't trigger any new connections on demand.
- **EvaluateConnection.** Evaluates the ActionParameters for each connection attempt. When this is used, the key ActionParameters, described below, is required to specify the evaluation rules.

ActionParameters

This is an array of dictionaries with the keys described below, evaluated in the order in which they occur. Required when Action is EvaluateConnection.

- **Domains.** Required. An array of strings that define the domains for which this evaluation applies. Wildcard prefixes are supported such as *.example.com.
- **DomainAction.** Required. Defines VPN behavior for the Domains. Values for the DomainAction key are:
  - **ConnectIfNeeded.** Brings up VPN if DNS resolution for the Domains fails such as when the DNS server indicates it can't resolve the domain name, if the DNS response is redirected, or if the connection fails or times out.
  - **NeverConnect.** Does not trigger VPN for the Domains.

When DomainAction is ConnectIfNeeded, you can also specify the following keys in the connection evaluation dictionary:

- **RequiredDNSServers.** Optional. An array of IP addresses of DNS servers to be used for resolving the Domains. These servers don't need to be part of the device's current network configuration. If these DNS servers aren't reachable, VPN will be triggered. Configure an internal DNS server or a trusted external DNS server.
- **RequiredURLStringProbe.** Optional. An HTTP or HTTPS (preferred) URL to probe, using a GET request. If DNS resolution for this server succeeds, the probe must also succeed. If the probe fails, VPN will be triggered.

Internet Services

Apple has built Internet services with the same security that OS X delivers throughout the platform—secure handling of data whether at rest on the device or in transit over wireless networks, protection of users' personal information, and threat protection against malicious or unauthorized access to information and services. Each service uses its own powerful security architecture without compromising the overall Mac ease of use.

Internet services help users communicate, create, and back up their personal data, all without compromising your organization's data.

These services include:

- Apple ID
- Find My Mac
- iCloud
- iCloud Keychain
- iMessage
- FaceTime

You can use an MDM solution to restrict the apps a Mac is able to use, or to remove access to the iCloud section of System Preferences.

At Apple, security and privacy are fundamental to the design of all our hardware, software, as well as our services. That's why we respect our customers' privacy and protect it with strong encryption, plus strict policies that govern how all data is handled. For more information, see apple.com/privacy.

Apple ID

An Apple ID is required to access services from Apple. You should understand Apple IDs so you can educate your users about how to set up their own.

An Apple ID is an identity that's used to log in to various Apple services such as FaceTime, iMessage, the iTunes Store, App Store, iBooks Store, and iCloud. These services give users access to a wide range of content to streamline business tasks, increase productivity, and support collaboration.

To get the most out of these services, users should have their own Apple ID. If they don't have one, they can create one even before they receive a Mac. Or they can use Setup Assistant in OS X for an easy, streamlined way to create an Apple ID right on their Mac.

For one-to-one and BYOD deployments, each user should have their own Apple ID. In a shared-use deployment, a corporate-owned Apple ID can be used to deploy content on multiple devices via MDM.

With an Apple ID, each employee can install apps and content provided by the organization without the need for IT to manage the Apple ID on the user's computer.

For more information on Apple IDs refer to this Apple web page.

iCloud

iCloud lets users store personal content such as contacts, calendars, documents, and photos and keep them up to date across multiple devices. iCloud secures your content by encrypting it when sent over the Internet, storing it in an encrypted format, and using secure tokens for authentication. Users can also share documents and projects with other iCloud users anywhere, anytime.

For more information about iCloud, refer to this Apple web page.

For more information about iCloud security and privacy, refer to this Apple Support article.

Note: Some features aren't available in all countries. Access to some services is limited to 10 devices.

Find My Mac

If a device is lost or stolen, it's important to lock and erase it. Find My Mac, part of the iCloud suite, allows users to locate the last reported location of their Mac using the iCloud web page or the Find My iPhone app on an iOS device.

With Find My Mac, a user can remotely play a sound on a lost Mac, lock that system so it can't be erased or used, and even execute a remote wipe. These capabilities all complement the remote lock and wipe abilities of MDM solutions, and a combination of these capabilities can be used at the same time to prevent data loss.

iCloud Keychain

iCloud Keychain lets users securely sync their passwords across Mac computers and iOS devices without exposing that information to Apple.

iCloud Keychain consists of two services:

- Keychain Syncing
- Keychain Recovery

In Keychain Syncing, devices can participate only after user approval, and each keychain item that's eligible to be synced is exchanged with per-device encryption via iCloud key value storage. The items are ephemeral and do not persist in iCloud after being synced.

Keychain Recovery provides a way for users to save their keychain with Apple, without giving Apple the ability to read the passwords and other data it contains. Even if the user has only a single Mac, keychain recovery provides a safety net against data loss. This is particularly important when Safari is used to generate random strong passwords for web accounts, because the only record of those passwords is in the keychain.

Secondary authentication and a secure escrow service are important features of Keychain Recovery. The user's keychain is encrypted using a strong password, and the escrow service only provides a copy of the keychain if a strict set of conditions is met.

iMessage

iMessage is a messaging service for Mac computers and iOS devices that enables one-to-one or group chats. iMessage supports text and attachments such as photos, contacts, and locations. And messages appear on all of a user's registered devices, so they can begin a conversation on one device and continue it on another.

iMessage uses the Apple Push Notification Service and end-to-end encryption with keys known only to the sending and receiving devices. Apple can't decrypt messages, and messages aren't logged.

FaceTime

FaceTime is Apple's video and audio calling service. FaceTime calls use the Apple Push Notification Service to establish a connection, then use Internet Connectivity Establishment (ICE) and Session Initiation Protocol (SIP) to create an encrypted stream. Users can communicate between any mix of Mac computers and iOS devices using FaceTime.

As with iMessage, FaceTime connections feature end-to-end encryption. Apple cannot decrypt the content streams.

Apple Push Notification service

Many services rely on the Apple Push Notification service (APNs). The APNs is a key part of how OS X and iOS learn of updates, MDM policies, and incoming messages. In order for your Mac to work with these services, you need to allow network traffic from the computer to Apple's network on port 5223, with a fallback option of port 443.

This traffic is a secured, binary protocol specific to APNs, and thus can't go through a proxy. Attempts to inspect the traffic or reroute it will result in the client, the APNs, and push provider servers marking the network conversation as compromised and invalid.

There are multiple layers of security applied to APNs at the endpoints and the servers. To read technical information about these precautions, refer to the Local and Remote Notification Programming Guide.

Security

OS X is built with multiple layers of security, so Mac can securely access network services and protect important data. OS X also provides secure protection through the use of password policies that can be delivered and enforced via MDM. And if a Mac falls into the wrong hands, a user or IT administrator can use a remote command to erase all private information.

Ensuring the security of Mac computers for enterprise use involves:

- Methods that prevent unauthorized use of the system
- Protecting data at rest, even when a computer is lost or stolen
- Networking protocols and the encryption of data in transmission
- Enabling apps to run securely, without compromising platform integrity

These capabilities work together to provide a secure computing platform. To learn more about OS X security, refer to this Apple web page.

Device and Data Security

Establishing strong policies for access to Mac computers is critical to protecting your organization's information. Passwords are the frontline of defense against unauthorized access, and they can be configured and enforced via MDM or directory service. OS X also provides secure methods for configuring Mac in an IT environment, where specific settings, policies, and restrictions must be in place. These methods provide flexible options for establishing a standard level of protection for authorized users.

Password policies

A password keeps unauthorized users from accessing data on the Mac. You can also set complex password polices via MDM or configuration profiles.

OS X lets you choose from an extensive set of password policies to meet your security needs, including:

- Require password
- Require alphanumeric value
- Minimum password length
- Minimum number of complex characters
- Maximum password age
- Time before autolock
- Password history
- Grace period for screen lock
- Maximum number of failed attempts
- Length of account lockout after failed attempts

Policy enforcement

You can distribute policies in a configuration profile that users install. And you can define a profile so that deleting it is only possible with an administrator password, or so that it's locked to the Mac and can't be removed without completely erasing all of the computer's contents. Password settings can be configured remotely using MDM solutions that push policies directly to the Mac, so you can enforce and update those policies without any action by the user.

If you're using a directory service such as Active Directory, the Mac can automatically use your domain password settings. If both Active Directory and MDM policies exist, the more stringent policy is applied.

FileVault 2

OS X Yosemite continues the advancement of Apple's full-disk encryption technology. On a Mac with an Intel Core i3 processor or greater, FileVault 2 is enabled in Setup Assistant and will use the hardware AES encryption those processors provide.

By leveraging FileVault 2, organizations can obtain comprehensive data-at-rest protection on Mac.

FileVault 2 can be managed via MDM with the following policies applied:

- Require FileVault 2.
- Use an institutional recovery key.
- Allow the user to set a personal recovery key.
- Force escrow of a personal key to a local server.
- Destroy in-memory FileVault 2 keys when computer is in sleep mode.

Further flexibility, such as key replacement and rotation, predefined user accounts, and recovery key validation can be found in the command-line *fdesetup* tool on every Mac.

The cryptographic modules in OS X have been validated to comply with U.S. Federal Information Processing Standard (FIPS) 140-2 Level 1. This validates the integrity of cryptographic operations in Apple apps and third-party apps that properly utilize OS X cryptographic services.

For more information, refer to these Apple Support articles:

OS X: Security Certifications and Validations

OS X: Apple FIPS Cryptographic Modules v4.0

Encrypted disks

Using the same technology built into FileVault 2, users can encrypt any disk that they use with their Mac, right in the Finder. Simply right-click an unencrypted disk and choose Encrypt Volume in order to secure the contents of the device.

Encrypted containers

OS X includes a robust disk imaging system that allows for the creation of encrypted virtual disks. These volumes are simple to create with the Disk Utility app, support up to 256-bit AES encryption, and work like any other disk on a Mac.

Users commonly use encrypted disk images to provide additional protection for sensitive documents and to protect data when it's sent to another user.

Email S/MIME

OS X continues to support per-message S/MIME, so S/MIME users can choose to always sign and encrypt email by default, or selectively sign and/or encrypt individual messages for greater control over the security of each mail message.

Certificates for use with S/MIME can be delivered to the Mac via configuration profile, MDM, SCEP, or Microsoft Active Directory Certificate Authority. This gives IT the flexibility needed to ensure that users always have the appropriate certificates installed.

External mail address marking

OS X supports creating a domain list of specific suffixes. Mail messages that aren't addressed to domains in the approved list are displayed in red. For example, if a user with example.com and group.example.com in their known domains list were to enter anyone@acme.com in a Mail message, that address would be marked clearly so the user would know the domain acme.com wasn't on their list.

Remote wipe

OS X fully supports remote wipe. If a Mac is lost or stolen, an administrator or the computer's owner can issue a remote-wipe command that removes all data from the system. A remote-wipe command may be initiated from an MDM solution or using the Find My Mac feature of iCloud.

Local wipe

Using FileVault 2 fully protects the contents of the OS X boot disk from tampering or inspection. IT administrators may start up a Mac from the OS X Recovery disk, built into every Mac, to locally wipe the contents of the boot drive securely without the need for additional devices or software.

Secure networking

Users must be able to access corporate networks from anywhere in the world. But it's also important for organizations to ensure their users are authorized and that data is protected during transmission. Built-in network security technologies in OS X accomplish these security objectives for both Wi-Fi and wired Ethernet connections.

OS X network security supports:

- Built-in Cisco IPSec, L2TP, PPTP
- SSL VPN via Mac App Store apps
- SSL/TLS with X.509 certificates
- WPA/WPA2 Enterprise with 802.1X
- Certificate-based authentication
- Shared-secret and Kerberos authentication
- RSA SecurID and CRYPTOCard hardware tokens

VPN

Many enterprise environments have some form of VPN deployed. These secure network services typically require minimal setup and configuration to work with OS X, which integrates with a broad range of commonly used VPN technologies.

For details about Virtual Private Networks, refer to this Apple web page.

IPSec

OS X supports IPSec protocols and authentication methods. For details, refer to the previous "Supported protocols and authentication methods" section.

SSL/TLS

OS X supports SSL v3 and Transport Layer Security (TLS) v1.0, 1.1, and 1.2. Safari, Calendar, Mail, and other Internet apps automatically use SSL and TLS to enable an encrypted communication channel between OS X and corporate services.

WPA/WPA2

OS X supports WPA2 Enterprise to provide authenticated access to your enterprise network over both Wi-Fi and Ethernet. WPA2 Enterprise uses 128-bit AES encryption, so user data is protected. And with support for 802.1X, the Mac can be integrated into a broad range of RADIUS authentication environments.

OS X supports these 802.1X authentication protocols:

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- EAP-AKA

- PEAP v0, v1
- LEAP

FaceTime and iMessage encryption

Each FaceTime session and iMessage conversation is encrypted end to end. OS X creates a unique ID for each user, ensuring communications are encrypted, routed, and connected properly.

App Security

To ensure apps can't be tampered with, OS X includes a sandboxed approach to app runtime protection and app signing. OS X also has a framework called Keychain, which facilitates secure storage of app and network service credentials in an encrypted storage location. For developers, OS X offers the Common Crypto framework that can be used to encrypt app data.

Runtime protection

Apps from the Mac App Store are sandboxed on OS X to restrict their access to data stored by other apps. System files, resources, and the kernel are also shielded from the user's app space. If one app needs to access data from another app, it can do so only by using the APIs and services provided by OS X.

Code signing

All Mac App Store apps must be signed. The apps included with every Mac are signed by Apple. Most third-party apps are signed by the developer using a certificate issued by Apple. This ensures that apps haven't been tampered with or altered. Runtime checks are made to ensure that an app hasn't become untrusted since it was last used.

Apps from outside the Mac App Store, such as Microsoft Office, are normally signed with an Apple-issued developer certificate as well. This allows you to validate that the app is genuine and hasn't been tampered with.

Apps developed in-house should also be signed so that you can validate their integrity.

Code signing is used extensively within OS X via a Mandatory Access Control (MAC) system. For example, code signing is used to identify allowed apps and to allow access through the Firewall.

Gatekeeper

Gatekeeper is a feature in OS X that allows you to select the level of code signing required to run an app on a Mac.

Gatekeeper supports three levels of validation to allow apps to run:

- Mac App Store
- Mac App Store and identified developers
- Anywhere

The accepted Gatekeeper setting may be set with MDM. When using managed settings, these additional Gatekeeper controls are available:

- Do not allow user to override Gatekeeper settings
- Custom system policy certificates and settings

Secure authentication framework

OS X provides a secure, encrypted keychain for storing digital identities, user names, and passwords. Keychain data is protected with Access Control Lists (ACLs), so credentials stored by third-party apps can't be accessed by apps with a different identity unless the user explicitly approves them. This provides the mechanism for securing authentication credentials on Mac computers across a range of apps and services within your organization.

Common Crypto architecture

App developers can use encryption APIs to protect their app data. Data can be symmetrically encrypted using proven methods such as AES, RC4, or 3DES. Current Intel Mac computers also provide hardware acceleration for AES encryption and SHA1 hashing, maximizing app performance.

App entitlements

By default, a sandboxed OS X app has very limited privileges. Developers must explicitly add entitlements to use most features such as iCloud, network access, or keychains. This ensures that apps can't grant themselves data access they weren't deployed with. OS X apps must ask for explicit user permission before using many Mac features such as location, contacts, camera, and stored photos.

Configuration and Management

This section describes the complete set of tools, programs, and services available to support your OS X deployments. You can streamline deployment through management techniques that simplify account setup, configure institutional policies, distribute apps, and apply restrictions. You can configure OS X preferences and accounts manually, or with an MDM solution. Users can then do most of the initial setup themselves through Setup Assistant, built into OS X. And after your Mac computers are configured and enrolled in MDM, they can be managed by your IT department.

MDM gives your organization the ability to securely enroll devices in the corporate environment, configure and update settings, monitor policy compliance, deploy apps, and remotely wipe or lock managed systems. Many MDM solutions are available for different server platforms. Each solution offers its own management console, features, and pricing. Before you choose an MDM solution, review this section to see which features are most important to your organization.

Several different configuration workflows and capabilities are possible, depending on who owns the Mac computers and how they are deployed. For more information, see the previous "Deployment Models" section.

Setup Assistant

OS X includes Setup Assistant to activate each new or erased Mac, configure basic settings, and personalize preferences such as language, location services, iCloud, and Find My Mac. Users can use these features on a Mac right out of the box to get up and running, or your organization can perform these basic setup tasks. Setup Assistant also lets users create a personal Apple ID, if they don't have one already.

Mac systems enrolled in the Device Enrollment Program and managed by MDM can skip these screens in Setup Assistant:

- Restore from backup. Doesn't restore from backup
- Apple ID. Doesn't prompt you to sign in with, or create, an Apple ID
- Terms of Service. Skips the Terms and Conditions screen
- Send diagnostics. Doesn't automatically send diagnostic information
- Location. Doesn't enable location services
- Registration. Doesn't show the registration screen

For more information about the Device Enrollment Program, refer to this Apple web page.

Configuration Profiles

A configuration profile is an XML file used to distribute configuration information to Mac computers. Configuration profiles automate the configuration of settings, accounts, restrictions, and credentials. They can be installed through an email attachment, downloaded from a web page, or installed on systems with MDM. If you need to configure a large number of Mac computers, or just prefer a hands-off, over-the-air deployment model, you can deliver configuration profiles through MDM.

Configuration profiles can be signed, preventing anyone from changing the settings contained in the profile. You can also mark a profile as locked to the Mac, so once installed, it can only be removed by wiping the system of all data or by entering a password (optionally).

With the exception of passwords, users can't change the settings provided in a configuration profile. Accounts that are configured by a profile, such as Exchange accounts, can only be removed by deleting the profile.

For more information, refer to Configuration Profile Key Reference on the Apple Developer website.

Mobile Device Management

OS X has a built-in MDM framework that lets third-party MDM solutions wirelessly interact with Mac. This lightweight framework was designed for OS X and iOS devices, and is powerful and scalable enough to configure and manage all the devices within an organization.

With an MDM solution in place, you can securely enroll devices in an organization, configure and update settings, monitor compliance with corporate policies, and remotely wipe or lock managed devices. MDM for OS X gives you a simple way to let users access network services while ensuring Mac computers are properly configured—no matter who owns them.

MDM solutions use APNs to maintain persistent communication with systems across both public and private networks. MDM requires multiple certificates to operate, including an APNs certificate to talk to clients and an SSL certificate to communicate securely. MDM solutions may also sign profiles with a certificate.

Most certificates, including an APNs certificate, must be renewed annually. When a certificate expires, an MDM server can't communicate with clients until the certificate is updated. Be prepared to update all MDM certificates before they expire. For more information about MDM certificates, refer to the Apple Push Certificates Portal.

In addition to device management, MDM also enables distribution, management, and configuration of apps and books purchased through the Volume Purchase Program, directly from a third-party software developer, or developed in-house.

To enable management, computers are enrolled with an MDM server using an enrollment configuration profile. This can be done directly by the user. For company-owned devices, MDM enrollment can be automated using the Device Enrollment Program (DEP), described below. When an administrator initiates an MDM policy, option, or command, a Mac receives notification of the action through the APNs. With a network connection, devices can receive APNs commands anywhere in the world.

Enrollment

Enrolling Mac in MDM enables cataloging and asset management. The enrollment process typically leverages Simple Certificate Enrollment Protocol (SCEP), which lets a Mac create and enroll unique identity certificates for authentication to MDM services.

In most cases, users decide whether or not to enroll their system in MDM, and they can disassociate from MDM at any time. Organizations should consider incentives for users to keep their computers managed. For example, require MDM enrollment for Wi-Fi network access by using the MDM solution to automatically provide the wireless credentials. When a user leaves MDM, their Mac attempts to notify the MDM server and their Wi-Fi access is removed.

The DEP can also be used to automatically enroll devices your organization owns in MDM during initial setup. Users with these devices won't be able to bypass MDM or unenroll their devices.

For more information about the DEP, refer to this Apple web page.

Configure

Once a Mac is enrolled, it can be dynamically configured with settings and policies by the MDM server, which delivers configuration profiles to the computer, which are automatically and silently installed by OS X.

Configuration profiles can be signed and locked—preventing the settings from being altered or shared—ensuring that only trusted users and systems configured to your specifications can access your network and services. If a user disassociates a Mac from MDM, all settings installed by MDM are removed.

The Profiles System Preference shows users what has been configured by MDM including accounts, apps, books, and restrictions.

Accounts

MDM can help your users get up and running quickly by setting up their email and other accounts automatically. Depending on the MDM solution you use and its integration with your internal systems, account payloads can also be prepopulated with a user's name, email address, and certificate identities for authentication and signing, as applicable.

MDM can configure the following types of accounts:

- Mail
- Exchange
- Calendar
- Subscribed Calendars
- Contacts
- LDAP
- VPN
- Identity
- Jabber
- 802.1X

Queries

An MDM server has the ability to query devices for a variety of information. This includes hardware information such as serial number, device UUID, MAC address, or FileVault 2 encryption status. And it includes software information such as the OS X version, restrictions, and a detailed list of all apps installed on the computer. This information can be used to help ensure that users maintain the appropriate set of apps. OS X allows queries about installed certificates, and the app assignment account hash of the logged-in user.

Management tasks

When a device is managed, it can be administered by the MDM server through a set of specific tasks including:

- **Changing configuration settings.** A command can be sent to install a new or updated configuration profile on a Mac. Configuration changes happen silently without user interaction.
- **Locking a computer.** If a Mac needs to be locked immediately, a command can be sent to lock the system with the current password.
- **Remotely wiping a computer.** If a Mac is lost or stolen, a command can be sent to erase all of the data on the system. Once a remote-wipe command is received, it can't be undone.
- **FileVault 2 encryption.** Indicates the state of FileVault 2 encryption and whether a personal recovery key, an institutional recovery key, or both have been set.

Certain tasks can be queued if a Mac is running Setup Assistant. Those tasks are:

- Invitation to the VPP
- Install apps
- Install media
- Lock a device

Managed apps

Distributing apps to your users can help them be more productive at work. But distribution is only the first step. Organizations also need to control how those apps connect to internal resources and how data security is handled when an employee transitions out of the organization—protecting corporate data without impacting the user's personal apps and data.

Managed apps in OS X v10.10 or later let your organization distribute free, paid, and in-house enterprise apps using MDM, providing the right balance between institutional security and user personalization.

MDM servers can deploy apps from the Mac App Store, from third-party developers, and developed in-house to computers over the air. Both paid and free Mac App Store apps can be managed by an MDM server using VPP managed distribution. For more information about managed distribution with MDM, refer to the Volume Purchase Program.

The VPP offers two options for installing Mac apps:

- Users with a personal Mac can install the app from the Mac App Store.
- On corporate-owned Mac computers enrolled with MDM, pushed app installation occurs silently, or users can install from the Mac App Store.

New in OS X Yosemite is the ability to install enterprise apps, whether developed in-house or by a third-party software developer, via MDM. This increased app management capability allows for MDM to manage the installation of Mac apps, regardless of their source. Apps that are not available from the Mac App Store can now be installed alongside your VPP apps. This allows for complete configuration of, and software delivery to, a Mac using only the built-in MDM support.

Installation of enterprise Mac apps requires the app to either be self-contained in the Applications folder on a Mac or installed by an Installer flat package signed with a valid distribution signature.

Managed apps can be disabled remotely by the MDM server, or when a user removes their own Mac from MDM. If a VPP app is still assigned to the user, or the user redeemed an app code using a personal Apple ID, that app can be downloaded again from the Mac App Store, but won't be managed. If an app is revoked from a user, it will continue to function for a limited time. Eventually the app is disabled and the user is informed that they need to purchase their own license to continue using it.

Managed books

With OS X and MDM, you can distribute and manage books, ePubs, and PDFs that you create or purchase via MDM—allowing for seamless management of training materials and other business documents.

Books, ePubs, and PDFs distributed by MDM have the same properties as other managed documents—they can be shared only with other managed apps or emailed using managed accounts. Books purchased through the VPP can be distributed through managed book distribution, but can't be revoked and reassigned. A book already purchased by a user can't be managed unless that book is explicitly assigned to the user through the VPP.

Profile Manager

In addition to third-party MDM solutions, Apple offers an MDM solution called Profile Manager, a service of OS X Server. Profile Manager makes it easy to configure Mac and iOS devices to your organization's specifications.

Profile Manager provides three components:

- **Over-the-air configuration.** Streamline the configuration of corporate-owned devices. Enroll Mac computers in MDM during activation and skip basic setup steps to get users up and running quickly.
- **Mobile device management service.** Profile Manager provides an MDM service that lets you remotely manage enrolled devices. After a Mac is enrolled, you can update its configuration over the network without user interaction, as well as perform other tasks. MDM is supported on Mac computers with OS X v10.7 or later installed.
- **App and book distribution.** Profile Manager can distribute apps and books purchased through the VPP. App and book assignment is supported on a Mac with OS X v10.9 or later installed.

For more information about Profile Manager, refer to this Apple web page.

Device Enrollment Program

The DEP provides a fast, streamlined way to deploy Mac computers your organization has purchased directly from Apple or participating Apple Authorized Resellers or carriers. You can automatically enroll Mac computers in MDM without having to physically touch or prep the systems before users get them. And you can further simplify the setup process for users by removing specific steps in Setup Assistant. You can also control whether or not a user can remove the MDM profile from their Mac. For example, you can order Mac computers from Apple, configure all the management settings, and have the systems shipped directly to each user's home address. Once a Mac is unboxed and activated, the computer enrolls in your MDM and all management settings, apps, and books are ready for the user.

The process is simple. After enrolling in the program, administrators log in to the DEP website, link the program to their MDM server, and "claim" the Mac computers purchased from Apple or participating Apple Authorized Resellers or carriers. The Mac systems can then be assigned to users via MDM. Once a user has been assigned, any MDM-specified configurations, restrictions, or controls are automatically installed.

Computers must meet the following criteria to be eligible for assignment using the DEP:

- Must be purchased directly from Apple, using your enrolled and verified Apple Customer Number(s), or be purchased from a participating Apple Authorized Reseller or carrier
- Must be ordered after March 1, 2011 (using the approved Apple Customer Numbers)

Note: The Device Enrollment Program isn't available in all countries or regions.

Eligible Mac systems are available for assignment to your MDM servers on the Apple Deployment Programs website. You can also look up devices by type and serial number within those orders. After new orders ship, you can search for them on the DEP website and automatically assign them to a specific MDM server. For example, when you place an order for 5000 MacBook Air computers, you can use the order number to assign all or a specific number of the systems to an existing authorized MDM server. You can also assign computers to a specific MDM server by serial number. This method is helpful when a Mac you need to assign is in your physical possession.

After a Mac has been assigned to an MDM server in the program, profiles and additional features may be applied using your organization's MDM server. These features include:

- Mandatory configuration
- Requiring authentication to your enterprise systems to complete setup
- Skipping steps in Setup Assistant

For more information about the Device Enrollment Program, refer to this Apple web page.

App and Book Distribution

OS X comes with a collection of powerful built-in apps that let employees accomplish everyday tasks right out of the box—from managing email and calendars to keeping track of contacts and web content. And the additional functionality users need to be productive can come from thousands of third-party apps for OS X available on the Mac App Store or from custom enterprise apps developed in-house or by third-party developers.

There are several ways to deploy apps and books to Mac computers throughout your organization. The most scalable method is to purchase them through the VPP and assign them to users with MDM. Your organization can also create apps in-house and deploy them by joining the Mac Developer Program.

When deploying apps and books, you should consider the following:

- Volume Purchase Program (VPP)
- Apps created by a third-party developer
- Apps and books developed in-house
- Caching Server

Volume Purchase Program

The VPP gives organizations a simple way to purchase apps and books in volume and distribute them to employees, contractors, teachers, or students. All paid and free apps on the Mac App Store and books on the iBooks Store are eligible for purchase through the program.

MDM solutions can be integrated with VPP, enabling you to assign apps and books to specific users or groups. When a user no longer needs an app, you can use MDM to revoke and reassign it to a different user. And each app or book is automatically available for download on a user's Mac. Once distributed, books remain the property of the recipient and aren't revocable or reassignable.

Note: Redemption codes can also be purchased through VPP for distribution to users or in situations where MDM isn't applicable.

The VPP website for medium and large organizations is the Volume Purchase Program for Business. The VPP for Business lets you get apps for OS X and books on a wide range of business topics.

For more information, refer to Apple Deployment Programs Help.

Note: The Volume Purchase Program isn't available in all countries or regions.

Enroll in the Volume Purchase Program

To purchase apps in volume, first enroll and create an account with Apple. You'll need to provide information about your organization, such as a D&B D-U-N-S number (if you're a business) and contact information. You'll also need to create an Apple ID that's used only for administration of this program.

Purchase apps and books in volume

To purchase apps and books for your business or institution, use the Apple ID associated with your Volume Purchase Program account to log in to the VPP website. Search for what you want to purchase, then indicate the number of copies needed. You can pay with a corporate credit card or VPP Credit procured using a purchase order. And there's no limit to the number of copies of an app you can purchase. The VPP website lists each of your purchases by order number, app or book name, total cost, and number of licenses.

For each copy of an app or book purchased, you can choose either redemption codes or managed distribution.

If you choose managed distribution, apps will be available for assignment via your MDM solution, provided it's linked to your VPP account and has a valid token.

If you choose to purchase redemption codes, you'll be notified by email when they're ready. Download a spreadsheet containing the redemption codes for each item, in the quantity purchased, from the account section of the VPP website. For example, if you were to purchase seven copies of FileMaker Pro, you would receive seven redemption codes for the app. The spreadsheet also contains a redemption URL for each redemption code. These URLs let users download and install the apps on their Mac without entering a redemption code.

You can purchase redemption codes only for paid apps and books. Both free and paid apps and books are available for managed distribution.

Managed distribution

When you buy apps and books in volume, you can distribute them via MDM using managed distribution to assign them to users on OS X Mavericks v10.9 or later or iOS 7 or later. You can also use redeemable codes sent directly to your users. When they no longer need an app or when they leave your organization, you can reassign it to a different user. Books can't be revoked after they're assigned.

Before MDM is used to assign apps to users, you'll need to link your MDM server to your VPP account using a secure token. You can download this secure token to your MDM server by accessing your account summary from the VPP store. For more information, refer to Apple Deployment Programs Help.

In order for users to participate in managed distribution via VPP, they must first be invited. When a user accepts an invitation to participate in managed distribution, their personal Apple ID is linked to your organization. The user doesn't need to tell you their Apple ID, and there's no need for you to create and provide Apple IDs for their use.

Note: Registering users and assigning apps and books can happen at any time, including before Mac systems are enrolled in MDM. In fact, enrolling Mac in MDM is optional for simply assigning apps and books to users.

Once an app is assigned to a user via MDM, it appears in the purchase history of the Mac App Store for that user. The user can be prompted to accept installation of the app, or in the case of a Mac enrolled in MDM, the app can be silently installed.

Distributed redemption codes

You can distribute redemption URLs by email or post them on a website made accessible to the appropriate groups and users. You may want to create a website that offers a catalog of the apps purchased and that issues redemption codes to authorized users. Many third-party MDM solutions provide a way to centrally manage and distribute codes.

To install the apps and books purchased for them, users open the redemption URL on their Mac. This takes them directly to the Mac App Store with the redemption code already entered, so all they need to do is authenticate with their Apple ID. It's the same process as with any other app from the Mac App Store, but because you've provided the prepaid redemption code, users aren't charged for the purchase.

Note: Each redemption code can be used only once. Each time a redemption code is used, an updated version of the purchase spreadsheet becomes available on the VPP website. Download the spreadsheet to see how many codes have been used, and to view the remaining redemption codes.

Once a user installs an app, it's updated just like any other app from the Mac App Store.

Third-party apps

Your organization may need to install apps that aren't available on the Mac App Store. With OS X, you can still install these apps by uploading either the app bundle or an Installer package to your MDM solution.

Note: In order to upload a Mac app to your MDM solution, it must either be in a single app bundle that's installed in the Applications folder, or be packaged in a signed Installer flat-package.

If you need more flexibility in your software deployment, you may want to consider traditional client management solutions. These often combine the ease of using MDM with an additional client agent that's installed to enable more complex interactions on each Mac.

In-House Apps

The Mac Developer Program offers a complete, integrated process for developing, testing, and distributing your apps to users across your organization. You can distribute in-house apps either by hosting them on a simple web server you create internally, or using an MDM or app management solution.

Deploy in-house apps

To develop and deploy in-house apps for OS X:

1. Register for the Mac Developer Program.
2. Prepare your app for distribution.
3. Sign your app with your distribution certificate.
4. Deploy the app to your users.

Register for app development

Although you can develop and deploy apps using the free Mac Developer Program web membership, enrolling in the full program gives you access to Developer Technical Support and signing certificates. Without a signing certificate you can't take advantage of powerful features such as app sandboxing, entitlements, or iCloud.

Once you register for the Mac Developer Program, you can request a developer certificate and provisioning profile. Use these during development to build and test your app. The development provisioning profile lets apps signed with your developer certificate run on registered devices. The ad hoc profile expires after three months and specifies which devices (by device ID) can run development builds of your app. Distribute your developer-signed build and the development provisioning profile to your development team and app testers.

Prepare apps for distribution

After you finish development and testing and are ready to deploy your app, sign your app using your distribution certificate. The designated Team Agent or the Admin for your program membership creates the certificate at the Mac Dev Center website or via Xcode.

Once you have the distribution certificate installed in the keychain on your development Mac, you can select it in Xcode to enable signing of your finished app.

Distribute in-house apps

Once you've completed testing and signing of your in-house Mac app you can distribute it via MDM or client management solution for a managed deployment. Or simply provide access to the app for users to install on their own.

If you signed your app with a certificate generated by a Certificate Authority (CA) other than Apple's, you'll need to distribute your CA Root Certificate and allow Gatekeeper to trust it. Both of these tasks can be accomplished via MDM.

In-House Books

OS X Yosemite brings major enhancements with the introduction of managed distribution for books. This feature lets you assign books to users via MDM and control content syncing, so the books remain under your organization's control. PDFs and ePubs you create can be assigned to users, revoked, and reassigned to different users when no longer needed, just like in-house apps.

Deploy Apps and Books

There are two ways to deploy apps and books:

- Use your MDM server to instruct managed devices to install an in-house or Mac App Store app, if your MDM server supports it.
- Post the app on a secure web server, so users can access it and perform the installation themselves.

Install apps and books using MDM

An MDM server can manage third-party apps from the Mac App Store as well as in-house apps.

To install an app, the MDM server sends an installation command to a Mac. If the app is from the Mac App Store, it will be downloaded and installed from Apple. If it's an in-house or third-party app it will be installed from your MDM solution.

On OS X Mavericks v10.9 or later, VPN connections can be specified at the app layer, so only the network traffic for that app is in the protected VPN tunnel. This ensures that private data remains private, and public data doesn't get mixed with it.

An MDM server can install books from the iBooks Store that you've assigned to a user through the VPP. MDM can also install managed PDFs, ePubs, and ebooks created in iBooks Author from your own servers and update them with newer versions, as needed. The server can prevent managed books from being backed up. Managed books will be removed when a user unenrolls from MDM.

Caching Server

OS X makes it so easy to access digital content that some users may request many gigabytes of apps, books and software updates over your organization's network. The demand for these assets comes in spikes—first with initial Mac deployment, then sporadically as users discover new content or as content is updated over time. These downloads can cause surges in demand for Internet bandwidth.

Caching Server is a service of OS X Server that saves previously requested content on your organization's local network. This reduces the bandwidth needed to download content. It does this by reducing outbound Internet bandwidth on private networks (RFC 1918) and storing cached copies of requested content on the local area network.

Caching Server in OS X Server caches the following types of content for Mac and iOS devices:

- OS X and iOS software updates
- Mac App Store and App Store apps
- Mac App Store and App Store updates
- Books from the iBooks Store
- iTunes U courses and content
- High-quality voices and language dictionaries

iTunes also supports Caching Server. The following types of content are supported by iTunes 11.0.4 or later (on both Mac and Windows):

- App Store apps
- App Store updates
- Books from the iBooks Store

Larger networks benefit from having multiple Caching Servers in place to take advantage of server content peering. For many deployments, configuring Caching Server is as simple as turning on the service. With Caching Server on OS X Server Yosemite, a NAT environment for the server and all devices that use it is no longer required. Caching Server can now be used on networks consisting of publicly routable IP addresses. Mac computers running OS X Mavericks v10.9 or later automatically contact a nearby Caching Server without any additional configuration.

For more information, refer to OS X Server Support.

Here's an explanation of the Caching Server workflow:

1. When a Mac on a network with one or more Caching Servers requests content from the iTunes Store or Software Update server, the Mac is referred to a Caching Server.
2. The Caching Server first checks to see whether it already has the requested content in its local cache.
    - If it does, it immediately begins serving the content to the Mac.
    - If the Caching Server doesn't have the requested asset, it attempts to download the content from another source. Caching Server 2 or later includes a peer replication feature that can use other Caching Servers on the network, if those servers have already downloaded the requested content.
3. As the Caching Server receives download data, it relays the data immediately to any Mac clients that have requested it and simultaneously caches a copy to disk.

Planning for Support

A robust service and support strategy is a key element to a successful deployment. AppleCare offers end-user technical support, comprehensive hardware coverage, and IT department support.

End-User Support | Comprehensive Hardware Coverage

AppleCare Protection Plan

Every Mac comes with a one-year limited warranty and complimentary telephone technical support for 90 days after the purchase date. This service coverage can be extended to three years from the original purchase date with the AppleCare Protection Plan for Mac or Apple Display. Your users will have the ability to directly contact Apple seven days a week, schedule out support calls, and start live chats. For hardware repairs, they can visit an Apple Authorized Service Provider or arrange for onsite service repairs for Mac desktops.

IT Department Support

AppleCare Help Desk Support

AppleCare Help Desk Support provides priority telephone access to Apple's senior technical support staff. It includes a suite of tools to diagnose and troubleshoot Apple hardware, which can help organizations manage resources more efficiently, improve response time, and reduce training costs. AppleCare Help Desk Support covers an unlimited number of support incidents for hardware and software diagnosis and troubleshooting, and issue isolation for Mac computers. Additionally, AppleCare Help Desk Support includes AppleCare Technician Training. This self-paced training will prepare your staff to diagnose and repair Mac computers in-house.

AppleCare OS Support

AppleCare OS Support includes AppleCare Help Desk Support, in addition to incident support. AppleCare OS Support provides support for system components, network configuration, and administration; integration into heterogeneous environments; professional software apps, web apps, and services; and technical issues requiring the use of command-line tools for resolution.

AppleCare OS Support offers three levels of support to meet your organization's needs:

- **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.

AppleCare for Mac Users

Every Mac comes with a one-year limited warranty and complimentary telephone technical support for 90 days after the purchase date. Extend your coverage to three years from your hardware product's original purchase date with the AppleCare Protection Plan. You get direct, one-stop access to Apple's award-winning telephone technical support for questions about Apple hardware, OS X, and Apple applications such as iLife and iWork. And you get global repair coverage for your Mac and Apple display through convenient service options.

AppleCare Self-Servicing Account Program

If your organization meets certain criteria, you may be able to enroll in the AppleCare Self-Servicing Account (SSA) program to perform in-house repairs on your Mac computers. The SSA program is designed for organizations that want the convenience of repairing their own products. Program participants ("Self-Servicers") must have an installed base of at least 50 Mac computers, are only authorized to repair the products they own or lease, and may not perform repair work for third parties.

There are two levels of membership in the SSA program:

- **Parts Only.** Self-Servicers participating at the Parts-Only tier receive replacement parts for covered repairs at no charge, but do not receive labor compensation. Self-Servicers participating at this tier typically have extended service agreements that only include parts coverage.
- **Parts and Labor.** Self-Servicers participating at the Parts-and-Labor tier receive replacement parts for covered repairs at no charge, and labor compensation for certain covered repairs when coverage includes labor. Self-Servicers with extended service agreements that don't include labor coverage aren't eligible to participate at the Parts-and-Labor tier.

For more information on the SSA program, refer to this Apple web page.

Please work with your designated Apple sales representative to discover the right AppleCare solution for your organization.

[1]FaceTime calling requires a FaceTime-enabled device for the caller and recipient and a Wi-Fi connection. FaceTime over a cellular network requires iPhone 4s or later, iPad with Retina display, or iPad mini with cellular data capability. Availability over a cellular network depends on carrier policies; data charges may apply. [2]Some features require a Wi-Fi connection. Some features are not available in all countries. Access to some services is limited to 10 devices.