macOS Security

Overview for IT

Apple designed the macOS platform with an integrated approach to hardware, software, and services that provides security by design and makes it simple to configure, deploy, and manage. macOS includes the key security technologies that an IT professional needs to protect corporate data and integrate within secure enterprise networking environments. Apple has also worked with standards bodies to ensure compliance with the latest security certifications. This overview briefly explains some of those features.

This document is organized into the following topic areas:

- **System security:** The integrated and secure software that forms the foundation of macOS.
- **Encryption and data protection:** The architecture and design that protects user data if the device is lost or stolen.
- **App security:** The systems that protect the Mac from malware and enable apps to run securely and without compromising platform integrity.
- **Authentication and digital signing:** The facilities included in macOS for credential management and support of industry-standard technologies such as smart cards and S/MIME.
- **Network security:** Industry-standard networking protocols that provide secure authentication and encryption of data in transit.
- **Device controls:** Methods that allow management of Apple devices, prevent unauthorized use, and enable remote wipe if a device is lost or stolen.

For more information about macOS deployment and management, refer to the macOS Deployment Reference at help.apple.com/deployment/macos.

For information on security features of Apple services not covered in this document, refer to the "iOS Security Guide" at www.apple.com/business/docs/iOS_Security_Guide.pdf.

System Security

macOS system security is designed so that both software and hardware are secure across all core components of every Mac. This architecture is central to security in macOS, and never gets in the way of device usability.

UNIX

The macOS kernel—the heart of the operating system—is based on the Berkeley Software Distribution (BSD) and the Mach microkernel. BSD provides basic file system and networking services, a user and group identification scheme, and many other foundational capabilities. BSD also enforces access restrictions to files and system resources based on user and group IDs.

Mach provides memory management, thread control, hardware abstraction, and interprocess communication. Mach ports represent tasks and other resources, and Mach enforces access to the ports by controlling which tasks can send a message to them. BSD security policies and Mach access permissions constitute the essential foundation of security in macOS, and they're critical to enforcing local security.

The kernel's security is essential to the security of the entire operating system. Code signing protects the kernel and third-party kernel extensions, as well as other system libraries and executables developed by Apple.

User permission model

An important aspect of Mac security is the granting or denying of access permissions (sometimes called access rights). A permission is the ability to perform a specific operation, such as gaining access to data or to execute code. Permissions are granted at the level of folders, subfolders, files, and apps, as well as for specific data in files, app capabilities, and administrative functions. Digital signatures identify the access rights of apps and system components.

macOS controls permissions at many levels, including the Mach and BSD components of the kernel. To control permissions for networked apps, macOS uses networking protocols.

Mandatory access controls

macOS also uses mandatory access controls—policies that set security restrictions created by the developer, which can't be overridden. This approach is different from discretionary access controls, which permit users to override security policies according to their preferences. Mandatory access controls aren't visible to users, but they're the underlying technology that helps enable several important features, including sandboxing, parental controls, managed preferences, extensions, and System Integrity Protection.

System Integrity Protection

OS X 10.11 or later includes system-level protection, called System Integrity Protection, which restricts components to read-only in specific critical file system locations to prevent malicious code from executing or modifying them. System Integrity Protection is a computer-specific setting that's on by default when you upgrade to OS X 10.11; disabling it removes protection for all partitions on the physical storage device. macOS applies this security policy to every process running on the system, regardless of whether it's running sandboxed or with administrative privileges.

For more information about these read-only areas of the file system, see the Apple Support article "About System Integrity Protection" at support.apple.com/HT204899.

Kernel extensions

macOS provides a kernel extension mechanism to allow dynamic loading of code into the kernel without the need to recompile or relink. Because these kernel extensions (KEXTs) provide both modularity and dynamic loading, they're a natural choice for any relatively self-contained service that requires access to internal kernel interfaces, such as hardware device drivers or VPN apps.

To improve security on the Mac, user consent is required to load kernel extensions installed with or after installing macOS High Sierra. This is known as

User-Approved Kernel Extension Loading. Any user can approve a kernel extension, even if they don't have administrator privileges.

Kernel extensions don't require authorization if they:

- Were installed on the Mac before upgrading to macOS High Sierra.
- Are replacing previously approved extensions.
- Are allowed to load without user consent by using the `spctl` command available when booted from the macOS Recovery partition.
- Are allowed to load via mobile device management (MDM) configuration. Starting with macOS High Sierra 10.13.2, you can use MDM to specify a list of kernel extensions that will load without user consent. This option requires a Mac running macOS High Sierra 10.13.2 that's enrolled in MDM either via the Device Enrollment Program (DEP) or via user-approved MDM enrollment.

For more information about kernel extensions, see the Apple Support article "Prepare for changes to kernel extensions in macOS High Sierra" at support.apple.com/HT208019.

Firmware password

macOS supports the use of a password to prevent unintended modifications of firmware settings on a specific system. This firmware password is used to prevent the following:

- Booting from an unauthorized system volume
- Alteration of the boot process, such as booting into single-user mode
- Unauthorized access to macOS Recovery
- Direct memory access (DMA) through interfaces such as Thunderbolt
- Target disk mode, which requires DMA

Note: The Apple T2 chip in iMac Pro prevents users from being able to reset the firmware password, even if they gain physical access to the Mac. On a Mac that does not have the T2 chip, additional precautions must be taken to prevent users from gaining physical access to the internals of the Mac.

Internet recovery

Mac computers automatically try to start up from macOS Recovery over the Internet when they're unable to start up from the built-in recovery system. When that happens, a spinning globe instead of an Apple logo appears during startup. Internet recovery enables a user to reinstall the latest version of macOS or the version that shipped with their Mac.

macOS updates are distributed through the App Store and performed by the macOS Installer, which leverages code signatures to ensure the integrity and authenticity of the installer and its packages prior to installation. Similarly, the Internet Recovery service is the authoritative source for the operating system that shipped with a particular Mac.

For more information about macOS Recovery, see the Apple Support article "About macOS Recovery" at support.apple.com/HT201314.

Encryption and Data Protection

Apple File System

Apple File System (APFS) is a new, modern file system for macOS, iOS, tvOS, and watchOS. Optimized for Flash/SSD storage, it features strong encryption, copy-on-write metadata, space sharing, cloning for files and directories, snapshots, fast directory sizing, atomic safe-save primitives, and improved file system fundamentals, as well as a unique copy-on-write design that uses I/O coalescing to deliver maximum performance while ensuring data reliability.

APFS allocates disk space on demand. When a single APFS container has multiple volumes, the container's free space is shared and can be allocated to any of the individual volumes as needed. Each volume uses only part of the overall container, so the available space is the total size of the container, minus the space used in all volumes in the container.

For macOS High Sierra, a valid APFS container must contain at least three volumes, the first two of which are hidden from the user:

- Preboot volume: Contains data needed for booting each system volume in the container.
- Recovery volume: Contains the Recovery Disk.
- System volume: Contains macOS and the User folder.

FileVault

Every Mac provides built-in encryption capability, called FileVault, to secure all data at rest. FileVault uses XTS-AES-128 data encryption to secure data on a Mac at rest. This can be applied to full volume protection to internal and removable storage devices. If a user enters an Apple ID and password during Setup Assistant, the assistant suggests enabling FileVault and storing the recovery key in iCloud.

A user who enables FileVault on a Mac is asked to provide valid credentials before continuing the boot process and to gain access to specialized startup modes, such as Target Disk Mode. Without valid login credentials or a recovery key, the whole volume remains encrypted and is protected from unauthorized access even if the physical storage device is removed and connected to another computer.

To protect data in an enterprise setting, IT should define and enforce FileVault configuration policies via MDM. Organizations have several options for managing encrypted volumes, including institutional recovery keys, personal recovery keys (that can optionally be stored with MDM for escrow), or a combination of both. Key rotation can also be set as a policy in MDM.

Encrypted disk images

In macOS, encrypted disk images serve as secure containers in which users can store or transfer sensitive documents and other files. Encrypted disk images are created using Disk Utility, located in /Applications/Utilities/. Disk images can be encrypted using either 128-bit or 256-bit AES encryption. Because a mounted disk image is treated as a local volume connected to a Mac, users can copy, move, and open files and folders stored in it. As with FileVault, the contents of a disk image are encrypted and decrypted in real time. With encrypted disk images, users can safely exchange documents, files, and folders by saving an encrypted disk image to removable media, sending it as a mail message attachment, or storing it on a remote server.

ISO 27001 and 27018 certifications

Apple has received ISO 27001 and ISO 27018 certification for the information security management system (ISMS) for the infrastructure, development, and operations that support these products and services: Apple School Manager, iCloud, iMessage, FaceTime, Managed Apple IDs, and iTunes U, in accordance with the Statement of Applicability v2.1, dated July 11, 2017. Apple's compliance with the ISO standard was certified by the British Standards Institution (BSI). To view the ISO 27001 and ISO 27018 certificates of compliance, see the BSI website:

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

Cryptographic validation (FIPS 140-2)

The cryptographic modules in macOS have been repeatedly validated for compliance with U.S. Federal Information Processing Standards (FIPS) 140-2 Level 1 following each release since OS X 10.6. As with each major release, Apple submits the modules to CMVP for revalidation when the Mac operating system is released. This program validates the integrity of cryptographic operations for Apple apps and third-party apps that properly use macOS cryptographic services and approved algorithms. All Apple FIPS 140-2 Conformance Validation Certificates can be found on the CMVP vendor page. CMVP maintains validation status of cryptographic modules under two separate lists depending on their current status at csrc.nist.gov/groups/STM/cmvp/inprocess.html.

Common Criteria Certification (ISO 15408)

Apple has previously achieved macOS certifications under the Common Criteria Certification program and is reengaging with an evaluation of macOS High Sierra against the Operating System Protection Profile (PP_OSv4.1). Apple continues to evaluate and pursue certifications against new and updated versions of the Collaborative Protection Profiles (cPPs) available today. Apple has taken an active role within the International Technical Community (ITC) in developing cPPs that focus on evaluating key mobile security technology.

Security certifications, programs, and guidance

Apple has worked with governments worldwide to develop guides that give instructions and recommendations for maintaining a more secure environment, also known as "device hardening" for high-risk environments. These guides provide defined and vetted information about how to configure and use built-in features in macOS for enhanced protection.

For the latest information on macOS security certifications, validations, and guidance, see the Apple Support article "Product security certifications, validations, and guidance for macOS" at support.apple.com/HT201159.

App Security

macOS includes built-in technologies to ensure that only trusted apps are installed and to help defend against malware. To ensure that legitimate apps can't be tampered with, macOS also includes a layered approach to app runtime protection and app signing.

Gatekeeper

To control the sources from which apps can be installed, macOS provides a feature called Gatekeeper. Gatekeeper allows users and organizations to set a required security level for installing apps.

With the most secure Gatekeeper setting, users can install only signed apps from the App Store. The default setting enables users to install apps from the App Store and apps that have a valid Developer ID signature. This signature indicates that the apps were signed by a certificate issued by Apple and that they haven't been modified since. Gatekeeper can also be completely disabled via a Terminal command, if necessary.

In addition, Gatekeeper applies path randomization in some cases, including when apps are launched directly from an unsigned disk image or from the location to which they were downloaded and automatically unarchived. Path randomization makes apps available from an unspecified read-only location in the file system before launching. This prevents apps from accessing code or content using relative paths, but also prevents them from self-updating if they're launched from this read-only location. Using the Finder to move an app, for example, to the Applications folder means that path randomization will no longer be applied.

The major security benefit of the default protection model is that it provides broad ecosystem protection. Should a malware author manage to steal or otherwise obtain Developer ID signing capability and use it to distribute malware, Apple can quickly respond by revoking the signing certificate. This will halt further spread of the malware. Such protections undercut the economic model of most malware campaigns on the Mac and provide broad protections to all users.

Users can temporarily override these settings to install any app. Organizations can use their MDM solution to establish and enforce Gatekeeper settings, as well as to add certificates to the macOS trust policy for evaluating code signing.

XProtect

macOS includes built-in technology for the signature-based detection of malware. Apple monitors for new malware infections and strains, and updates XProtect signatures automatically—independent from system updates—to help defend Mac systems from malware infections. XProtect automatically detects and blocks the installation of known malware.

Malware removal tool

Should malware make its way onto a Mac, macOS also includes technology to remediate infections. In addition to monitoring for malware activity in the ecosystem to be able to revoke Developer IDs (if applicable) and issue XProtect updates, Apple also issues updates to macOS to remove malware from any impacted systems that are configured to receive automatic security updates. Once the malware removal tool receives updated information, malware is

removed after the next restart. The malware removal tool doesn't automatically reboot the Mac.

Automatic security updates

Apple issues the updates for XProtect and the malware removal tool automatically. By default, macOS checks for these updates daily. For more information on automatic security updates, see the Apple Support article "Mac App Store: Automatic security updates" at support.apple.com/HT204536.

Runtime protection

System files, resources, and the kernel are shielded from a user's app space. All apps from the App Store are sandboxed to restrict access to data stored by other apps. If an app from the App Store needs to access data from another app, it can do so only by using the APIs and services provided by macOS.

Mandatory app code signing

All apps from the App Store are signed by Apple to ensure that they haven't been tampered with or altered. Apple signs any apps provided with Apple devices. Many apps distributed outside the App Store are signed by the developer using an Apple-issued Developer ID certificate (combined with a private key) in order to run under default Gatekeeper settings.

Apps from outside the App Store are normally signed with an Apple-issued developer certificate as well. This lets you validate that the app is genuine and hasn't been tampered with. Apps developed in house should also be signed with an Apple-issued Developer ID so that you can validate their integrity.

Mandatory Access Controls (MAC) require code signing to enable entitlements protected by the system. For example, apps requiring access through the firewall must be code signed with the appropriate MAC entitlement.

Authentication and Digital Signing

For convenient and secure storing of users' credentials and digital identities, macOS includes the Keychain and other tools to support authentication and digital signing technologies like smart cards and S/MIME.

Keychain architecture

macOS offers a repository called Keychain, which conveniently and securely stores user names and passwords, including digital identities, encryption keys, and secure notes. It can be accessed by opening the Keychain Access app in /Applications/Utilities/. Using a keychain eliminates the requirement to enter—or even remember—the credentials for each resource. An initial default keychain is created for each Mac user, though users can create other keychains for specific purposes.

In addition to user keychains, macOS relies on a number of system-level keychains that maintain authentication assets that aren't user-specific, such as network credentials and public key infrastructure (PKI) identities. One of these keychains, System Roots, is immutable and stores Internet PKI root certificate authority (CA) certificates to facilitate common tasks like online banking and e-commerce. You can similarly deploy internally provisioned CA certificates to managed Mac computers to aid in the validation of internal sites and services.

Secure authentication framework

Keychain data is partitioned and protected with Access Control Lists (ACLs), so credentials stored by third-party apps can't be accessed by apps with different identities unless the user explicitly approves them. This protection provides the mechanism for securing authentication credentials on Apple devices across a range of apps and services within your organization.

Touch ID

Mac systems with a Touch ID sensor can be unlocked using a fingerprint. Touch ID doesn't replace the need for a password, which is still required to log in after startup, restart, or logout of a Mac. When logged in, users can quickly authenticate with Touch ID whenever they're asked for a password.

Users can also use Touch ID to unlock password-protected notes in the Notes app, the Passwords pane of Safari preferences and many preference panes within System Preferences. To increase security, users must enter a password instead of using Touch ID to unlock the Security & Privacy pane in System Preferences. If FileVault is turned on, users must also enter a password to manage Users & Groups preferences. Multiple users who log in to the same Mac can use Touch ID to switch accounts.

For more information on Touch ID and its security, see the Apple Support article "About Touch ID advanced security technology" at support.apple.com/HT204587.

Auto Unlock with Apple Watch

Users with Apple Watch can use it to automatically unlock their Mac. Bluetooth Low Energy (BLE) and peer-to-peer Wi-Fi allow Apple Watch to securely unlock a Mac after ensuring proximity between the devices. This requires an iCloud account with two-factor authentication (TFA) configured.

For details on the protocol, as well as more information about Continuity and Handoff features, refer to the "iOS Security Guide" at www.apple.com/business/docs/iOS_Security_Guide.pdf.

Smart cards

macOS Sierra and above includes native support for personal identity verification (PIV) cards. These cards are widely used in commercial and government organizations for TFA, digital signing, and encryption.

Smart cards include one or more digital identities that have a pair of public and private keys and an associated certificate. Unlocking a smart card with the personal identification number (PIN) provides access to the private keys used for authentication, encryption, and signing operations. The certificate determines what a key can be used for, what attributes are associated with it, and whether it's validated (signed) by a CA.

Smart cards can be used for two-factor authentication. The two factors needed to unlock a card are "something you have" (the card) and "something you know" (the PIN). macOS Sierra and above has native support for smart card login window authentication and client certificate authentication to websites on Safari. It also supports Kerberos authentication using key pairs (PKINIT) for single sign-on to Kerberos-supported services.

For more information about smart card deployment with macOS, refer to the macOS Deployment Reference at help.apple.com/deployment/macos.

Digital signing and encryption

In the Mail app, users can send messages that are digitally signed and encrypted. Mail automatically discovers appropriate RFC 822 case-sensitive email address subject or subject alternative names on digital signing and encryption certificates on attached PIV tokens in compatible smart cards. If a configured email account matches an email address on a digital signing or encryption certificate on an attached PIV token, Mail automatically displays the signing button in the toolbar of a new message window. If Mail has the recipient's email encryption certificate or can discover it in the Microsoft Exchange Global Address List (GAL), an unlocked icon appears in the new message toolbar. A locked lock icon indicates the message will be sent encrypted with the recipient's public key.

Per-message S/MIME

macOS supports per-message S/MIME. This means that S/MIME users can choose to always sign and encrypt messages by default or to selectively sign and encrypt individual messages.

Identities used with S/MIME can be delivered to Apple devices using a configuration profile, an MDM solution, the Simple Certificate Enrollment Protocol (SCEP), or Microsoft Active Directory Certificate Authority.

Network Security

In addition to the built-in safeguards Apple uses to protect data stored on Mac computers, there are many network security measures that organizations can take to keep information secure as it travels to and from a Mac.

Mobile users must be able to access corporate networks from anywhere in the world, so it's important to ensure that they're authorized and their data is protected during transmission. macOS uses—and provides developer access to—standard networking protocols for authenticated, authorized, and encrypted communications. To accomplish these security objectives, macOS integrates proven technologies and the latest standards for Wi-Fi data network connections.

TLS

macOS supports Transport Layer Security (TLS 1.0, TLS 1.1, and TLS 1.2) and DTLS. It supports both AES-128 and AES-256, and prefers cipher suites with perfect forward secrecy. Safari, Calendar, Mail, and other Internet apps automatically use this protocol to enable an encrypted communication channel between the device and network services.

High-level APIs (such as CFNetwork) make it easy for developers to adopt TLS in their apps, while low-level APIs (such as SecureTransport) provide fine-grained control. CFNetwork disallows SSLv3, and apps that use WebKit (such as Safari) are prohibited from making an SSLv3 connection.

As of macOS High Sierra and iOS 11, SHA-1 certificates are no longer allowed for TLS connections unless trusted by the user. Certificates with RSA keys shorter than 2048 bits are also disallowed. The RC4 symmetric cipher suite is deprecated in macOS Sierra and iOS 10. By default, TLS clients or servers implemented with SecureTransport APIs don't have RC4 cipher suites enabled, and are unable to connect when RC4 is the only cipher suite available. To be more secure, services or apps that require RC4 should be upgraded to use modern, secure cipher suites.

App Transport Security

App Transport Security provides default connection requirements so that apps adhere to best practices for secure connections when using NSURLConnection, CFURL, or NSURLSession APIs. By default, App Transport Security limits cipher selection to include only suites that provide forward secrecy, specifically ECDHE_ECDSA_AES and ECDHE_RSA_AES in GCM or CBC mode. Apps are able to disable the forward secrecy requirement on a per-domain basis, in which case RSA_AES is added to the set of available ciphers.

Servers must support TLS 1.2 and forward secrecy, and certificates must be valid and signed using SHA-256 or better with a minimum 2048-bit RSA key or 256-bit elliptic curve key.

Network connections that don't meet these requirements will fail, unless the app overrides App Transport Security. Invalid certificates always result in a hard failure and no connection. App Transport Security is automatically applied to apps that are compiled for macOS 10.11 or later.

VPN

Secure network services like virtual private networking (VPN) typically require minimal setup and configuration to work with macOS. Mac computers work with VPN servers that support the following protocols and authentication methods:

- IKEv2/IPSec with authentication by shared secret, RSA certificates, ECDSA certificates, EAP-MSCHAPv2, or EAP-TLS
- SSL VPN using the appropriate client app from the App Store
- Cisco IPSec with user authentication by password, RSA SecurID or CRYPTOCard, and machine authentication by shared secret and certificates
- L2TP/IPSec with user authentication by MS-CHAPV2 password, RSA SecurID or CRYPTOCard, and machine authentication by shared secret

In addition to VPN solutions from third parties, macOS supports the following:

- **VPN On Demand** for networks that use certificate-based authentication. IT policies specify which domains require a VPN connection by using a VPN configuration profile.
- **Per-App VPN** for facilitating VPN connections on a much more granular basis. MDM can specify a connection for each managed app and specific domains in Safari. This helps ensure that secure data always goes to and from the corporate network—and that a user's personal data doesn't.

Wi-Fi

macOS supports industry-standard Wi-Fi protocols, including WPA2 Enterprise, to provide authenticated access to wireless corporate networks. WPA2 Enterprise uses 128-bit AES encryption, giving users the highest level of assurance that their data remains protected when sending and receiving communications over a Wi-Fi network connection. With support for 802.1X, Mac computers can be integrated into a broad range of RADIUS authentication environments. Methods for 802.1X wireless authentication include EAP-TLS, EAP-TTLS, EAP-FAST, EAP-AKA, PEAPv0, PEAPv1, and LEAP.

WPA/WPA2 Enterprise authentication can also be used at the login window of macOS so the user logs in to authenticate to the network.

The macOS Setup Assistant supports 802.1X authentication with user name and password credentials using TTLS or PEAP.

Firewall

macOS includes a built-in firewall to protect the Mac from network access and denial-of-service attacks. It supports the following configurations:

- Block all incoming connections, regardless of app
- Automatically allow built-in software to receive incoming connections
- Automatically allow downloaded and signed software to receive incoming connections
- Add or deny access based on user-specified apps
- Prevent the Mac from responding to ICMP probing and portscan requests

Single sign-on

macOS supports authentication to enterprise networks using Kerberos. Apps can use Kerberos to authenticate users to services they're authorized to access. Kerberos can also be used for a range of network activities, from secure Safari sessions and network file system authentication to third-party apps. Certificate-based authentication (PKINIT) is supported, although app adoption of a developer API is required.

GSS-API SPNEGO tokens and the HTTP Negotiate protocol work with Kerberos-based authentication gateways and Windows Integrated Authentication systems that support Kerberos tickets. Kerberos support is based on the open-source Heimdal project.

The following encryption types are supported:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

To configure Kerberos, acquire tickets with Ticket Viewer, log in to a Windows Active Directory domain, or use the command-line `kinit` tool.

AirDrop security

Mac computers that support AirDrop use BLE and Apple-created peer-to-peer Wi-Fi technology to send files and information to nearby devices, including AirDrop-capable iOS devices running iOS 7 or later. The Wi-Fi radio is used to communicate directly between devices without using any Internet connection or Wi-Fi access point. This connection is encrypted with TLS.

For more information about AirDrop, AirDrop security, and other Apple services, see the "Network Security" section of the "iOS Security Guide" at www.apple.com/business/docs/iOS_Security_Guide.pdf.

Device Controls

macOS supports flexible security policies and configurations that are easy to enforce and manage. This enables organizations to protect corporate information and ensure that employees meet enterprise requirements, even if they're using computers they've provided themselves—for example, as part of a "bring your own device" (BYOD) program.

Organizations can use resources such as password protection, configuration profiles, and third-party MDM solutions to manage fleets of devices and help

keep corporate data secure, even when employees access this data on their personal Mac computers.

Password protection

On Mac computers with Touch ID, the minimum passcode length is eight characters. Long and complex passcodes are always recommended, as they are harder to guess or attack.

Administrators can enforce complex passwords and other policies using MDM or by requiring users to manually install configuration profiles. An administrator password is needed for the macOS passcode policy payload installation.

For details about each policy available in MDM settings, see help.apple.com/deployment/mdm/#/mdm4D6A472A.

For developer details about each policy, refer to the Configuration Profile Reference at developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef.

Configuration enforcement

A configuration profile is an XML file that allows an administrator to distribute configuration information to Mac computers. If the user deletes a configuration profile, all the settings defined by the profile are also removed. Administrators can enforce settings by tying policies to Wi-Fi and data access. For example, a configuration profile that provides an email configuration can also specify a device password policy. A user won't be able to access mail unless the password meets the administrator's requirements.

A macOS configuration profile contains a number of settings that can be specified, including:

- Passcode policies
- Restrictions on device features (for example, disabling the camera)
- Wi-Fi or VPN settings
- Mail or Exchange server settings
- LDAP directory service settings
- Firewall settings
- Credentials and keys
- Software updates

For a current list of profiles, refer to the Configuration Profile Reference at help.apple.com/deployment/mdm/#/mdm5370d089.

Configuration profiles can be signed and encrypted to validate their origins, ensure their integrity, and protect their contents. Configuration profiles can also be locked to a Mac to completely prevent their removal, or to allow removal only with a password. Configuration profiles that enroll a Mac in an MDM solution can be removed—but doing so also removes managed configuration information, data, and apps.

Users can install configuration profiles that are downloaded from Safari, sent in a mail message, or sent over the air using an MDM solution. When a user sets up a Mac in DEP or Apple School Manager, the computer downloads and automatically installs a profile for MDM enrollment.

MDM

macOS support for MDM allows businesses to securely configure and manage scaled Mac, iPhone, iPad, and Apple TV deployments across their organizations. MDM capabilities are built on existing macOS technologies such as configuration profiles, over-the-air enrollment, and the Apple Push Notification service (APNs). For example, APNs is used to wake the device so it can communicate directly with its MDM solution over a secured connection. No confidential or proprietary information is transmitted by APNs.

Using MDM, IT departments can enroll Mac computers in an enterprise environment, wirelessly configure and update settings, monitor compliance with corporate policies, and even remotely wipe or lock managed Mac computers.

Device enrollment

Device enrollment, part of Apple School Manager and Apple Deployment Programs, provides a fast, streamlined way to deploy Mac computers that an organization has purchased directly from Apple or through participating Apple Authorized Resellers.

Organizations can automatically enroll computers in MDM without having to physically touch or prep the computers before users get them. After enrolling, administrators sign in to the program website and link the program to their MDM solution. The computers they purchased can then be automatically assigned with an MDM solution. Once a Mac has been enrolled, any MDM-specified configurations, restrictions, or controls are automatically installed. All communication between computers and Apple servers are encrypted in transit with HTTPS (SSL).

The setup process for users can be further simplified by removing specific steps in Setup Assistant, so users are up and running quickly. Administrators can also control whether or not the user can remove the MDM profile from the computer and ensure that device restrictions are in place from the very start. Once the computer is unboxed and activated, it enrolls in the organization's MDM solution—and all management settings, apps, and books are installed. Note, Device Enrollment is not available in all countries or regions.

For more information related to businesses, see Apple Deployment Programs Help at help.apple.com/deployment/business. For more information related to education, see Apple School Manager Help at help.apple.com/schoolmanager.

Restrictions

Restrictions can be enabled—or in some cases, disabled—by administrators to prevent users from accessing a specific app, service, or function of the device. Restrictions are sent to devices in a Restrictions payload within a configuration profile. Restrictions can be applied to macOS, iOS, and tvOS devices.

A current list of available restrictions for IT managers can be viewed at: help.apple.com/deployment/mdm/#/mdm2pHf95672

Remote wipe and remote lock

Mac computers can be erased remotely by an administrator or user. Instant remote wipe is available only if the Mac has FileVault enabled. When a remote wipe command is triggered by MDM or iCloud, the computer sends an acknowledgment and performs the wipe. With a remote lock, MDM requires that a six-digit passcode be applied to the Mac, rendering any user locked out until this passcode is typed in.

Privacy

Apple believes privacy is a fundamental human right, so every Apple product is designed to use on-device processing wherever possible, limit the collection and use of data, provide transparency and control over your information, and build on a strong foundation of security.

Apple has numerous built-in controls and options that allow macOS users to decide how and when apps utilize their information, as well as what information is being utilized. For more information, see www.apple.com/privacy.