What's New for IT

WWDC 2025 v1.2

Contents

Introduction

This document is a summary of new management-related features in Apple operating systems, services, and apps. It also describes updates to the Apple Device Management framework. It's a supplement to the Apple Platform Deployment, Apple Platform Security, and Apple Platform Certifications documentation, which are all designed to help IT administrators understand the key technologies for securing, managing, and deploying Apple devices at scale, and providing an optimal user experience.

This document covers updates to the following:

- Apple School Manager and Apple Business Manager
- Device management
- App management
- Identity management
- Education-specific content

For planned support for device management features listed in this document, contact the organization's device management service developer.

For more information about content in this document, see the WWDC25 video What's new in managing Apple devices.

Note: This material is provided for informational purposes only; Apple assumes no liability related to its use. The Apple software and services discussed hereunder are prerelease versions that may be incomplete and may contain inaccuracies or errors that could cause failures or loss of data.

Apple School Manager and Apple Business Manager updates

Apple School Manager and Apple Business Manager are the foundation for managing Apple devices at scale, helping organizations automate deployment, secure access, and maintain control across every stage of the device life cycle.

Limit device sign-in to Managed Apple Accounts

Depending on individual requirements, organizations may allow their users to sign in with any Apple Account on organization-owned devices, or may want to ensure users can use only a Managed Apple Account.

Later this year, a new access management setting in Apple School Manager and Apple Business Manager lets organizations control whether users can sign in with any Apple Account or only a Managed Apple Account (from the same organization) on organization-owned devices. This impacts any new sign-in with an Apple Account, including Setup Assistant during first-time device setup, but doesn't affect personal Apple Accounts already signed in.

Combined with earlier access management features that restrict Managed Apple Account sign-in to managed or supervised devices, organizations now have a comprehensive way to control how they use these accounts across their devices.

For more information, see "Customize user access to certain apps and services" in the following:

- Apple School Manager User Guide
- Apple Business Manager User Guide

Apple School Manager and Apple Business Manager APIs

Apple School Manager and Apple Business Manager support APIs for organizations to automate device management tasks. For example, organizations can use those APIs to integrate with procurement and asset systems.

Users with the roles of Administrator and Site Manager (Apple School Manager only) can create API accounts that apps can use to access organization data and perform device management tasks.

The APIs support the following endpoints:

Name	Endpoint
List of Device Management Services	`GET /v1/mdmServers`
List All Devices	`GET /v1/orgDevices`
Get Device Information	`GET /v1/orgDevices/{id}`
Get Device Management Service Information for a Device	`GET /v1/orgDevices/{id}/relationships/assignedServer`
Get All Devices Assigned to Device Management Service	`GET /v1/mdmServers/{id}/relationships/devices`
Assign or Unassign Devices from Device Management Service	`POST /v1/orgDeviceActivities`
Get Batch Action Activity Status	`GET /v1/orgDeviceActivities/{id}`

For more information, see Apple School and Business Manager APIs on the Apple Developer website.

Device management migration

A device management service is an essential component to remotely manage and secure Apple devices. Organization-owned devices can automatically enroll in a device management service as part of the Setup Assistant process after unboxing the device, powering it on, and connecting it to a network. The current reenrollment of organization-owned devices in another device management service requires a full erase of the device or a complex manual process.

Organizations may have a need to reenroll devices in a device management service for many reasons, such as:

- Moving from an on-premises to a cloud-based device management service.
- Moving devices into a single device management service when acquiring another company.
- Migrating from one device management service to one from a different developer.

Apple School Manager and Apple Business Manager will support migrating to a new device management service. This includes the following features:

- Users with the roles of Administrator, Site Manager (Apple School Manager only), and Device Enrollment Manager can set a deadline for completing enrollment, and view the pending migrations notification on the device page.
- Users receive notifications to confirm reenrollment, with more frequent notifications leading up to the deadline.
- If the user doesn't take action, the organization can enforce migration and reenrollment. This involves a restart on an iPhone or iPad, and a nondismissible full-screen prompt on a Mac.
- If the device has no internet connectivity after unenrollment, the user receives a prompt to manually connect to proceed.
- iPhone and iPad devices have the option to preserve apps and their associated data if the new device management service delivers the apps before sending the `DeviceConfigured` command.
- After reenrollment, the new device management service creates new Activation Lock bypass codes.

Important: To provide continued service access and a seamless user experience, administrators need to ensure the new device management service applies configurations that match those of the previous device management service and use the `await_device_configured` key for Managed Apps, FileVault, and Activation Lock configurations.

Requirements

To migrate from one device management service to another, organizations need to meet the following requirements. If an organization doesn't meet the requirements, devices are unable to show the deadline option, and bulk actions result in failures (which appear in the activity log).

- Devices with iOS, iPadOS, or macOS 26.
- The organization needs to own the device and enroll it with Automated Device Enrollment. Additionally, Mac computers that are unenrolled and reenrolled with profile-based enrollment are supported for migration.
- If the organization enrolls the device manually using Apple Configurator, it needs to be after the 30-day provisional period.
- Migrating to and from the device management service within Apple Business Essentials isn't currently supported.

Note: Organizations can use the device filters to locate ineligible devices.

For more information, see Migrate managed devices to another device management service in Apple Platform Deployment.

Unmanaged Apple Account list

Currently, organizations can view the total number of personal (unmanaged) Apple Accounts on verified domains to determine how many users might receive notifications when initiating a domain capture.

Later this year, organizations will be able to download a list of email addresses on verified domains for those Apple Accounts that are signed in to Apple web services, such as the Apple Developer Program, the AppleCare Enterprise Portal, and the Apple Push Notification services portal.

Developer services for Managed Apple Accounts

Organizations can take advantage of the Apple Developer Program when issuing Managed Apple Accounts to their developers, which allows them to benefit from centralized user management and federated authentication.

Starting this year, Managed Apple Accounts work for developer services like notarization, including command-line tools like `notarytool` and `stapler`, and app-specific passwords.

Device warranty information

AppleCare information for devices helps IT teams track coverage, plan repairs, and make informed decisions about support and replacements, including reduced downtime and improved device life-cycle management.

Later this year, device warranty and AppleCare coverage information for organization-owned devices (that aren't released from the organization) will be available in Apple School Manager and Apple Business Manager.

IMEI, EID, and MAC address information

Inventory details in Apple School Manager and Apple Business Manager provide a comprehensive view of all assigned devices for an organization. This includes device type, serial number, order information, and assignment status for streamlined deployment and management. Earlier this year, the list expanded to include IMEI and EID information of organization-owned devices.

Later this year, physical MAC addresses for the following will be included for organization-owned iPhone and iPad devices:

- Wi-Fi
- Bluetooth

Alternative service discovery for account-driven enrollments

As part of the enrollment process, when a user enters a Managed Apple Account under the “Sign in to Work or School account” section on their personal or organization-owned device, the operating system uses the domain of the Managed Apple Account to query a service discovery resource from a specific well-known file. This provides the device with the enrollment URL, which determines the device management service it enrolls with. Generally, an organization hosts this well-known file on their domain.

If an organization is unable to host the file on their domain, the following process is available:

- Devices with iOS 18.2, iPadOS 18.2, macOS 15.2, visionOS 2.2, or later, can fetch the service discovery resource from an alternative location.
- A device management service can provide an alternative service discovery location for verified domains in Apple School Manager and Apple Business Manager. For more information, see Assign Account-Driven Enrollment Service Discovery on the Apple Developer website.
- Users with the role of Administrator can then use the default device management service assignment to configure the alternative service discovery location per device type for iPhone, iPad, Mac, and Apple Vision Pro.

For more information, see Account-driven enrollment methods with Apple devices in Apple Platform Deployment.

Granular privileges for the Device Enrollment Manager role

Users with the role of Administrator now have additional granularity to define privileges for the Device Enrollment Manager and Site Manager (Apple School Manager only) roles. This change allows these two roles to have only the appropriate privileges they need to perform device actions. Organizations can enable or restrict the following privileges for users with the roles of Device Enrollment Manager and Site Manager:

- Add and remove device management services
- Manage Automated Device Enrollment
  - List device management services
  - Add devices using Apple Configurator
- Assign devices
  - Manage default device management service assignments
  - Assign devices to device management services
- Release devices from the organization
- Remove Activation Lock from organization-owned devices

For more information, see “Device privileges” in the following:

- Apple School Manager User Guide
- Apple Business Manager User Guide

Device management updates

Apple continues to evolve platform management with updates to the device management protocol, giving IT teams better control, automation, and greater transparency.

Content filtering

To help ensure the safety of their users and to protect their organizations, schools and businesses use solutions to control the websites and URLs users can access. Filtering based on the domain names of websites covers many URL-filtering use cases; however, this also blocks access to the entire page. To achieve a more dynamic and flexible process, URL filtering requires examining more of the URL, or even the full URL.

On devices with iOS, iPadOS, and macOS 26, organizations can use a new Network Extension URL-filtering API to provide a comprehensive and privacy-preserving URL-filtering solution across the entire system. URL filtering leverages Apple Private Information Retrieval (PIR) and Oblivious HTTP Relay hosted by Apple to help protect user privacy. To perform URL filtering:

1. The built-in Network Extension system process examines all the URL requests.
2. It then checks each URL against an on-device prefilter app that the developer provides.
3. If necessary, it performs a PIR query against the developer's PIR database to get a match, which indicates whether to allow or block the URL request.

The developer's URL filter app needs to provide only the URL of their database to the Network Extension framework. The Network Extension framework then performs URL filtering using the provided database. The developer's URL filter app isn't part of the filtering path, and has no access to any user networking data. This results in an organization not knowing which websites users attempt to visit, while providing security and compliance assurance.

For more information, see the WWDC25 video, Filter and tunnel network traffic with Network Extension.

Safari management

On devices with iOS, iPadOS, macOS, and visionOS 26, new configurations for Safari allow organizations to customize the browsing experience for their users.

With the new `com.apple.configuration.safari.bookmarks` and `com.apple.configuration.safari.settings` configurations, organizations can:

- Configure bookmarks for Safari so users can easily access organization resources and websites. Bookmarks appear in a separate folder, and organizations can arrange individual bookmarks in subfolders to organize how they appear to the user.
- Have more flexibility to customize the browsing experience by defining what users see when opening a new window or tab in Safari. For example, they might set the start page to the default Safari start page or a homepage that the organization defines, or allow a Safari extension to define a page to open.
- Configure additional Safari functions to meet their needs.

Feature	Key	Supported operating systems
Clear the browser history	`AllowHistoryClearing`	iOS, iPadOS, macOS, visionOS
Private browsing	`AllowPrivateBrowsing`	iOS, iPadOS, macOS, visionOS
Summarization of content	`AllowSummary`	iOS, iPadOS, macOS, visionOS
JavaScript execution	`AllowJavaScript`	iOS, iPadOS
Prevent pop-ups	`AllowPopups`	iOS, iPadOS
Cookie handling	`AcceptCookies`	iOS, iPadOS
Fraud warnings	`AllowDisablingFraudWarning`	iOS, iPadOS

App preservation for Return to Service

Return to Service—available on iPhone, iPad, Apple TV, and now on Apple Vision Pro—allows IT administrators to prepare a device for the next user without manual setup. After securely erasing the device, it automatically enrolls in a device management service and configures itself with the appropriate settings, making it ready for the next user quickly and securely.

On devices with iOS, iPadOS, and visionOS 26, Return to Service can also preserve Managed Apps. It securely erases user data, but app binaries remain to make the process even faster. To leverage this new behavior, use the following processes.

On Apple Vision Pro, Return to Service is available for the user to trigger from the Lock Screen or the Control Center. Organizations can also launch Return to Service automatically after a set period of inactivity that they define with the `SharedDeviceConfiguration.TemporarySessionTimeout` key in the `Settings` command.

First-time setup

1. Join the device to a Wi-Fi network.
2. Upon activation, the device receives a management configuration specifying the following:
   - Setup Assistant panes to skip during the initial setup.
   - A new key, `is_return_to_service`, which indicates using Return to Service for the device.
   - The `await_device_configured` flag.
3. Organizations can enforce a software update as part of the enrollment.
4. The device enrolls into management.
5. The device creates a bootstrap token and sends it to the device management service (similar to macOS). The bootstrap token in iOS, iPadOS, and visionOS is required to authenticate subsequent Return to Service operations, but the device sends it only during the *initial* setup. Developers need to ensure that they save the bootstrap token for all subsequent resets (because the device can't send it again).
6. The operating system installs and preserves Managed Apps during Return to Service.
7. The device management service sends the `DeviceConfigured` command to release the device from the Remote Management Setup Assistant pane.
8. A file system snapshot occurs.

Organizations can deliver profiles and declarations during the awaiting configuration state as well, but the operating system doesn't preserve them.

Device reset

The device management service triggers Return to Service and includes the following:

- The configuration required for Wi-Fi connectivity.
- The escrowed bootstrap token.
- If necessary, the enrollment profile for the device management service. If organizations don't specify one, the device queries Apple School Manager or Apple Business Manager. For example, organizations can provide the device with an enrollment profile that allows for unattended enrollment when they don't want to require interactive user authentication.

The process works like this:

1. The operating system securely erases the previous user's data from the device.
2. The device restarts.
3. The device reverts to the file system snapshot.
4. The device joins the Wi-Fi network that Return to Service specifies.
5. Organizations can enforce a software update as part of the enrollment.
6. The device enrolls into management.
7. The operating system installs Managed Apps and configurations, and doesn't download any previously preserved apps.

8. The device management service sends the `DeviceConfigured` command to release the device from the Remote Management Setup Assistant pane.

Quick Start on Apple Vision Pro

With enhancements to Quick Start in visionOS 26, users with a personal Apple Account can import their saved Apple Vision Pro setup data that they store in iCloud or on their iPhone. This removes the need to perform hands and eyes enrollment, and shortens the time before a user can begin using their Apple Vision Pro.

Managed Setup Assistant on Apple Vision Pro

Automated Device Enrollment provides a zero-touch and customizable enrollment experience to users on organization-owned devices.

When using Automated Device Enrollment on an Apple Vision Pro with visionOS 26, organizations can skip certain panes like the selection of a location or accepting terms and conditions in Setup Assistant. When skipping a pane, visionOS uses the more privacy-preserving setting for that feature.

Organizations can skip the following Setup Assistant panes when using Return to Service:

- Optic ID
- Passcode
- Data and Privacy

Manually register Apple Vision Pro

Registering devices in Apple School Manager and Apple Business Manager offers additional management functions for organization-owned devices, such as using Automated Device Enrollment or managing Activation Lock.

Organizations can manually add an Apple Vision Pro with visionOS 26 to Apple School Manager or Apple Business Manager even if they don’t purchase the device directly from Apple, an Apple Authorized Reseller, or an authorized cellular carrier.

When an Apple Vision Pro is at the initial Hello pane in Setup Assistant, and an iPhone running Apple Configurator is next to it, Apple Vision Pro displays a six-digit code to the user wearing the device, which Apple Configurator uses for manual pairing. To register the device, select Manual Pairing in Apple Configurator, then enter the six-digit code.

Audio accessory settings

iPhone and iPad devices now display the friendly name of AirPods with the H1 (or later) chip directly on the setup screen. This friendly name helps users easily identify their own AirPods if other users’ AirPods are in range. Also, with the latest update, if the operating system detects multiple AirPods in pairing mode, a link takes the user directly to the Bluetooth settings, which lists all available devices so they can manually select and pair with their AirPods.

In certain deployment scenarios—like shift workers or students in a classroom—users share a single device, but also want to benefit from the great audio experience of their personal AirPods and Beats audio accessories that use the H1 and H2 chips.

On supervised devices with iOS and iPadOS 26 (including Shared iPad):

- The new `com.apple.configuration.audio-accessory.settings` configuration can enable temporary pairing of AirPods and Beats audio accessories without syncing the pairing information with iCloud.
- Pairing information will be automatically removed at the end of each day, with the default removal time set to midnight. The removal time can be customized by the administrator.
- A new button will be added to the Headphone Settings page, allowing users to convert a temporary pairing into a permanent (local) pairing.

Software updates

Declarative software update management offers a robust and flexible way to enforce software updates while providing great user transparency. This year, the transition to declarative software updates is complete with support for Apple TV and Apple Vision Pro. The declarative software update approach replaces the previous process based on mobile device management commands, queries, configuration profiles, and restrictions.

On devices with tvOS 18.4 or later and visionOS 26:

- Organizations can enforce software updates using the `com.apple.configuration.softwareupdate.enforcement.specific` configuration. Devices can also provide proactive status reporting about the update process using status reports.
- Organizations can use the `com.apple.configuration.softwareupdate.settings` configuration on supervised Apple TV and Apple Vision Pro devices to configure:
  - *Frequency of notifications:* To show a notification only 1 hour before the enforcement deadline
  - *Software update deferrals:* To control which versions to offer to users
  - *Automatic software update behavior:* To allow, enforce, or disable automatic downloads and installation of software updates
  - *Recommended cadence:* To define whether users have the option to upgrade to the next major version (visionOS only)

Important: Software update management using mobile device management commands, restrictions, the `com.apple.SoftwareUpdate` payload, and queries is deprecated and Apple will remove it next year. Going forward, organizations can manage and enforce software updates using only declarative software update management.

Apple Intelligence features management

To address industry regulations and internal policies that require control over certain Apple Intelligence features, Apple provides device management controls using the `Restrictions` payload and `Math Settings` configuration for Writing Tools, Smart Script, Image Playground, Math Notes, and other features as, and when, they become available to the public. Management control is also available for the ChatGPT integration in Writing Tools and Siri.

For more information, see the following in the Apple device management GitHub repository:

- The com.apple.applicationaccess payload
- The math.settings configuration

On an Apple Vision Pro with visionOS 2.4 or later, devices can use Apple Intelligence features, and can also have device management controls similar to those available on iPhone, iPad, and Mac.

Organizations can manage the following Apple Intelligence features for iOS, iPadOS, macOS, and visionOS:

Feature	Configuration	Requires supervision?
Apple Intelligence Report	`allowAppleIntelligenceReport`	Yes

ChatGPT	`allowExternalIntelligenceIntegrations`
	`allowExternalIntelligenceIntegrationsSignIn`
	`allowedExternalIntelligenceWorkspaceIDs`
		No
		No
		Yes

Genmoji	`allowGenmoji`	Yes
Image Playground	`allowImagePlayground`	Yes
Image Wand	`allowImageWand`	Yes
Mail Smart Replies	`allowMailSmartReplies`	Yes
Mail Summary	`allowMailSummary`	Yes
Notes Transcription	`allowNotesTranscripton`	Yes
Notes Transcription Summary	`allowNotesTranscriptionSummary`	Yes
Safari Summary	`allowSafariSummary`	Yes
Siri	`allowAssistant`	No
Visual Intelligence Summary	`allowVisualIntelligenceSummary`	Yes
Writing Tools	`allowWritingTools`	Yes

Network relay hostnames

Network relays are a built-in way to securely and transparently tunnel traffic, and are a more efficient alternative to VPN.

On devices with iOS 18.4, iPadOS 18.4, macOS 15.4, tvOS 18.4, visionOS 2.4, or later, the `com.apple.relay.managed` configuration supports FQDNs (hostnames) in addition to domain-based rules. This adds flexibility to control which traffic routes through the relay. The following options are available:

- If an organization specifies `MatchDomains`, excluded FQDNs need to be subdomains to take effect.
- If an organization doesn't specify `MatchDomains` or FQDNs, all traffic (except excluded domains) goes through the relay. Organizations can also exclude FQDNs. Exact matches bypass the relay.

EnrollmentSSO and required app

EnrollmentSSO allows a dedicated identity app to handle authentication during device enrollment. This enables secure, single sign-on access to organizational resources using the organization's identity provider (IdP), and removes repeating authentication prompts.

As part of the enrollment process, the required app automatically installs and a device management service enforces it. Users can't delete it, ensuring critical apps—like a device management service's employee self-service app—always install when enrolling or reenrolling a device.

On devices with iOS 18.4, iPadOS 18.4, visionOS 2.4, or later, account-driven enrollments support the ability to configure both of the following, which allows for more flexible deployment scenarios:

- Authenticate using EnrollmentSSO
- Install a required app

Desktop and Documents syncing using File Provider extensions

Users appreciate the ease of use of iCloud Desktop and Documents, which keeps their Desktop and Documents folders on Mac synchronized and accessible from any device. In an organizational setting, they may be using other cloud storage solutions. If the cloud storage solution integrates with the File Provider extension, the same seamless user experience and functionality is available to users.

On a Mac with macOS 15.2 or later, organizations can use the `com.apple.fileproviderd` configuration to control which File Provider extensions to use:

- For Desktop and Documents folder synchronization
- With the internal storage volume or external volumes

Battery health for iPad

Status reports allow devices to proactively inform a device management service about status changes. The battery health feature provides increased visibility of device health.

On an iPad with iPadOS 15.4 or later, the following iPad models can report their battery health status:

- iPad Pro (M4)
- iPad Air (M3)
- iPad Air (M2)
- iPad (A16)
- iPad mini (A17 Pro)

Messaging and calling app management

Organizations rely on calling and messaging apps for corporate communication. IT administrators need to ensure they use appropriate apps to meet company policies and regulatory compliance.

- On an iPhone with iOS 18.4 and an iPad with iPadOS 18.4, or later, organizations can restrict modifications to the default calling and messaging apps using the `allowDefaultCallingAppModification` and `allowDefaultMessagingAppModification` keys in the `Restrictions` payload.
- On an iPhone and iPad with iOS and iPadOS 26, organizations can set the default calling and messaging apps using the `Calling` and `Messaging` keys in the `Settings` command. They can apply the command even when setting the corresponding restriction.

When communicating with friends and family outside work, users are likely to use iMessage, FaceTime, and RCS. On an organization-owned iPhone, these services are often restricted.

On an iPhone and iPad cellular models with iOS and iPadOS 26, organizations can limit these services to ones they manage. Organizations can also provide a list of ICCIDs associated with cellular plans to limit which lines are available for use with:

- *iMessage and FaceTime:* Using the `deniedICCIDsForiMessageFaceTime` key
- *RCS messaging:* Using the `deniedICCIDsForRCS` key

Both of these keys are part of the `Restrictions` payload.

Automatic Reboot

Automatic Reboot is a security mechanism introduced in iOS 18.1 and iPadOS 18.1 that leverages the Secure Enclave to monitor device unlock events. If a device remains locked for a prolonged period, it automatically reboots, transitioning from an After First Unlock state to a Before First Unlock state. During the reboot, the device purges sensitive security keys and transient data from memory.

For additional control, iOS 18.4 and iPadOS 18.4 introduced the `IdleRebootAllowed` setting to allow device management administrators to enable or disable Automatic Reboot. With this setting, administrators can programmatically enable or disable Automatic Reboot behavior to align with organizational security protocols and operational requirements.

Note: Automatic Reboot is disabled by default on supervised devices.

Although Automatic Reboot enhances security, it can inadvertently cause devices to lose their Wi-Fi connection upon reboot. This loss of connectivity may disrupt device management service operations, especially in environments where persistent network access is critical.

For more information, see SettingsCommand.Command.Settings.MDMOptions.MDMOptions on the Apple Developer website.

Apple Configurator support for Shortcuts

Using the Shortcuts app, organizations can create workflows to uniformly and efficiently configure large numbers of iPhone and iPad devices with Apple Configurator 2.18 or later. Shortcuts provide helpful feedback on the progression of individual actions, and they can also automate shortcuts based on devices being attached, detached, and more.

For more information, see Use Shortcuts automations in Apple Configurator for Mac in the Apple Configurator for Mac User Guide.

App management updates

Declarative app management redefines how organizations deploy and control apps across Apple platforms. It allows devices to autonomously install apps, and provides greater insights using status reports. The declarative configuration also provides additional options not available using the previous device management command-based approach.

Declarative app management

On devices with iOS, iPadOS, macOS, and visionOS 26, the `com.apple.configuration.app.managed` configuration offers new options to define installation and update behavior on a per-app basis. This gives organizations even more control over apps and their management, including:

- Organizations can enforce, disable, and set automatic updates of App Store apps to follow user preferences.
- When installing apps from the App Store, they can install them with, and pin them to, a specific version, allowing for a more controlled release management process.
- To provide additional transparency about installed apps, the existing status report that provides insights into the app installation and management status now also contains information on the update progress.
- Organizations can restrict app downloads over cellular networks (iOS and iPadOS only).

Declarative app management on Mac

On a Mac with macOS 26, organizations can deploy App Store apps, Custom Apps, and packages (.pkg files) using declarative device management. Features include the following:

- The `com.apple.configuration.app.managed` and `com.apple.configuration.package` configurations allow organizations to install an app or package as *required* or *optional*.
- Organizations can configure automatic updates of App Store apps and install a specific version.
- Using status reports, a device management service can receive automatic notifications about the status of an app and whether it deployed successfully.
- The ManagedAppDistribution framework is also available for macOS, allowing device management developers to display and facilitate installation of apps that they manage declaratively by using a unified and intuitive interface.

Configuring Managed Apps

Organizations often need to customize the user experience of an app according to their specific needs, or even for a particular group of users.

On devices with iOS 18.4, iPadOS 18.4, visionOS 2.4, or later, organizations can deploy app-specific configurations and secrets (like passwords, certificates, and identities) in a secure way to Managed Apps that adopt the ManagedApp framework. This allows organizations to customize the behavior of an app, streamline the user experience, and strengthen security with the `com.apple.configuration.app.managed` configuration. Examples include:

- Preconfigure a Managed App or app extension for a specific device or user.
- Use automatically provisioned identities for authentication and signing.
- Securely receive API access tokens.
- Acquire certificates for custom trust (pinning certificates).
- Use hardware-bound keys and Managed Device Attestation for strong device authentication.

For more information, see the ManagedApp framework on the Apple Developer website.

Identity management updates

Platform Single Sign-On helps organizations streamline Mac deployment and user access with seamless authentication tied to sign-in credentials from IdPs. Using secure, hardware-backed identity attestation with effortless setup during device enrollment, users can sign in to all their apps and services quickly, without compromising security.

Platform Single Sign-On attestation

Platform Single Sign-On creates secure, device-bound keys to authenticate users seamlessly across apps and services. Attestation of these keys ensures they're hardware-backed and trusted, strengthening identity security, and preventing credential misuse.

On a Mac with macOS 15.4 or later, a Platform SSO extension on a supervised Mac can request an attestation with the `AllowDeviceIdentifiersInAttestation` configuration key to get strong assurance about device identifiers (UDID and serial number). Using the strong assurances, organizations can also use attestation to silently and securely perform device registration during first-time setup.

Simplified setup for Platform Single Sign-On

On a Mac with macOS 26, organizations can activate and enforce Platform Single Sign-On (SSO) during Setup Assistant with Automated Device Enrollment. The process works like this:

1. macOS configures Platform SSO as the first pane in Setup Assistant, prompting users to authenticate with their IdP. Users can't proceed without Platform SSO registration.
2. After a successful sign-in, SSO can provide an authenticated enrollment in a device management service, and if federated to the same IdP, can sign in to the user's Managed Apple Account without having to enter credentials again. The iCloud Setup Assistant pane needs to be visible to the user (not skipped) for this to work.
3. macOS creates a local account, and the password either syncs with the IdP or the user sets it using a Secure Enclave-backed key.
4. If necessary, macOS can sync the local account login profile picture from the IdP.

For shared setups to get directly to the Login Window ready for use, SSO registration can run silently using attestation during Setup Assistant with Auto Advance.

Authenticated Guest Mode with Platform Single Sign-On

With Platform SSO, a shared Mac deployment can support multiple users by enabling sign-in with credentials from IdPs.

On a Mac with macOS 26, Platform SSO adds Authenticated Guest Mode, which provides an expedited login experience, including single sign-on for apps and websites. This is designed for users who use a Mac for a short period of time, such as a hospital nurse or student. The process works like this:

1. A user can log in to any shared Mac using their work or school credentials at the login window. Login requires the device to be able to reach the IdP.
2. When they log in, macOS uses single sign-on to access apps and websites.
3. When they log out, macOS erases local data for the account, and the shared Mac is ready for the next user to log in.

Tap to log in to Mac with Platform Single Sign-On

In organizations where multiple users share devices across shifts or classes, having to type their user names and complex passwords repeatedly throughout the day can slow down workflows, lead to login fatigue, and increase the risk of mistyped credentials.

Platform SSO addresses this by offering a faster, more seamless sign-in experience tied to an organizational identity. On a Mac with macOS 26, Platform Single Sign-On adds Tap to Login, a simple, secure, passwordless experience.

Instead of a password, macOS uses an Access Key credential tied to the user's IdP account. This is an NFC-based hardware-backed key that a device uses for authentication. iOS and watchOS store the key in Apple Wallet. macOS requires Authenticated Guest Mode for authentication with an Access Key.

The Access Key credential also works with Express mode, which doesn't require Face ID, Touch ID, or even unlocking the device. Users can unlock shared Mac computers (with an NFC reader connected) with just a tap of their iPhone or Apple Watch, combining convenience with strong authentication.

For more information, see Provisioning in the Apple Wallet Access Program Guide.

Kerberos Single Sign-On

Configuring single sign-on with Kerberos on iPhone and iPad using `com.apple.sso` is deprecated. In a future update, organizations can manage and configure single sign-on using only Extensible Single Sign-On.

Education-specific updates

Schoolwork makes it easy for teachers to distribute assignments, collaborate one-on-one with students, and view progress. Designed to work seamlessly with apps using ClassKit, it helps educators personalize learning with powerful insights.

Schoolwork

Schoolwork 3.1 adds the following features:

- Additional review options and examples:
  - *Letter- and number-rating systems:* A-F, rubric scales
  - *Completion status:* Got it, not yet, not done
  - *Satisfactory scale:* Excellent, satisfactory, unsatisfactory
- A feature to create customized items while reviewing assessments, which include emojis, numbers, and letters
- An option to export question analytics to PDF

AppleSeed for IT

AppleSeed for IT is designed specifically for enterprise and education customers committed to testing each new version of Apple beta software in their organizations. Organizations with Apple School Manager or Apple Business Manager designate which account roles in their organization may participate. Participants then use their Managed Apple Account to access the program, and associate their feedback with their organization.

To access program resources, sign in at AppleSeed for IT using a Managed Apple Account from the organization, and accept the program terms. Participants can then download beta software, access beta documentation, and participate in test plans and surveys specific to enterprise and education environments. For additional details, see the AppleSeed Program Planning Guide, which is available in the Downloads section of the AppleSeed for IT web portal.

Additional resources

Learn more about Apple deployment and security at the following websites:

- Apple Platform Deployment
- Apple Platform Security
- Apple Platform Certifications
- Apple Configurator User Guide for iPhone
- Apple Configurator User Guide for Mac
- Apple School Manager User Guide
- Apple Business Manager User Guide
- Apple Deployment Guide for K–12 Education
- Classroom User Guide
- Schoolwork User Guide

Note: The websites listed above update with content from this document when the features move from beta to public release.

For more information on developer information regarding the device management changes in this document, see the following:

- Device Management on the Apple Developer website
- The Apple device management GitHub repository

Apple
One Apple Park Way
Cupertino, CA 95014
www.apple.com

028-0082