What’s New for Enterprise and Education

WWDC

June 2021 (v1.0)

Contents

Introduction

This document is a summary of new security and deployment-related features in macOS 12, iOS 15, iPadOS 15, and tvOS 15. It also describes updates to Apple School Manager, Apple Business Manager, AppleSeed for IT, and to the Apple mobile device management (MDM) framework. It is a supplement to the *Deployment Reference for iPhone and iPad*, the *Deployment Reference for Mac*, *Mobile Device Management Settings for IT Administrators*, and *Apple Platform Security*, all designed to help administrators understand the key technologies for deploying Apple devices at scale and providing an optimal experience for users.

This document covers the following topics:

- Security
- Management of Apple devices
- Apple apps
- Apple Services

For planned support for MDM features listed in this document, contact your MDM vendor.

NOTE: This material is provided for information 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.

Security updates

Apple continues to increase the security of our hardware, software, and services. The following are security-related updates for macOS 12, iOS 15, iPadOS 15, and tvOS 15.

Unlock iPhone with Apple Watch

An iPhone can be unlocked by an Apple Watch when a user is detected with their nose and mouth covered. The iPhone must be running iOS 14.5 or later, and the Apple Watch must be running watchOS 7.4 or later. MDM administrators can also use a restriction to prevent this feature.

For more information, see System security for watchOS in Apple Platform Security.

iCloud Private Relay

iCloud Private Relay helps protect users when browsing the web with Safari (including all DNS name resolution requests) and a small subset of app content. This helps prevent user profiling. It does this by using different types of proxies, an *ingress proxy*, managed by Apple and an *egress proxy*, managed by a content provider. To use iCloud Private Relay, the user must be running beta versions of iOS 15, iPadOS 15, or macOS 12, and be signed in to their paid iCloud account with their Apple ID. iCloud Private Relay can then be turned on in Settings > iCloud or System Preferences > iCloud. iCloud Private Relay doesn’t affect private domains (for example, domains that aren’t publicly listed) and is unable to be used with:

- Managed Apple IDs
- Other proxies (for example, an existing web proxy)
- Local network traffic (for example, network traffic on the same subnet)
- Network extensions and virtual private networks (VPNs)

Without iCloud Private Relay
When a device connects to the internet, it’s using an internet service provider (ISP) to obtain an IP address. For a cellular connection, the ISP is the carrier. When a user visits websites, anyone on that IPS’s network can view the website requests based on the DNS addresses of the websites the user entered. This allows ISPs to compile a list of websites a user visits. The servers that host the websites can also obtain the IP address of the user’s device, determine an approximate location of the device, and get a list of other websites the user visited, even if cross-tracking is turned off in Safari.

With iCloud Private Relay
After iCloud Private Relay is configured by the content provider, only Apple and the ISP will be able to obtain the IP address of the device because Apple manages the ingress proxy. The egress proxy selects an IP address related to

the device’s city or region and receives only the DNS name of the website from the ingress proxy, which is then used to connect the device to the website.

To help make sure every transaction is secure, iCloud Private Relay uses the following means:

- The QUIC transport layer network protocol
- The HTTP/3 protocol
- The Oblivious DNS-over-HTTPS (DoH) protocol extension
- Blind signatures

IMPORTANT: During this process no one—not even Apple—can see both the IP address of the device and the website or app content the user is viewing.

Preventing iCloud Private Relay
Network administrators can prevent this by blocking access to mask.icloud.com. Users will see a message stating that in order to access the internet, they must turn off iCloud Private Relay or connect to another network.

For more information, see the WWDC sessions *Get ready for iCloud Private Relay* and *Accelerate networking with HTTP/3 and QUIC*.

macOS management updates

The following macOS updates add new device management capabilities to Mac computers.

Apple Configurator for iPhone

Apple Configurator for iPhone allows an account with the role of Administrator or Device Enrollment Manager to add a Mac to Apple School Manager or Apple Business Manager regardless of where the Mac computers were purchased. When a device is set up this way, it behaves like any other enrolled device, with mandatory supervision and MDM enrollment. The user has a 30-day provisional period to remove the device from enrollment, supervision, and MDM.

How it works
An Apple School Manager or Apple Business Manager account with the role of Administrator or Device Enrollment Manager signs in to Apple Configurator for iPhone and uses the iPhone camera to scan an image in the Mac Setup Assistant. After the Mac is assigned to the organization, it appears in an "Added by Apple Configurator" MDM server placeholder in Apple School Manager or Apple Business Manager; the Administrator or Device Enrollment Manager can then assign it to an MDM server for Automated Device Enrollment.

For more information, see the WWDC session *Manage devices with Apple Configurator*.

Managed apps

With macOS 12, apps can be managed if User Enrollment is the method used to enroll in an MDM solution (this feature is already possible with Device Enrollment and Automated Device Enrollment). Managed apps that use CloudKit will now use the Managed Apple ID associated with the MDM enrollment. MDM administrators must add the `InstallAsManaged` key to the `InstallApplication` command. Similar to iOS and iPadOS apps, these apps can be automatically removed when a user unenrolls from MDM.

System extensions

In macOS 11.3, installing the System Extension payload changed the state of a system extension. For example, if a system extension was pending user approval, installing the payload activated the extension. Conversely, removing the payload deactivated the system extension.

With macOS 12, there is a new feature, called `RemovableSystemExtension`, which will allow an MDM administrator to remove an app's system extensions. No local administrator authentication is required to remove the system extension.

Device lock

Starting in macOS 11.5, MDM administrators can lock a Mac with Apple silicon with a six-digit PIN (and include a short message). After the command has been sent to the device, the device restarts and the user can see the message and optional phone number. The user can't restart into macOS until the PIN has been entered and validated by the Mac.

recoveryOS password

Starting in macOS 11.5, MDM administrators can set (using the new `SetRecoveryLock` command) a password that must be entered before a user can restart a Mac with Apple silicon into the recoveryOS. For example, the user won't be able to modify security settings or erase the Mac. This password can be set only by the MDM solution; it can be removed by the MDM solution, unenrolling in MDM, or if the Mac is erased. MDM administrators can also verify a recoveryOS password is set by using the new `VerifyRecoveryLock` command.

Erase all content and settings

Mac computers with Apple silicon or an Apple T2 Security Chip running macOS 12 will now allow a local administrator—or, if enrolled in MDM, an MDM administrator— to perform an *Erase All Content and Settings*, similar to iOS, iPadOS, tvOS, and watchOS. All user data is erased along with any additional volumes on the Mac. For a Mac with Apple silicon, the security settings are also reset to their default state (Full Security). An MDM solution can also:

- Use a restriction to prevent erasing all content and settings on a Mac (this feature already exists for iPhone and iPad devices).
- Use the `EraseDevice` command to erase all content and settings.

Mac mini and Lights Out Management (LOM)

The Lights Out Management (LOM) payload works with a Mac mini (M1, 2020) with a 10 Gbit Ethernet card.

macOS, iOS, and iPadOS management updates

The following updates add new device management capabilities to macOS, iOS, and iPadOS devices.

Managing software updates

MDM administrators can prevent devices from offering over-the-air software updates to users until a specified period of time has expired since those updates were published by Apple. They can specify a custom value, anywhere from 1 to 90 days. This delay applies to all operating system updates, although MDM has the ability to send specific updates to devices irrespective of the above restriction. Deferring software updates is available in iOS 11.3 or later, iPadOS 13.1 or later, macOS 10.13 or later, and tvOS 12.2 or later.

In macOS 11.3 or later, an MDM administrator may choose to delay major releases for a longer time than they can delay minor releases, thus allowing users to still benefit from important security updates while the administrator works to approve the latest major release for production in their environment. For example, an administrator may choose to hold back a major release while, in contrast, immediately offering every minor release. In this way, the administrator can work to approve the latest major release for production in their environment, while at the same time users can benefit from important security updates. For more information, see Managing software updates for Apple devices in MDM Settings for IT Administrators.

Installing software updates
In iOS 15, iPadOS 15, and macOS 12, an iPhone, iPad, iPod touch, and Mac will have the ability for an MDM solution to calculate update applicability in a timely and accurate manner as soon as an update is published. For example, MDM can request a macOS version (such as 12.1) when making a command to `ScheduleOSUpdate`, and then devices will be able to get available updates through a query to the Apple Software Update server.

With macOS 12, there is now support for the following:

- A new `DeviceInformation` query key, called `SoftwareUpdateModelID`, returns the hardware model string to determine what updates are eligible for specific Mac models (also supported on iOS and iPadOS).
- Specify the maximum number of deferrals, after which a forced update will occur. This allows more control over the `InstallLater` action to enforce updates by specifying the number of times the device should prompt to install before the update is enforced. This number is defined by the `MaxUserDeferrals` key. This key implies the existing action, `InstallForceRestart` after the maximum number of deferrals has been reached.

- Using the `ProductVersion` key (already supported on iOS and iPadOS).
- Installing a beta update of macOS (already supported on iOS and iPadOS).

The `ScheduleOSUpdate` command `InstallAction` string can include the following:

Action	Earliest OS	Support	Description
InstallASAP	iOS 9 iPadOS 13.1 macOS 11 tvOS 12	Major Minor	In iOS, iPadOS, and tvOS, install a previously-downloaded software update. In macOS, download the software update and trigger the restart countdown notification. The bootstrap token for can be used for macOS.
Default	iOS 9 iPadOS 13.1 macOS 11 tvOS 12	Major Minor	Download or install the update, depending on the current state. MDM administrators can check the `UpdateResults` dictionary to review scheduled updates.
InstallForceRestart	macOS 11	Minor	Perform the Default action and then force a restart if the update requires it. The bootstrap token for can be used for macOS. **WARNING:** InstallForceRestart may result in data loss.
NotifyOnly	iOS 9 iPadOS 13.1 macOS 11 tvOS 12	Minor	Download the software update without installing it.
DownloadOnly	macOS 11	Minor	Download the software update and notify the user through the App Store.
InstallLater	macOS 11	Minor	Download the software update and install it at a later time. The bootstrap token for can be used for macOS.

For more information, see ScheduleOSUpdateCommand.Command.UpdatesItem in Apple Developer documentation.

Slimmed macOS updates

There are two parts to a macOS update, all contained in a single disk image:

- *Base system image:* This contains the recoveryOS and is larger for a Mac with Apple silicon.
- *macOS and preinstalled apps:* This contains updates to macOS and updates to apps that came preinstalled with macOS.

In macOS 12, the size of a software update can be reduced—in some cases up to 2GB. This is accomplished with server-side file system matching. Updates to the base system *and* operating system updates will get changes based on the differences (similar to a repository branch) and images differences will then match the local operating system differences. In this way, updates will contain only the differences.

Update path

Users will have the option to update to iOS 15 or iPadOS 15 (the next latest major version), or to continue to update to newer versions of iOS 14 and iPadOS 14, even after iOS 15 and iPadOS 15 are released. MDM administrators can force the device to allow all updates, or only current major version updates. MDM vendors can use three values to manage this feature for devices enrolled in MDM. A new Settings command with a `SoftwareUpdateSettings` dictionary will contain a key (`RecommendationCadence`) with three values:

- *2:* It will show the update path for the operating system with highest version number.
- *1:* It will show the software update with the lower version number, if available.
- *0:* It will show both options (the default).

For more information, see the WWDC session *Manage software updates in your organization*.

iOS and iPadOS management updates

The following updates add new device management capabilities to iOS and iPadOS devices.

User enrollment updates

User Enrollments in iOS 15 and iPadOS 15 adds support for iCloud Drive as well as a new account-based enrollment experience. For example, when a user brings their own Apple device to work or school, they sign in with their Managed Apple ID (in Settings > General > VPN & Device Management) and are presented with an instance of iCloud Drive that's owned by the organization.

When a user enrolls their device, the MDM solution can verify the user before the enrollment profile is downloaded to the device. Also, the MDM solution doesn't have to personalize each user enrollment. The four stages of user enrollment into MDM are:

1. *Service discovery:* The device identifies itself to the MDM solution.
2. *User enrollment:* The user's credentials are sent to the MDM solution to pass these on to an identity provider (IdP) for verification.
3. *Session token:* A session token is issued to the device to allow ongoing authentication.
4. *MDM enrollment:* The enrollment profile is sent to the device with payloads configured by the MDM administrator.

Users can still access files in their personal iCloud Drive too. The iCloud Drive for the organization appears in the Files app. In iOS and iPadOS, Managed apps and managed web-based documents all have access to the organization's iCloud Drive—and through existing restrictions, the MDM administrator can keep specific personal and organizational documents separate.

For more information, see the WWDC session *Discover account-driven User Enrollment*.

Managed pasteboard restriction

Managed pasteboard is a new restriction with iOS 15 and iPadOS 15 that allows control over the pasting of content from an app using Open In management to follow the managed Open In rules that are enforced. Apple apps that work with the managed pasteboard include Calendar, Files, Mail, and Notes. Third-party apps are controlled based on whether they are managed or not. When a user attempts to paste content where it isn't permitted, a "Paste Not Allowed" notice appears along with the organization's name (which can be changed using the `Settings` command). Apps also can't request items from the pasteboard when this restriction is used and the content crosses the managed boundary.

Required app

With iOS 15 and iPadOS 15, MDM administrators will be able to install an app on unsupervised devices at the time of enrollment. The user must consent to this installation when they enroll in the MDM solution. To enable this feature, administrators set the `iTunesStoreID` of the App Store app in the MDM profile. They must then make sure the app has a device or user license and send the `InstallApplication` command after MDM enrollment. MDM administrators can also add a managed app attribute to make sure the user can't remove the app. If the user already has the app installed, they'll receive an alert requesting MDM management of the app.

Payload identifiers

With iOS 15 and iPadOS 15, payloads in a single configuration profile that contain the same UUID will no longer be able to be installed. Each payload must contain a unique UUID.

MAC address broadcasting

With tvOS 15, Apple TV will no longer broadcast its MAC address. To prevent unwanted pairing attempts, a new key in the TV Remote payload for iOS and iPadOS—*TVDeviceName*—can be used to remove Apple TV device names in the Apple TV remote widget.

VPN location change

With iOS 15 and iPadOS 15, VPN configurations will now appear in Settings > General > VPN & Device Management.

Temporary session for Shared iPad

In iPadOS 14.5 or later, MDM administrators can send a settings command to Shared iPad that configures Shared iPad to show only the Temporary Session option at the sign-in screen and to set each type of Shared iPad session to sign out automatically after a specified period of inactivity.

MDM updates

The following updates add a new device management capability to MDM, along with payload updates to macOS and to iOS and iPadOS.

Declarative management

Declarative management is an update to the existing protocol for device management that can be used in combination with the existing MDM protocol capabilities. It allows the device to asynchronously apply settings and report status back to the MDM solution without constant polling. The four types of declarations are listed below.

Configurations
Description: Configurations are similar to MDM's existing profile payloads; they represent the policies to be applied to the device. For example, accounts, and settings, and restrictions.

*Support: A*ccounts (Calendar, Contacts, Exchange, Google, LDAP, Mail, Subscribed calendar), passcode, profiles, status subscriptions

Assets
Description: Assets consist of reference data that's required by configurations for large data items and per-user data; assets have a one-to-many relationship with configurations.

Support: User identity, user name, password

Activations
Description: Activations are a set of configurations that are applied atomically to the device and that can include predicates, such as "device type is iPad" or "OS version greater than 14." There is a many-to-many relationship between activations and configurations.

Support: A list of configurations, a list of predicates

Management
Description: Management is used to convey overall management state to the device, describing details about the organization and capabilities of the MDM solution.

For more information, see the WWDC session *Meet declarative device management*.

macOS MDM updates

Payload updates for macOS

Payload	Description
Kernel Extensions	Allow users who aren't local administrators to approve kernel extensions.
Extensible Single Sign-On	Include a managed app bundle ID for access control.
Extensible Single Sign-On	Add preferred Kerberos Key Distribution Centers (KDCs).
Setup Assistant	Skip the Allow unlock with Apple Watch pane.
System Extensions	In macOS 11.3, installing or removing this payload can change the state of system extensions on the Mac. If a containing app activates a system extension and the system extension is in a pending state, installing a payload that allows the extension completes the activation process. If a system extension is active, removing a payload that allows the extension deactivates that extension.

New restrictions for macOS

Restriction	Description
Force a delayed major macOS software update	Defer major macOS updates, such as macOS 12 for a period of time.
Force a delayed minor macOS software updates	Defer minor macOS updates, such as macOS 11.5 for a period of time.
Enforce a major macOS software update delay	Enforce a major macOS software update delay, such as macOS 12 to be installed.
Enforce a minor macOS software update delay	Enforce a minor macOS software update delay, such as macOS 11.5 to be installed.
Enforce a non-macOS software update delay	Enforce a non-macOS software update delay, such as a supplemental update to be installed.
Allow erase all content and settings	Prevent users from using Erase All Content and Settings on their Mac.

Updated and new commands and queries for macOS

Category	Command or query	Description
Command	Restart	`NotifyUser` option added to notify the user the Mac will restart. If no user is logged in to the Mac, it will restart without any notification. Introduced in macOS 11.3.
Command	Restart	Rebuild the kernel cache and list paths for specific kernel extensions (KEXTs).
Command	SetRecoveryLock	Set the recoveryOS password.
Command	VerifyRecoveryLock	Verify whether a recoveryOS password has been set.
Query	DeviceInformation	Install iPhone and iPad apps on a Mac with Apple Silicon from Apps and Books in Apple School Manager and Apple Business Manager. Introduced in macOS 11.3.
Query	DeviceInformation	Query whether the device is a Mac with Apple silicon.
Query	Device Information	Return the hardware model string to the MDM solution.

iOS and iPadOS MDM updates

Payload updates for iOS and iPadOS

Payload	Description
Extensible Single Sign-On	Add preferred KDCs.
TV Remote	A new key, `TVDeviceName` can be used to remove Apple TV device names in the remote widget.

New payloads for iOS and iPadOS

Payload	Description
Certificate Revocation (iOS 14.2 and iPadOS 14.2)	Use the Certificates Revocation payload to revoke certificates on an iPhone or iPad. For example, an MDM administrator can create a list of certificates for revocation. Specifying a certificate authority (CA) enables revocation checking for all certificates chaining up to that CA.

New restrictions for iOS and iPadOS

Restriction	Description
Allow Near-field communications (NFC) (iOS 14.2)	Users can’t use built-in NFC hardware in compatible devices running iOS 14.2 or later.
Allow putting an iOS or iPadOS device into Recovery Mode from an unpaired host (Supervised only) (iOS 14.5 and iPadOS 14.5)	iPhone, iPad, and iPod touch previously allowed any external host computer to start a device in Recovery Mode, which meant that the host computer could completely erase the device and restore the operating system. iOS 14.5 and iPadOS 14.5 now prevent this behavior by default.
Force on-device dictation (Supervised only) (iOS 14.5 and iPadOS 14.5)	Users can use dictation instead of their keyboard to enter text with many apps and features that use the keyboard on iPhone, iPad, or iPod touch running iOS 14.5 or iPadOS 14.5. This setting prevents dictated content from being sent to Siri servers for processing.
Auto unlock (iOS 14.5 and watchOS 7.4)	With watchOS 7.4, users can’t use their Apple Watch to unlock their paired iPhone running iOS 14.5.
Force on-device translation	Prevent content for translation from being sent to Apple servers for processing.
Require Managed Pasteboard	Prevent the copying and pasting of content from an app using Open In management to an app that isn’t managed.

Updated and new commands and queries for iOS and iPadOS

Category	Command or query	Description
Settings (iPadOS 14.5)	TemporarySessionOnly	Send a settings command to Shared iPad that allows MDM administrators to configure Shared iPad to show only the Temporary Session option at the sign-in screen.
Settings (iPadOS 14.5)	TemporarySessionTimeout	Set the temporary session of Shared iPad to sign out automatically after a specified period of inactivity.
Settings (iPadOS 14.5)	UserSessionTimeout	Set a user session of Shared iPad to sign out automatically after a specified period of inactivity.
Settings (iPadOS 14.5)	SharedDeviceConfiguration	A dictionary that contains shared device configuration settings.
Settings	SoftwareUpdateSettings	
Query	Device Information	Return the hardware model string to the MDM solution.

Learn more about MDM:

- MDM payloads
- MDM restrictions
- MDM commands
- MDM queries

Apple app updates

The following education apps have been updated for iPadOS 14.5 or later and macOS 11.3 or later.

Classroom

With Classroom for iPad 3.4.1 or Classroom for Mac 2.4.1, teachers can connect to classes in three different configurations in Classroom using their Managed Apple ID from Apple School Manager. They can then invite other teachers and students to the class. The types of classes are:

- *Nearby*: All students are in the same room with the teacher, connected to the school's Wi-Fi network.
- *Remote*: All students (and the teacher) are remote, connected to their Wi-Fi network or using a cellular connection from their iPad (requires the iPad have cellular capability).
- *Hybrid*: Some students are in the same room with the teacher, connected to the school's Wi-Fi network, and some students are remote.

No mobile device management (MDM) solution is required, although integrating with one can change how the student devices function in the classes. These classes are also not compatible with the education configuration profile from the MDM solution that creates MDM-synced classes.

It doesn't matter whether the teacher and students have iPad devices, Mac computers, or a combination of both, the Classroom user interface for the teacher is the same.

For more information, see:

- Classroom User Guide for iPad
- Classroom User Guide for Mac

Schoolwork

Updates to Schoolwork 2.3 include the following:

- Exit tickets to survey student learning
- Request and create credentials in Schoolwork
- Refreshed, simplified sidebar navigation
- Common Cartridge file format support
- View student progress on files and links

For more information, see:

- Schoolwork User Guide for teachers
- Getting Started Guide for teachers
- Set Up Guide for administrators

Additional updates

Assessment Mode
In iOS 15, iPadOS 15, and macOS 12, Assessment Mode will support more than one app available to the user.

Apple services updates

Below are updates to enterprise and educational services, along with information on AppleSeed for IT and deprecated services.

Apple School Manager and Apple Business Manager

Apple School Manager and Apple Business Manager allow organizations to seamlessly enroll devices in an MDM solution, buy apps and books in bulk, and create Managed Apple IDs.

Domain verification
On May 26, 2021, Apple required organizations to verify all domains associated with Apple School Manager or Apple Business Manager. This means the organization will no longer be able to create new Managed Apple IDs on unverified domains after May 26, 2021.

In December of 2021, all Managed Apple IDs associated with unverified domains will be automatically moved to the reserved domain associated with the organization.

For more information, see the Apple Support article, Verify domains in Apple Business Manager and Apple School Manager.

Tax-exempt status verification
In an update this summer, a user with the role of Administrator in Canada and the United States can enter and update their organization's tax information as taxable or tax-exempt. If tax-exempt is selected, an Apple Customer Number or Certificate ID that's provided by Vertex (a third-party company) must be added. If the organization doesn't have a Certificate ID, a user with the role of Administrator will use the built-in tax-exempt certificate process in Apple School Manager or Apple Business Manager.

For more information, see:

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

Apps and Books management updates

Apps and Books API
With version 2 of the Apps and Books API, MDM vendors can take advantage of a number of improvements when managing an organization's content. MDM vendors who adopt version 2 of the Apps and Books API will be able to manage an organization's content more quickly, more efficiently, and more reliably.

Note: IT administrators should ask their MDM vendor when this update will be supported.

Real-time notifications
MDM vendors can subscribe to real-time notifications for state changes to assignments, assets, and registered users, so they don't need to continually request the latest state. The notifications are opt-in, and vendors will receive notifications for just the types they subscribe to in client configuration. Features include:

- *Assignment notifications:* Notify in real-time exactly what assignments have successfully been performed and to which devices.
- *Asset notifications:* Notify in real-time when changes to assets (apps or books) occur from purchases, transfers, or refunds.
- *Registered user notifications:* Notify in real-time the latest state of users for both their initial creation and subsequent invitation acceptance.

Asynchronous processing
The Apps and Books management API will use asynchronous processing for incoming requests, thereby providing a synchronous response for each management action. As a result, parallelism will be handled on the server side, which allows for optimizations that lead to larger requests being fulfilled more quickly. For large deployments (for example, back-to-school) this significantly improves response times and reliability.

Increased request sizes
Asynchronous processing allows the API to accept larger request sizes. It will support multiple assets, (up to 25 from 1) and more devices (up to 1,000 from 10) in a single request. These dynamic limits are exposed in service configuration. As a result of these improvements, a deployment of 25 apps to 10,000 users—which used to take 25,000 requests—can be accomplished in just 10 requests.

For more information, see the WWDC session *Improve MDM Assignment of Apps and Books and developer documentation*.

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 Business Manager or Apple School Manager designate which account roles in their organization can participate. Participants use their Managed Apple ID to access the program and their feedback is associated with their organization.

To access program resources, sign in to https://appleseed.apple.com/it using a Managed Apple ID issued by 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 more information, see the AppleSeed Program Planning Guide, which is available in the Downloads section of the AppleSeed for IT web portal.

Deprecated services

iTunes U

iTunes U will be discontinued at the end of 2021. Until then, it will continue to be supported and available to all existing customers. However, institutions and instructors can no longer create new iTunes U instructors or courses or publish new public courses. To assist with migration, Apple will:

- Add support for ClassKit to iTunes U so administrators can easily transition to Schoolwork
- Offer an export feature to iTunes U to support moving to third-party apps and to learning management systems

For more information, see the iTunes U May 2021 Update.

Additional resources

Learn more about Apple deployment and security in the following documents:

- AppleSeed for IT
- Apple Platform Security
- Security Certifications and Compliance Center
- Deployment Reference for iPhone and iPad
- Deployment Reference for Mac
- MDM Settings for IT Administrators
- Apple Configurator 2 User Guide
- Apple School Manager User Guide
- Apple Business Manager User Guide
- Classroom User Guide for iPad
- Classroom User Guide for Mac
- Schoolwork User Guide for Teachers
- Schoolwork User Guide for Students

For more information on developer information regarding the MDM changes in this document, see Device Management on the Apple Developer website.