What’s New for Enterprise and Education

iOS 11, macOS High Sierra 10.13, tvOS 11, and deployment tools and services

September 2017
Introduction

This document is a summary of what’s new in iOS 11, macOS High Sierra 10.13, and tvOS 11 for IT system administrators. It complements the iOS Deployment Reference and the macOS Deployment Reference to help you understand the key technologies for deploying devices at scale and providing an optimal experience for your users. It provides information about recent updates that enhance deploying and supporting iPhone, iPad, iPod touch, Apple TV, and Mac computers in a large-scale organization such as an enterprise or education institution.

This guide covers the following topics:

- Networking
- Device Enrollment
- Configuration and Management
- Apple School Manager
- Apple Apps and Tools

Learn more about Apple device deployment at: https://www.apple.com/support/business-education/
Networking

The following updates optimize how Apple devices and apps run within a network infrastructure.

Wi-Fi

QoS for macOS
The “fast lane” can now be applied to macOS apps by IT administrators, allowing them to be prioritized for optimal performance on Cisco networks.

Networking APIs
New APIs allow networking solution developers to get performance insight and reporting from iOS devices as they join and roam on Wi-Fi networks.

Collaboration

Tap to join
Conference URLs are now added to the iOS Calendar event schema so users can simply tap to join Cisco Spark or Cisco WebEx voice calls and video meetings directly from the event window in Calendar (and Notifications).

WebRTC for Safari
Safari now supports Web Real-Time Communication (WebRTC) protocols and APIs. This enables developers to create clientless solutions for web meetings and other collaboration solutions in Safari on Mac.

ReplayKit
Share what's on a user’s iOS screen with another user via video collaboration apps such as Cisco Spark and Cisco WebEx. Live stream what's on a user’s iOS screen from any app that supports ReplayKit.

Security

Content filtering APIs
New APIs in iOS 11 build on content filtering functionality first introduced in iOS 8 to enable greater visibility of file and data used across iOS devices and apps.

General DNS settings
DNS settings on supervised iOS devices can now be configured to allow apps to verify URLs with the content filter prior to the connection being made. App trust or site trust mismatches will be stopped.

S/MIME
Users now have the ability to manage separate defaults independently for S/MIME signing and encrypting. This is supported for all mail accounts, not just Exchange.

Modern Authentication
iOS 11 now supports Office 365 modern authentication, which is based on Active Directory Authentication Library (ADAL), leveraging the Open Authorization 2 (OAuth 2) standard and Multi-Factor Authentication.
Active Directory support
macOS High Sierra 10.13 requires a domain functional level of 2008 or greater when binding to Active Directory.

Encryption
Trust for SHA-1 signed certs has been removed for all TLS connections in iOS 11, macOS High Sierra 10.13, and tvOS 11.

Trust for certs using RSA key sizes smaller than 2048 bits has been removed across all TLS connections to servers in iOS 11, macOS High Sierra 10.13, and tvOS 11.

The default version of TLS used for EAP-TLS negotiation in iOS 11, macOS High Sierra 10.13, and tvOS 11 is TLS v1.2. This can be changed using a configuration profile.
Device Enrollment

The following enhancements are available to Apple devices using Apple School Manager and the Device Enrollment Program (DEP).

Adding devices to Apple School Manager or DEP

You can now add iOS and tvOS devices to Apple School Manager or DEP using Apple Configurator 2.5, even if they were not purchased directly from Apple, an Apple-authorized retailer or an authorized cellular carrier. When you set up a device that has been manually enrolled, it will behave like any other enrolled device, with mandatory supervision and mobile device management (MDM) enrollment. However, the user has a 30-day provisional period to remove the device from enrollment, supervision, and MDM.

tvOS capabilities

tvOS adds new device management capabilities that allow you to configure Apple TV for use in many common education and enterprise scenarios—from a dedicated classroom or conference room AirPlay destination to kiosks running custom apps in Single App Mode.

Device enrollment
tvOS devices can be enrolled in MDM using Apple School Manager or DEP. This includes the ability to supervise Apple TV and skip some or all of the tvOS Setup Assistant panes.

Zero-touch setup
Apple School Manager and DEP make it possible to enroll Apple TV in MDM and fully configure it by simply plugging in power and an Ethernet connection. If Apple School Manager or DEP settings have already been configured for that specific Apple TV, it powers up and enrolls in MDM without any user input. This allows MDM commands to set its name, install enterprise apps, and install configuration profiles to fully configure Apple TV.

Supervision
tvOS devices can now be supervised using Apple School Manager, DEP, or Apple Configurator 2. Some settings and commands require supervision.

Deprecated enrollment settings

While existing enrollment settings are not changed, in the future all iOS and Apple TV devices added to Apple School Manager or DEP will be supervised with mandatory MDM enrollment. The following settings will be rejected, and have been deprecated:

• Optional MDM enrollment
• Preparing unsupervised devices
Configuration and Management

The following updates add new device management capabilities to Apple devices.

**NOTE:** Support for the DES algorithm has been deprecated in the SCEP payload in iOS 11, macOS High Sierra 10.13, and tvOS 11.

**iOS**

**iOS Payloads**

**Cellular payload (iOS 10.3)**
You can set the protocol to IPv4, IPv6, or both for the following:
- Voice protocol
- Default data protocol
- Roaming data protocol

**DNS Proxy payload—Supervised only (iOS 11)**
Automatically identifies the app and DNS provider that have a proxy network extension.

**IKEv2 configurations in the VPN payload (iOS 11)**
Allows you to set the minimum and maximum TLS version (1.0, 1.1, 1.2) for IKEv2 connections.

**iOS Restrictions**

The following restrictions can be enabled to allow or restrict the use of some features:
- Manual creation of virtual private networks (VPNs) (iOS 11)
- Remove system apps (iOS 11)
- AirPrint (iOS 11)
- AirPrint discovery with iBeacon (iOS 11)
- AirPrint saving authentication credentials to Keychain (iOS 11)
- Force AirPrint to require a trusted TLS certificate (iOS 11)

**Supervised only**
- Dictation (iOS 10.3)
- You can force a device to use only the Wi-Fi networks you specify in the Wi-Fi payload (iOS 10.3)
- The above restriction now excludes Wi-Fi networks in carrier payloads (iOS 11)
- Allow a teacher to observe a student’s screen in Classroom when a student joins a class (iOS 10.3)
- Allow a teacher to lock an app open in Classroom when a student joins a class (iOS 11)
- Allow a teacher to perform actions in Classroom when a student joins a class (iOS 11)
Supervised only in 2018

Some restrictions that were previously available to all managed devices will be available only on supervised devices in 2018:

- App installation
- App removal
- FaceTime
- Safari
- iTunes
- Explicit content
- Multiplayer gaming
- Add Game Center friends
- iCloud documents and data

iOS Command and queries

iOS

- Check if the iOS device is network tethered (iOS 10.3)
- Erase device now provides an option to preserve data plan for Apple SIM devices (iOS 11)

iOS—Supervised only

- Perform an iOS update on passcode-locked devices without removing the passcode (iOS 10.3)
- Play Lost Mode sound on an iOS device (iOS 10.3)
- Restart an iOS device (iOS 10.3)
- Shut down an iOS device (iOS 10.3)

macOS

macOS Payloads

Smart card (macOS 10.12.4)
Allows you to set which smart cards to be paired. Includes certificate check and defining the number of smart cards per user.

System migration (macOS 10.12.4)
Allows you to set if the user can specify additional custom paths, which should also be copied when migrating from a Windows PC.

Security and privacy payload (macOS 10.13)
- Updated FileVault escrow personal recovery key for APFS.
- You can enforce new password requirements when the screen is locked.

Network payload (macOS 10.13)
You can configure Ethernet connection settings based on status: first, second, first active, second active, etc.

Extensions payload (macOS 10.13)
Allow or deny extensions and extension points.

IKEv2 configurations in the VPN payload (macOS 10.13)
Allows you to set the minimum and maximum TLS version (1.0, 1.1, 1.2) for IKEv2 connections.
macOS Restrictions

The following restrictions can be enabled to allow or restrict the use of some features:

macOS 10.12.4
- iCloud Mail, Contacts, Calendars, Reminders, Bookmarks, Notes (granular for each)
- Touch ID to unlock the screen
- iCloud desktop and documents

macOS High Sierra 10.13
- Content caching
- User can set lock message
- Diagnostics sent to Apple
- Safari AutoFill
- Dictation
- AirDrop
- User can modify their password
- Delay software update notification
- Game Center
- Multiplayer games
- Add Game Center friends

macOS Commands and queries
- Delay OS update for DEP-enrolled devices
- List users
- Unlock user
- Delete user
- Set Firmware password*
- Verify Firmware password
- Query Firmware password
- Query active extensions
- Query for available OS updates
- Restart
- Shut down

*NOTE: If you want to update the firmware password on a device that already has one set, you’ll need to provide the current password.
tvOS

**tvOS Payloads**

**General settings (tvOS 10)**
You use the General payload to define the name and identifier of a profile, and to specify when the user can remove the profile after it is installed.

**Certificates (tvOS 10)**
You use the Certificates payload to add certificates and identities to the device.

**Network (tvOS 10)**
You use the Network payload to configure network settings on Apple TV.

**SCEP (tvOS 10)**
You use the SCEP payload to specify settings that allow the device to obtain certificates from a certificate authority (CA) using the Simple Certificate Enrollment Protocol (SCEP).

**Global HTTP Proxy—Supervised only (tvOS 10.2)**
Use the Global HTTP Proxy payload to specify a proxy for all HTTP traffic to and from the device. If you choose Manual proxy type, you need the proxy server address—including its port, and optionally a user name and password—for logging in to the proxy server. If you choose Auto proxy type, you can enter a proxy auto-configuration (PAC) URL.

**Single App Mode—Supervised only (tvOS 10.2)**
Use the Single App Mode payload to specify a single app that can be used on an Apple TV.

**Conference Room Display (tvOS 10.2)**
Use the Conference Room Display payload to force a supported Apple TV into Conference Room Display mode. You can also include an optional message that is displayed onscreen. To undo a change to these settings, remove the profile from the device.

**AirPlay (tvOS 11)**
Require first-time passcode, passcode, or password for AirPlay.

**App configuration (tvOS 11)**
Use the App Configuration payload to provide managed app settings.

**Home Screen layout—Supervised only (tvOS 11)**
Use the Home Screen layout payload to configure the Home Screen layout of Apple TV.

**tvOS Restrictions**
The following restrictions can be enabled to allow or restrict the use of some features:

- Require AirPlay passcode on first use (tvOS 10.2)

**Supervised only**

- Pair with iOS Remote app (tvOS 10.2)
- Modify name of Apple TV (tvOS 10.2)
- AirPlay security passcode (tvOS 11)
- Restrict app usage—allows any apps to be placed in an approved list or in a disapproved list (tvOS 11)
tvOS Commands

• Install enterprise tvOS apps via MDM (tvOS 10.2)
• Erase (tvOS 10.2)
• Restart (tvOS 10.2)

Device enrollment updates

The following Setup Assistant screens can now be skipped.

iOS 11
• Keyboard chooser
• Apple Watch migration

tvOS 11
• Sign in to TV provider
• Set up with your iOS device

Certificate pinning

MDM enrollment payloads can now include an approved list of trusted certificates for communication with the MDM solution.

NOTE: Check with your MDM vendor to ensure that this feature is supported.

Certificate trust

Partial trust
Partial trust of certificates was introduced in iOS 10.3. MDM vendors’ certificates were trusted for all communications except SSL. Additionally, if the certificate was installed manually, only partial trust was enabled. The user had to manually enable full trust.

Full trust
If a certificate is automatically installed from a payload from an MDM vendor or installed using Apple Configurator 2, that certificate is fully trusted. If the certificate is manually installed by a profile that also contains an MDM enrollment payload, the certificate is also given full trust. The certificate payload should be in the MDM enrollment profile to remove the step of manually trusting the certificate.
Apple School Manager

The following are updates to Apple School Manager, a simple web-based portal for IT administrators to manage people, devices, and content all from one place.

New features

• Streamlined design and new user interface
• New activity view to log all your actions
• Ability to set initial temporary passwords for all Student Managed Apple IDs
• Support for PowerSchool (9.0 or later)
• New filter and search for location, classes, and accounts
• Ability to delete unused and inactive accounts

Enhancements

• Increased support for up to five Administrator accounts
• Better error handling of activity logs via crash reporter
• Change your user profile under settings
• Export account sign-ins via PDF or CSV
• Password reset emails and PDFs are now localized
• Apply Managed Apple ID format changes to existing users
• Managed Apple ID format can now include a user’s SIS username
• Ability to bulk update of Apple ID formats
• Emails now support mobile devices

View Apple School Manager release notes: https://support.apple.com/en-us/HT207191
Apple Apps and Tools

The following updates increase the functionality of Apple devices and how they work with Classroom, Shared iPad, Apple Configurator, Profile Manager, and Content Caching.

Classroom

Updates
- Teachers can create classes without requiring any configuration via MDM (2.0).
- Teachers and students can share documents and URLs with each other (2.0).
- Teachers can mute student devices (2.0).
- Using the three new restrictions listed above, schools can get most of the behavior of IT-created classes for teacher-created classes on supervised student devices (2.1).
- Student activity view presented to teacher at conclusion of each class session (2.1).

Classes
Teacher-created classes allow students to control which Classroom features the teacher can use without prompting the student each time.

Shared iPad

Restore user quota
After updating to iOS 10.3 or later, you can restore user quota management in one of these ways:
- Delete all existing user caches from the iPad.
- Erase the device and reconfigure it as Shared iPad.

Apple Configurator 2.5

Apple Configurator 2.5 supports all of the iOS and tvOS payload and restrictions updates shown in the Configuration and Management section of this document.

Add through device enrollment
Allows you to add iOS devices and Apple TV that you have in your possession to Apple School Manager or DEP.

Network pairing
Use Apple Configurator 2.5 on macOS High Sierra 10.13 to connect to Apple TV running tvOS 11 over your network.

Profile Manager

Profile Manager supports all of the iOS, macOS, and tvOS payload and restrictions updates shown in the Configuration and Management section of this document.
Content Caching

The caching service is now built into macOS High Sierra 10.13 and configured in the Sharing pane of System Preferences, with all of the previous caching service settings available. A new feature, called Parents, allows you to select a Mac that will serve all of its cached content to your Mac. For example, if you have a district office, you could make an iMac your parent for the caching service. Locations throughout the city could use the district office as their parent caching service, allowing potential updates to flow from the district office to each location. Parents can also host other caching services, making tiered caching configuration possible.

NOTE: Caching iCloud content should not be done by a parent content caching service. Each location should cache their own iCloud content.

Tethered caching

A tethered caching service is available in macOS 10.12.4 or later. This service allows Mac to share its Internet connection with many iOS devices connected via USB and cache-specific types of content as they are installed on each connected device.

How it works

Content is downloaded once to the Mac and cached before it is delivered over USB to each of the connected iOS devices for installation. This can save time, local Wi-Fi, and bandwidth when using a cart or USB hub and updating several devices at once—as compared with each device updating individually over Wi-Fi. It is particularly useful for installing many large apps while preparing devices for the beginning of a semester or new school year. Depending on your Internet connection, caching content may take some time.

The following are required for the tethered caching service in macOS 10.12.4 or 10.12.5:

• Running the command to enable the service requires administrator privileges.
• All iOS devices must have iOS 10.3 or later installed.
• Mac must have macOS 10.12.4 or later installed.
• Mac must be connected to the Internet via Ethernet and have Wi-Fi turned off.
• A portable Mac should be plugged into a power source, because the tethered caching service prevents it from going to sleep.

The following are required for the tethered caching service in macOS 10.13:

• Enable “share Internet connection” in the Content Caching pane of the Sharing pane in System Preferences.
• All iOS devices must have iOS 10.3 or later installed.
• Mac must have macOS High Sierra 10.13 or later installed.
• Mac must be connected to the Internet via Ethernet or Wi-Fi.
• A portable Mac should be plugged into a power source, because the tethered caching service prevents it from going to sleep.