Hey folks. My name is Darren Wallace and I'm one of the London Apple Admins Organisers. Most people know me as Daz_Wallace on the Mac Admins Slack.
As some of you may be aware, we've had some new OSes released, and today I'm going to fly through some changes to make you aware of.

I've split this talk into 4 key areas as shown above, all of which are based of Apple's recently released Knowledge Base Articles

iOS 17

https://support.apple.com/en-us/HT213892

First up, iOS 17

iOS 17 - https://support.apple.com/en-us/HT213892

DEVICE MANAGEMENT

- MDM can enable account-driven Device Enrollment
- Apple Configurator in iOS 17 can now assign a device to an MDM server
- Sign-in with Apple automatically uses the Managed Apple ID for Managed Apps and a personal Apple ID for non-managed apps.
- MDMs can now enforce a minimum operating system version on Enrolment
- Declarative device management can now be used to manage updates on iOS and iPadOS.
- iOS now provides support for private, data-only cellular networks using LTE, and 5G

- MDMs can enable account-driven Device Enrollment to allow users to enroll their iOS or iPadOS device into management using their organization's Managed Apple ID in Settings.
- Apple Configurator in iOS 17 can now assign a device to an MDM server while it is being added to Apple School Manager, Apple Business Manager, or Apple Business Essentials.
- Sign-in with Apple automatically uses the Managed Apple ID for Managed Apps and a personal Apple ID for non-managed apps.
- MDMs can now enforce a minimum operating system version on enrolling devices when using Automated Device Enrollment.
- Declarative device management can now be used to manage updates on iOS and iPadOS.
- iOS now provides support for private, data-only cellular networks using LTE, 5G Non-standalone (NSA), or 5G Standalone (SA).

iOS 17 - https://support.apple.com/en-us/HT213892

DEVICE MANAGEMENT

- MDM can use "Return to Service" to pre-supply details on an erase command
- Apple Watch can be managed by MDM
- Certs and Identities can be deployed using ACME, SCEP and encrypted PKCS#12 containers
- Self-signed CA certs are automatically added to the device's root trust certificates
- User enrolled devices can be set to disallow Auto Lock being set to "Never"
- MDM can now report on the battery health of iOS devices.

- With Return to Service, MDM can send an erase command including Wi-Fi details, and an optional MDM enrollment profile, so the device can erase all data and automatically proceed to the Home Screen, ready to be used.
- An Apple Watch can be enrolled and managed by MDM when paired to a supervised iPhone.
- New declarations support the deployment of certificates and identities using ACME, SCEP, or an encrypted PKCS#12 container and certificates as .pem or .der encoded files.
- Certificates from a self-signed Certificate Authority (CA) are automatically added to the device’s trusted root certificates.
- Devices enrolled with User Enrollment can now be configured to disallow Auto Lock from being set to Never, which helps to protect organizational data.
- MDM can now report on the battery health of iOS devices.

iOS 17 - https://support.apple.com/en-us/HT213892

BUG FIXES AND OTHER IMPROVEMENTS

- Canceled Exchange events no longer remain on Calendar if they’ve been deleted elsewhere.
- Devices respond to MDM more reliably.
- Apple devices now support 802.1x using EAP-TLS with TLS 1.3
- Network Relay can use a secure HTTP/3 or HTTP/2 relay for proxy all TCP and UDP traffic
- iOS and iPadOS devices support configuring 802.1X over Ethernet.

- Canceled Exchange events no longer remain on Calendar if they’ve been deleted elsewhere.
- Devices respond to MDM more reliably.
- Apple devices now support connection to 802.1X networks using EAP-TLS with TLS 1.3 (EAP-TLS 1.3).
- With Network Relay, a secure HTTP/3 or HTTP/2 relay can be configured to proxy all TCP and UDP traffic.
- iOS and iPadOS devices support configuring 802.1X over Ethernet.

First up, iOS 17

iPadOS 17 - https://support.apple.com/en-us/HT213891

DEVICE MANAGEMENT

- All the same as iOS 17!

- All the same as iOS 17!

iPadOS 17 - https://support.apple.com/en-us/HT213891

SHARED IPAD ENHANCEMENTS

- Using Share iPad? Please refer to "Upgrade your Shared iPad to iPadOS 17" for important information regarding the upgrade process.
  - https://support.apple.com/en-gb/HT213910
  - TL;DR:
    - If you use your Mobile Device Management (MDM) solution to upgrade a Shared iPad, the upgrade won't install if there are existing user accounts on the iPad.
    - If you use the Finder or Apple Configurator on a Mac to update the Shared iPad, the existing users won't be able to log in after the upgrade.
    - Use MDM to remove all users prior to upgrade

- Using Shared iPads? Please refer to "Upgrade your Shared iPad to iPadOS 17" for important information regarding the upgrade process.
- Ouch...

iPadOS 17 - https://support.apple.com/en-us/HT213891

SHARED IPAD ENHANCEMENTS

- MDM can fully configure Shared iPad for a user after they sign in
- New users can skip 'Setup' via a new MDM key
  - `SkipLanguageAndLocaleSetupForNewUsers`
- A Shared iPad using temporary sessions now honours the QuotaSize for those users

- iPadOS 17 allows an MDM solution to fully configure Shared iPad for a particular user after they sign in, ensuring that the device is ready to go when the user is presented with the Home Screen.
- In iPadOS 17, new users devices can skip setup.
- Skip setup: To streamline the sign-in flow even further, a new SkipLanguageAndLocaleSetupForNewUsers option tells the device to use the system settings for all new users.
- Temporary session: A Shared iPad configured for temporary sessions now honors the QuotaSize key for the temporary user. This key helps reserve sufficient space to install apps or other media while a user is signed in.

iPadOS 17 - https://support.apple.com/en-us/HT213891

BUG FIXES AND OTHER IMPROVEMENTS

- All the same as iOS 17!

- All the same as iOS 17!

macOS 14 Sonoma

https://support.apple.com/en-us/HT213893

First up, iOS 17

macOS 14 Sonoma - https://support.apple.com/en-us/HT213893

DEVICE MANAGEMENT

- Better MDM Software Update control
- ADE can be enforced after Setup Assistant
- MDM can enable account-driven Device Enrollment
- Full screen ADE nag
- Platform SSO improvements (#platform-sso)
- Password requirements better
- More granular System Settings restrictions
- MDM can enforce FileVault for Admin users during Setup Assistant

- MDM can enforce software updates by a certain date and time and users get additional information in System Settings when an update is requested and when it's enforced.
- Automated Device Enrollment can be enforced after Setup Assistant.
- MDM can enable account-driven User Enrollment and account-driven Device Enrollment to allow users to enroll their Mac using their Organization ID in System Settings. Profile-based User Enrollment is deprecated and will be removed in a future release.
- The notification that requests the user enroll in MDM is replaced with a full-screen Setup Assistant experience for a Mac using Automated Device Enrollment.
- New features in platform single sign-on.
- Enhancements to password requirement enforcement.
- MDM can granularly restrict more individual settings in System Settings.
- MDM can require admin users to turn on FileVault during Setup Assistant.

macOS 14 Sonoma - https://support.apple.com/en-us/HT213893

DEVICE MANAGEMENT

- macOS now supports Managed Device Attestation.
- Some built in macOS services can be configured via Declarative device management
- Declarative device management can deploy certificates and identities
- New Network relay supports tunnelling as an alternative to VPN
- MDM can set the order in which proxy extensions handle network traffic
- Support for hardware-bound private keys using ACME
- Better screen sharing between Apple Silicon Macs over good connections

- macOS now supports Managed Device Attestation.
- Declarative device management can manage a set of configurations for some built-in services.
- New declarations support the deployment of certificates and identities.
- A new built-in network relay supports secure and transparent tunnelling of traffic as an alternative to using VPN when accessing internal resources.
- MDM can set the order in which transparent proxy extensions handle network traffic.
- macOS now supports the creation of hardware-bound private keys for certificates issued using the ACME protocol.
- Screen sharing capabilities are improved between Mac computers with Apple silicon over high-bandwidth connections.

macOS 14 Sonoma - https://support.apple.com/en-us/HT213893

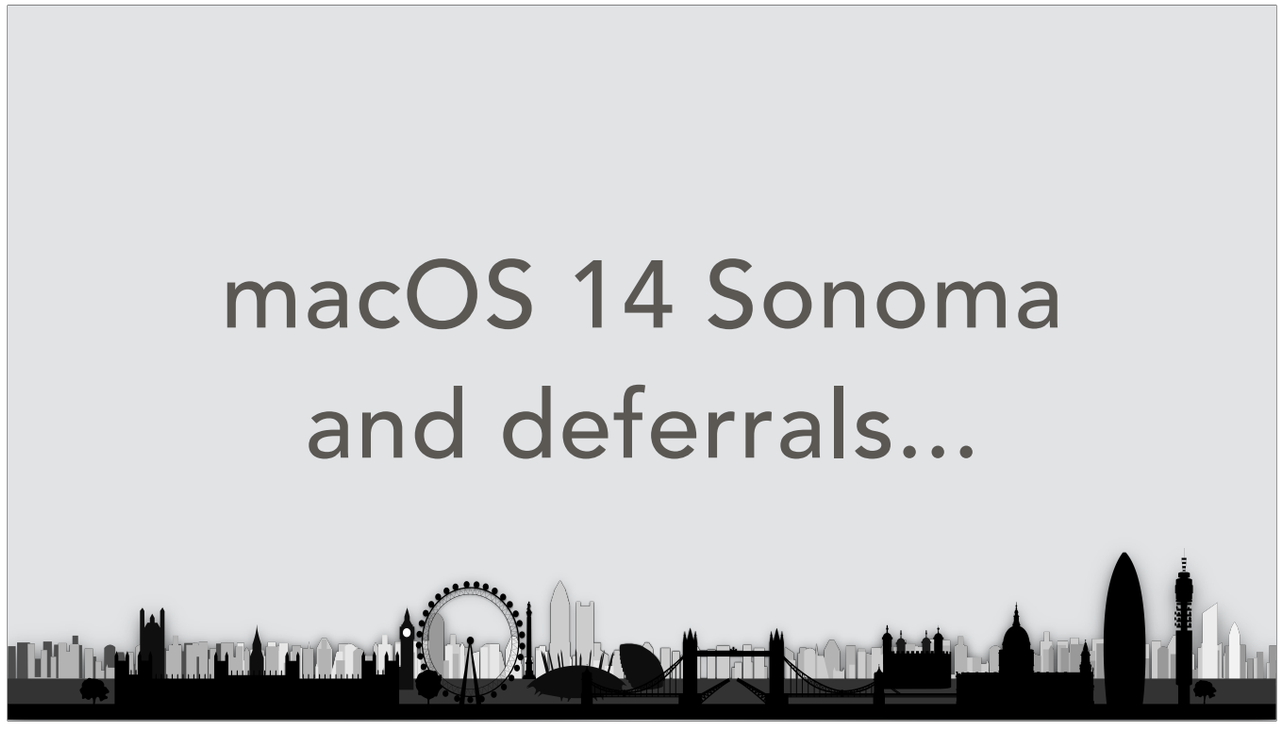
BUG FIXES AND OTHER IMPROVEMENTS

- Apple devices now support 802.1x using EAP-TLS with TLS 1.3
- Finder can be used to revive or restore a USB-connected DFU Mac
- Removing `.AppleSetupDone` no longer relaunches Setup Assistant
- The `audit` subsystem is now disabled by default and is deprecated
- TouchID for sudo can now persist across software updates using:

  `/etc/pam.d/sudo_local`

- Resolved an issue with Exchange events not syncing in Calendar

- Apple devices now support connection to your organization's 802.1X networks using EAP-TLS with TLS 1.3.
- A Mac running macOS Sonoma can revive or restore a USB-tethered Mac in DFU mode using Finder.
- Removing /private/var/db/.AppleSetupDone no longer relaunches Setup Assistant if a local user already exists on the Mac. Erase All Contents and Settings can reset the device and launch Setup Assistant.
- The deprecated audit subsystem is disabled by default in macOS Sonoma. See the auditd manual page for details.
- Touch ID can be allowed for sudo with a configuration that persists across software updates using /etc/pam.d/sudo_local. See /etc/pam.d/sudo_local.template for details.
- Resolved an issue where Exchange events failed to sync in Calendar for some users.

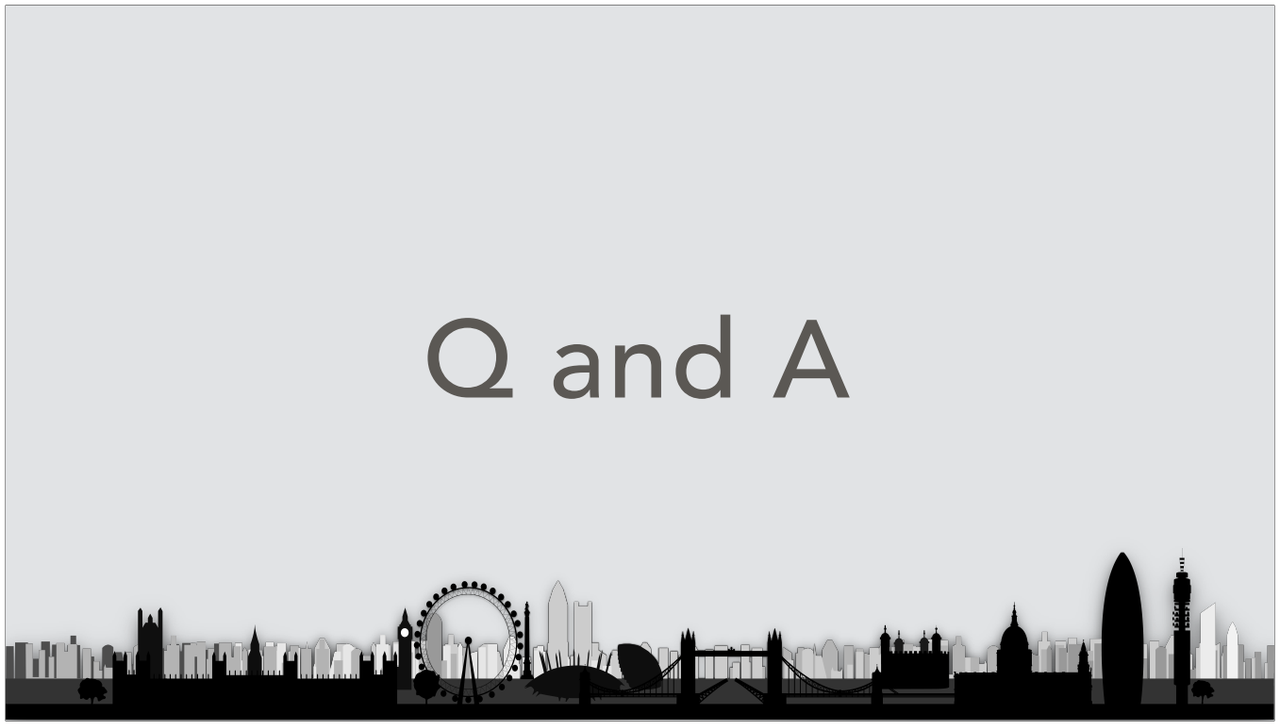


First up, iOS 17

macOS 14 Sonoma and deferrals...

- macOS Sonoma *is* an update to macOS Ventura
- However, it'll appear in the Software Update section of System Settings
- Users can upgrade without being local admins!
- Option 1: Work to provide and verify support ASAP
- Option 2: Defer
  - Defer is a maximum of 90-days. Release was on the 25th September. Deferral will expire on 25th December!

- macOS Sonoma is an update to macOS Ventura
- However, it'll appear in the Software Update section of System Settings
- Users can upgrade without being local admins!
- Option 1: Work to provide and verify support ASAP
- Option 2: Defer
- Defer is a maximum of 90-days. Release was on the 25th September. Deferral will expire on 25th December!



Thanks everyone, is there any questions?