2020
TECH DEEP DIVE

Apple for Enterprise

June 23, 2020 Version 1.0

THE EMEA

Table of contents

1. Preface

The keynote of June 22nd and our Apple for Enterprise paper contains all the new features, visible for the end-user of macOS, iPadOS and iOS.

In this paper we focus on the new technology driving this improved user experience and take a deep dive in the new security control, MDM settings, managed apps and a whole new approach to VPN with the introduction of Per Account VPN!

What was referred to as Big Sur in the keynote presentation is technically macOS 11, the next big iteration of the macOS 10.X OS!
We might use both macOS 11 and Big Sur in this document, referring to the same.

This document puts the focus on the new Apple enterprise features based on the public information from the Apple website and publicly available third-party sources.

Developer beta-versions have been released so developers can go ahead and get creative.
Public beta will be available as of July.
The official launch is planned for this fall.

This document is not a programming guide or training on how to set-up the new features, we provide background on the functionality and more details will be discussed during our upcoming Masterclass webinar! Stay connected and get informed!

Enjoy the reading!

2. Change log

23/06/2020 Version 1.0

3. Before you start

Concerning OS Beta and public Beta programs, you should be aware that:
Your employees have the possibility to take part in this program, unless you tell them not to.

There’s no security risk – the MDM protocol is NOT changing. However, your management system will not recognize the exact mobile OS version and could take unexpected measures such as quarantining the mobile device.

Certain apps might not be working correctly or fail to work on BETA OS versions.

Our recommendation is to advise your employees to install the BETA only on private or test devices that are NOT managed by your MDM or EMM system.

Remember a roll-back to a previous OS version is not supported.

In this paper we will only focus on those new features that deliver a true enterprise value or facilitate data security/privacy. This document does not summarize all new OS features; please refer to www.apple.com for more details on the complete listing.

Written by Björn Kemps, Sebastien Leroy, Raphaël Sapyn and Ulrik Van Schepdael based on the WWDC publicly available information and common sense.

Check https://developer.apple.com/enterprise/ for the latest updates.
No information available through this program is part of this whitepaper.

If you have a developer account, check the enterprise resources for detailed protocol and profile reference details.

4. Deployment and Provisioning

4.1 macOS

With Auto Advance configured in MDM, organizations can order Mac computers and, after they arrive, simply plug them into Ethernet and power them on. The Mac will locate the assigned MDM solution and be automatically configured based on settings from the MDM solution, including skipping all Setup Assistant screens. The user then enters a known username and password at the login window.
note: *If the Mac is configured to use FileVault, an initial additional step requires the user's password.*

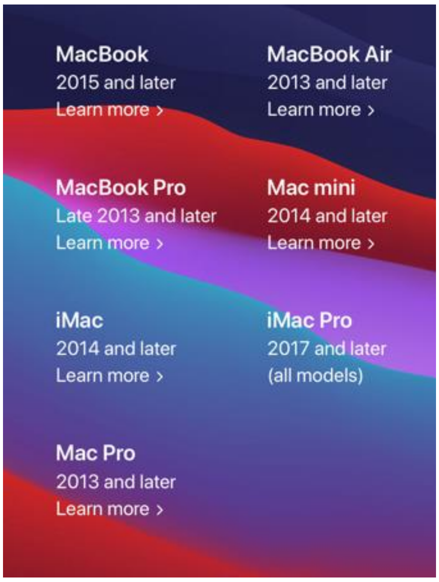
4.2 tvOS

For tvOS this feature was already available if the device is loaded in Apple Business Manager. By simply plugging in power and an ethernet connection, the device will enroll automatically and fully configured in UEM.

In the enterprise we're constantly looking for immediate gains in time and efficiency. The Auto Advance feature is one of those "little things" a regular user don't mind but a system engineer just loves.
More automation to come, including Lights Out Management, in next releases

5. Configuration Management

5.1 macOS 11 Supervision



MacBook
2015 and later
Learn more ›

MacBook Air
2013 and later
Learn more ›

MacBook Pro
Late 2013 and later
Learn more ›

Mac mini
2014 and later
Learn more ›

iMac
2014 and later
Learn more ›

iMac Pro
2017 and later
(all models)

Mac Pro
2013 and later
Learn more ›

We have been waiting for this feature for some years and finally it's there: macOS Supervision!

With macOS 11, UEM enrollments that are user-approved are now considered supervised. This supervision occurs under two conditions:
-either the Mac is enrolling for the first time
-it's being upgraded to macOS 11.

Supervision isn't possible with User Enrollment into MDM; in which case the Mac is always unsupervised.

Available on all Mac's (see visual) supporting macOS 11.

Supervised Mac computers can take advantage of features such as:

- Activation Lock bypass codes
- Control over what software is updated and when
- Use supervised payloads, restrictions, commands, and queries
- Query and delete local user accounts

Supervision is a proven technology on iOS and iPadOS providing more and deeper controls on the devices. To some extend it limits the freedom of the user, but on the other hand it allows far more remote services. Overall, with supervised devices, the enterprise is able to provide a more predictable and reliable experience for its employees.
With an improved efficiency as result!

5.2 Software updates

This year, Apple unified installation technology across all platforms. The Mac now uses the same reliable and secure installation technology as iOS and iPadOS.

Qualification of OS updates is now server-driven, similar to iOS and iPadOS.
macOS knows the exact layout of the system volume, so it can install software updates in the background using an APFS snapshot. Updating in the background while the user is at their Mac happens quickly and goes unnoticed by the user.

This process is similar to the experience users have with iPhone and iPad. The snapshots are cryptographically sealed using authenticated APFS.

With macOS 11, UEM solutions will have more granularity when managing software updates for supervised devices, including:

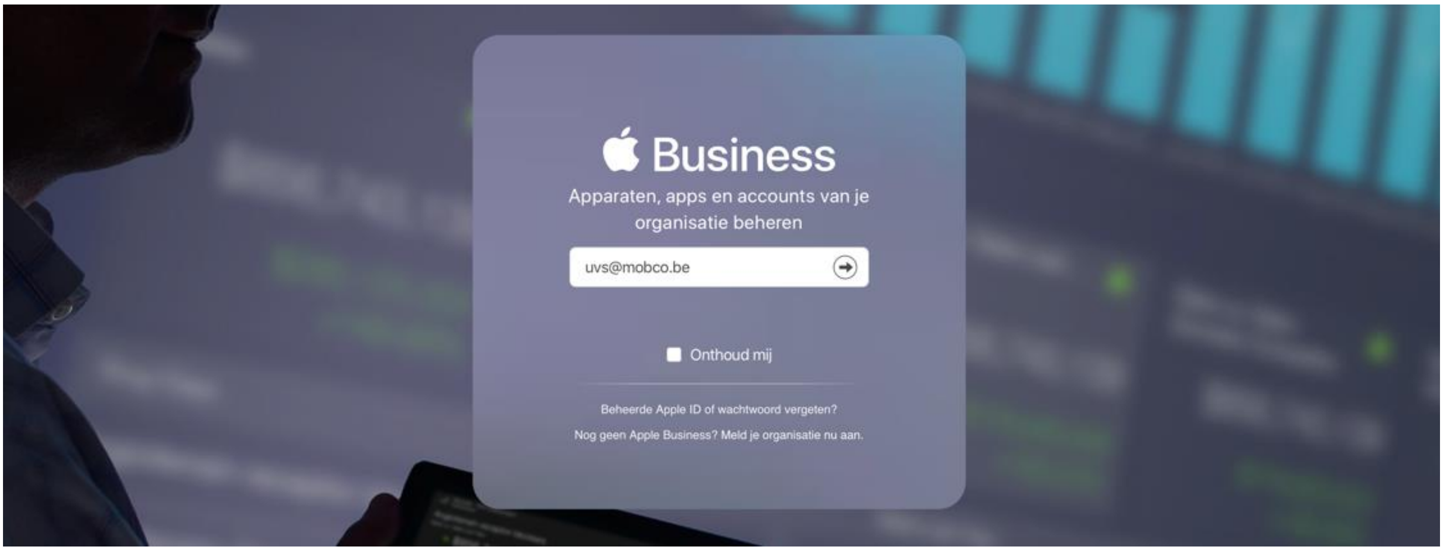
- All macOS updates share the same deferral limit (up to 90 days).
- OS updates (major OS version, minor OS version, supplemental and security) and/or non-OS updates (ie. Safari) can be deferred.
- Starting with macOS 10.15.4, administrators can defer major updates, such as macOS 11.
- Force a software update of any type, including (if necessary) a restart.
- Make the software update visible to the user but not force an install.

The new software update features give flexibility to both the user and the administrator. The user can continue to work while the updates are installed in the background.
On the other hand the administrator or system engineer gets more flexibility in update schemes and deferrals. And above all, it’s secure!

5.3 Managed Apps

Managed apps are available on iOS and iPadOS for some years and is now coming to macOS 11. Free, paid, or custom apps from Apple Business Manager are installed over the air using MDM.

Managed apps can be preconfigured with various settings and provide more control than apps downloaded by the user. The MDM solution can remove managed apps or specify whether the apps should be removed when the MDM profile is removed.



Business

Apparaten, apps en accounts van je organisatie beheren

uvs@mobco.be

□ Onthoud mij

Beheerde Apple ID of wachtwoord vergeten?

Nog geen Apple Business? Meld je organisatie nu aan.

Managed Apps are the cornerstone of the success iOS and iPad saw in business. It provided secure communication between business apps and allowed enterprises to go a few steps beyond traditional app deployment: configuration, control and network!
In many projects we see these values as the missing piece of the puzzle to fully benefit from macOS in business.
This is not a nice feature, it basically announces a new era of macOS management for the enterprise!

5.4 Non-removable Managed Apps

In iOS 14 and iPadOS 14, Managed Apps now have the ability to be marked as non-removable. Previously, administrators had to completely lock the home screen and prevent the deletion of all apps, which constrained the user's ability to manage their own apps.
Administrators can mark their mission-critical managed apps as non-removable. When users try to delete or offload a Managed apps, it prevents it and displays an alert.
Non- removable Managed Apps ensures that an organization's users always have the apps they need on their devices.

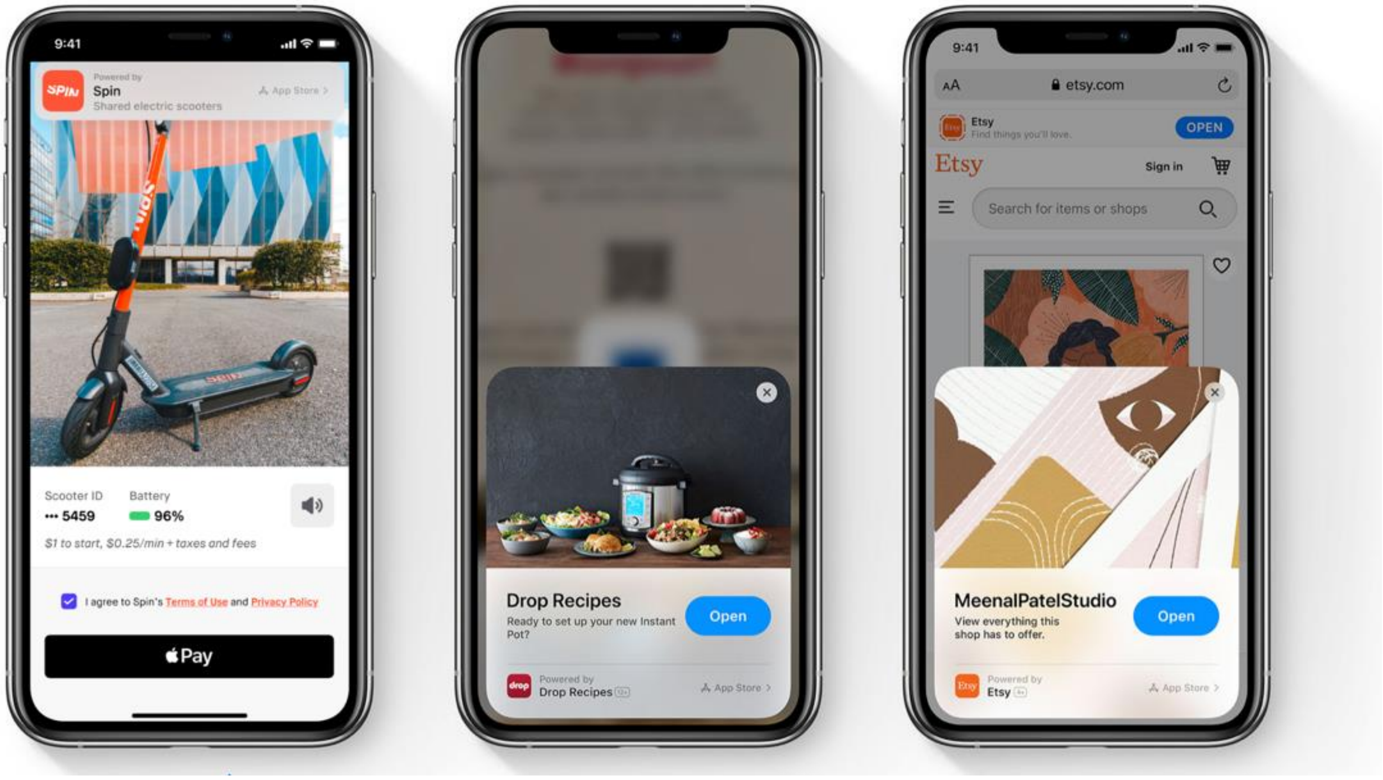
This feature is a popular request in our user community. As a consequence of the Managed Apps feature, we finally can have the flexibility to block removing business critical apps like UEM or MTD clients.

5.5 Allow App Clips

Announced as the "light weight" apps that easily install for quick actions, the Clips do provide a true business advantage: to provide and to consume. However, you might not want employees using the devices to install whatever Clip they encounter and block that feature.

App

App



- iOS & iPadOS: Allow App Clips (*restrict the ability to add App Clips, a new "light weight" type of app and remove already installed App Clips.*

- macOS: Defer software update: now including supplemental and security updates.

We believe the App Clips will be a popular new feature, but since they will be accessible through QR codes, NFC Tags, and can be shared between users this could cause a potential security risk, so good to see they can be restricted.

5.6 DNS Settings

From the https://www.cloudflare.com/learning/dns/dns-security/ website:

“Standard DNS queries, which are required for almost all web traffic, create opportunities for DNS exploits such as DNS hijacking and man-in-the-middle attacks. These attacks can redirect a website’s inbound traffic to a fake copy of the site, collecting sensitive user information and exposing businesses to major liability. One of the best known ways to protect against DNS threats is to adopt the DNSSEC protocol.”

Implementing DNS security makes a lot of sense to protect your business content and also to prevent network “companions” to understand what services or apps your employees are actually using.
A requirement for some organizations.

5.7 Per Account VPN

In the tradition of VPN configuration we think back of the very first VPN profiles we were able to push to iPhones. Over the years, and with every iteration of the OS we got new controls.
A big announcement was made with Per App VPN, where no longer traditional device wide VPN technology was required, but where we could channel all traffic from one app in one tunnel.
Although it covers almost all potential use cases, there are scenario's where even the Per App VPN doesn't provide a solution.

In 2020, for iPadOS and iOS, Apple announces the Per Account VPN doing just as it says: it channels all traffic for that account through that tunnel.

Think about your email client connecting to a certain internal email server, where the email app is not using the VPN for all other personal accounts.

This works for Calendar, Exchange ActiveSync, Contacts, LDAP and Mail.

Difficult to emphasize how important this features actually is, unless you have this strict requirement and were waiting for it.
Important for businesses where cloud services are not part of their daily activities.

5.8 Per App VPN Update

The improved Per App VPN support responds to much more use cases than initially thought. Ever since the Per App VPN exists for Managed Apps, we are struggling with cloud services and on-premise authentication.
Should we run the authentication traffic through a tunnel, and thus also all the app traffic OR should we open the Identity Provider to the internet (like your ADFS) and hope nothing bad happens?

With the new Excluded Domains feature we are able list Cloud Identity Providers to be connected directly, benefitting from regional instances or load balancing. Or, the other way around and keep the Identity Provider behind a tunnel while connecting directly to for example Salesforce.com.

Available on all OS platforms.

We can call it split tunnel for Per App VPN, and it comes down to the same traffic routes, but managed on the device without fiddling around with complex server infrastructure AND manageable on a per App basis!
Keep one VPN solution, but with granular per App controls, the way we like it!

5.9 Always On VPN we said, Always!

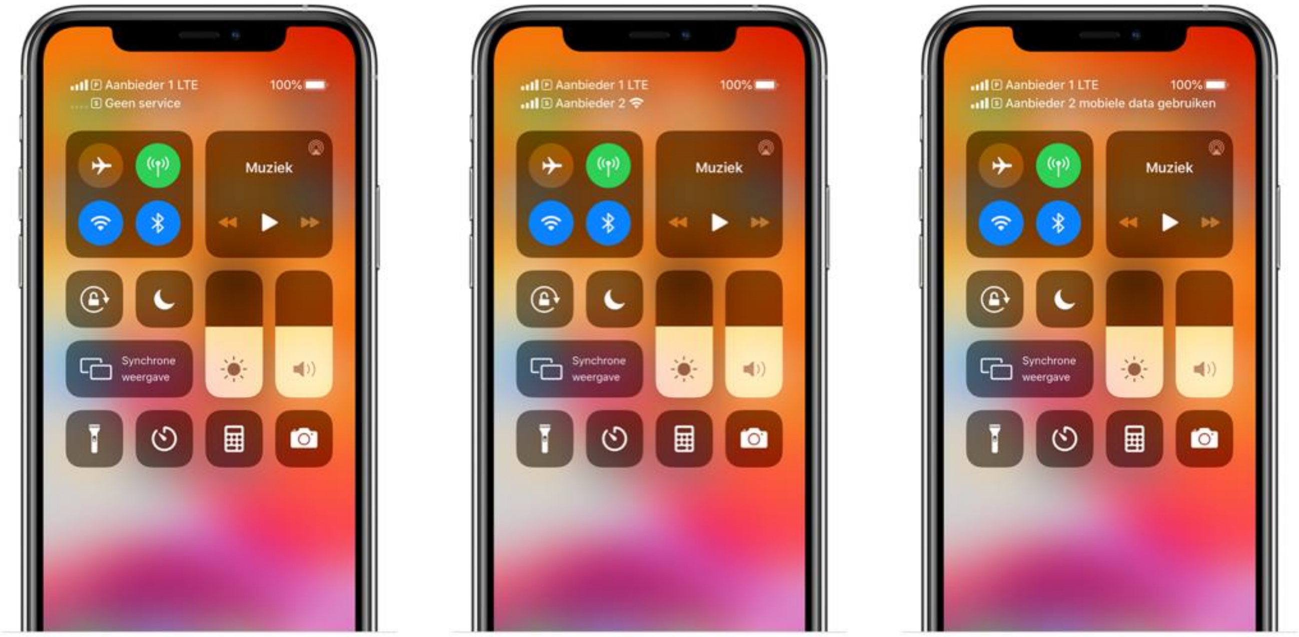
With the ability to route all network traffic for iPadOS and iOS we have fulfilled a requirement that is omnipresent in high security organisations.

As important is the possibility to ensure the On-Demand device wide VPN cannot be turned off, you could call this a restriction but it’s there to protect the business, app, data and finally the employee.

Great new VPN features making this the VPN controls so granular almost any scenario can be achieved. Mobile IT Experts go wild when they see these new possibilities. We understand if you don’t, a bit.

5.10 eSIM identifier

The eSIM offering is getting stronger day by day and most of the local operators are offering these in some form or shape. The downside is that the process is still labor intensive and true benefits are often not (yet) available.

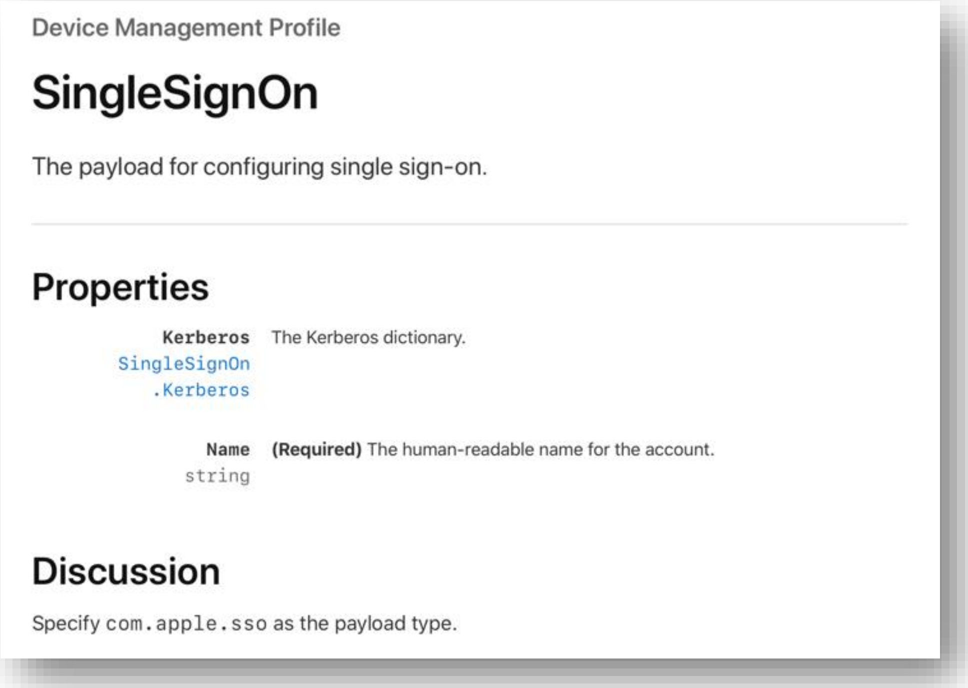


For enterprises the business benefit of eSIM is crystal clear, by using the right MDM controls we can provision, control, remove, upgrade,… the eSIM remotely.
Think about the potential savings in logistics!
This fist MDM control to read information announces a great new chapter for MDM!

5.11 Identity Management and Single Sign-on (SSO)

When you are pointing your device strategy to the enterprise, where security is key, you should cover the authentication part.
This is exactly what has been done over the years and now gets a complete update to even better answer the business requirements when using iPadOS, iOS and macOS!

Embedded wildcard matching is an SSO extension offering a much easier setup of large Identity Providers using a common URL scheme, with slightly different URLs to identify specific customers or tenants.



Device Management Profile

SingleSignOn

The payload for configuring single sign-on.

Properties

`Kerberos` `SingleSignOn.Kerberos` The Kerberos dictionary.

`Name` `string` **(Required)** The human-readable name for the account.

Discussion

Specify `com.apple.sso` as the payload type.

The built-in Kerberos extension available on all platforms is better customizable and with better support for Per App VPN.

When user or employee experience is key, this topic should be on top of the list.
Combined with smart VPN configuration (on per device, per app or per account level), the SSO is a must have to enable secure and efficient work!