Scalefusion

Apple Device Management: How Enterprises Can Make Most of Their Apple Devices

AN E-BOOK FOR IT TEAMS

Scalefusion

Tables of Content

01 Executive Summary

02 Need for Apple Device Management

03 An Overview of Apple Device Management

04 A Quick Look into Apple Business Manager

05 Apple Device Management Modes

06 Apple Device Management: Important Concepts

07 Apple Device Lifecycle Management

08 Scalefusion Apple Device Management: An Introduction

- Apple Device Provisioning
- Policy Configuration via Device Profiles
- Apple App Deployment and Management
- iOS Device Management Modes
- Compliance Alerts and Task Automation
- Scripting
- Driving Apple Device Security
- Managing Content
- Remote Support
- Delivering OS Updates
- Device Inventory Monitoring and Reporting
- Location Tracking and Geofencing
- Scalefusion OneIdP: UEM-Integrated IAM

09 Case Studies

10 Key Takeaways

Executive Summary

Apple devices are indispensable to modern workplaces, valued for their seamless integration, strong security, and user-friendly interfaces. This e-book offers a concise blueprint for IT professionals, business owners, and enthusiasts aiming to streamline Apple device management effectively.

Using this e-book, you can explore deployment strategies to ensure a secure and consistent setup for Apple devices. You can learn how to maximize Apple's security features and help bolster organizational security using Apple MDM. Gain practical insights into Apple device management, covering enrollment, distribution, updates, and user experience cohesion to unveil the potential of Apple devices in enterprise environments.

Scalefusion

Need for Apple Device Management

Apple Mobile Device Management (MDM) is essential for organizations using Apple devices for work. It empowers seamless management of iPhones, iPads, and Macs, ensuring consistent security and compliance. MDM enables centralized control over configurations, applications, and security policies, optimizing device performance. It simplifies the enrollment process, saving time and resources. Robust security features, such as passcode enforcement and remote wiping, offer enhanced data protection.

IT administrators benefit from remote monitoring and troubleshooting capabilities, minimizing disruptions. Compliance standards are easily enforced, aligning devices with organizational policies. Apple MDM is instrumental in streamlining app deployment and updates, fostering a secure, organized, and efficient mobile device environment for businesses.

80%

of businesses reported using Apple devices, showcasing their widespread adoption in 2022

Device sold in 2022

61
million iPads

232
million iPhones

26
million

Mac and MacBook units were sold in 2022

Scalefusion

An Overview of Apple Device Management

Over the years, Apple's approach to device management has undergone a transformative journey, reflecting the company's commitment to user-friendly technology. Initially, when Apple introduced the Macintosh in 1984, device management was a rudimentary concept. Users had limited control, and the focus was on individual device interactions.

The turning point came with the release of the iPhone in 2007, marking a paradigm shift in Apple's device management philosophy. iOS, the operating system powering the iPhone, prioritized seamless integration with Macs and other Apple devices. iCloud, introduced in 2011, further streamlined data synchronization across devices, reducing user hassles.

The launch of the Apple Configurator in 2012 marked a pivotal moment for administrators, providing a centralized tool for configuring and deploying multiple devices simultaneously. Over the years, Apple's commitment to enhancing device management capabilities continued with the introduction of Mobile Device Management (MDM) solutions. This allowed organizations to oversee large-scale deployments of Apple devices efficiently.

Apple's journey in device management reflects a commitment to simplicity and efficiency, empowering users and organizations to harness the full potential of their interconnected Apple ecosystem. With the evolving needs of modern workplaces, Apple device management has undergone a metamorphosis. The introduction of the Apple Business Manager (ABM) in 2018 further enhanced how enterprises manage Apple devices.

While ABM on its own is a great starting point to itemize all the Apple devices (owned by the organization) used in the workplace, it can only perform a limited number of tasks around full-blown device management. This is why using an MDM on top of ABM is the key to making the most of enterprise Apple devices.

A Quick Look into Apple Business Manager

Apple Business Manager, or ABM, serves as a web-based portal designed to streamline the deployment, management, and procurement of Apple devices and services for businesses. Apple School Manager (ASM) serves the same purpose for educational institutions. It provides a centralized space for IT administrators and managers to oversee various facets of their Apple ecosystem, from device enrollment to app distribution.

Apple Business Manager easily handles Apple devices, apps, and services in businesses or schools. It helps organizations manage their Apple setup efficiently, ensuring users have a smooth experience while keeping things secure and following the rules.

Key Elements of Apple Business Manager

Automated Device Enrollment (ADE)

Purchase and deploy devices in bulk, facilitating scalability for organizations. Enroll devices through methods like automated or manual device enrollment. Customize the enrollment process, device configurations, and display of custom messages during setup.

Volume Purchase Program (VPP)

Purchase apps and books through VPP, distributing them to users' devices. Eliminate the need for individual app purchases and streamline license management.

For educational institutions, Apple School Manager (similar to Apple Business Manager) offers specialized features, including support for Managed Apple IDs for students and faculty, shared iPad usage, and tools for configuring devices for student use.
Learn More: A Beginner's Guide to Apple Business Manager

Apple Device Management Modes

It is important to consider the primary device ownership models to understand the device management modes and effective ways to manage them. For employee-owned devices, policies are selectively applied to work apps and data. Whereas company-owned devices can be supervised or unsupervised.

Company-owned devices

Purchased and distributed by the organization; the organization may or may not have complete control over deployment.

Employee-owned devices/BYOD

Purchased by employees for personal use, selectively used for work-related tasks.

Apple Devices that support MDM

iPad with iOS 4.3 or later or iPad 13.1 or later

iPhone with iOS 4 or later

Apple Watch with watchOS 10 or later

Apple TV with tvOS 9 or later

Mac computers with OS X 10.7 or later

Scalefusion

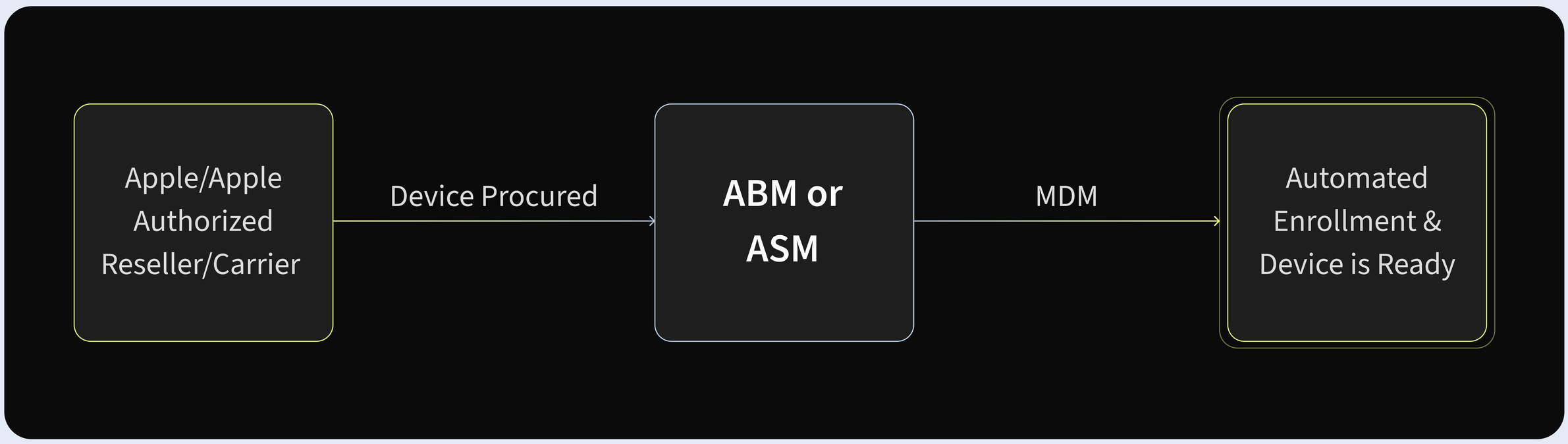
Apple Device Management Modes

Supervised devices

Devices purchased directly from Apple or its authorized resellers and carriers and deployed using the DEP—Device Enrollment Program. The organization completely controls the settings on the device. Ideal for a fully managed device mode of operation.

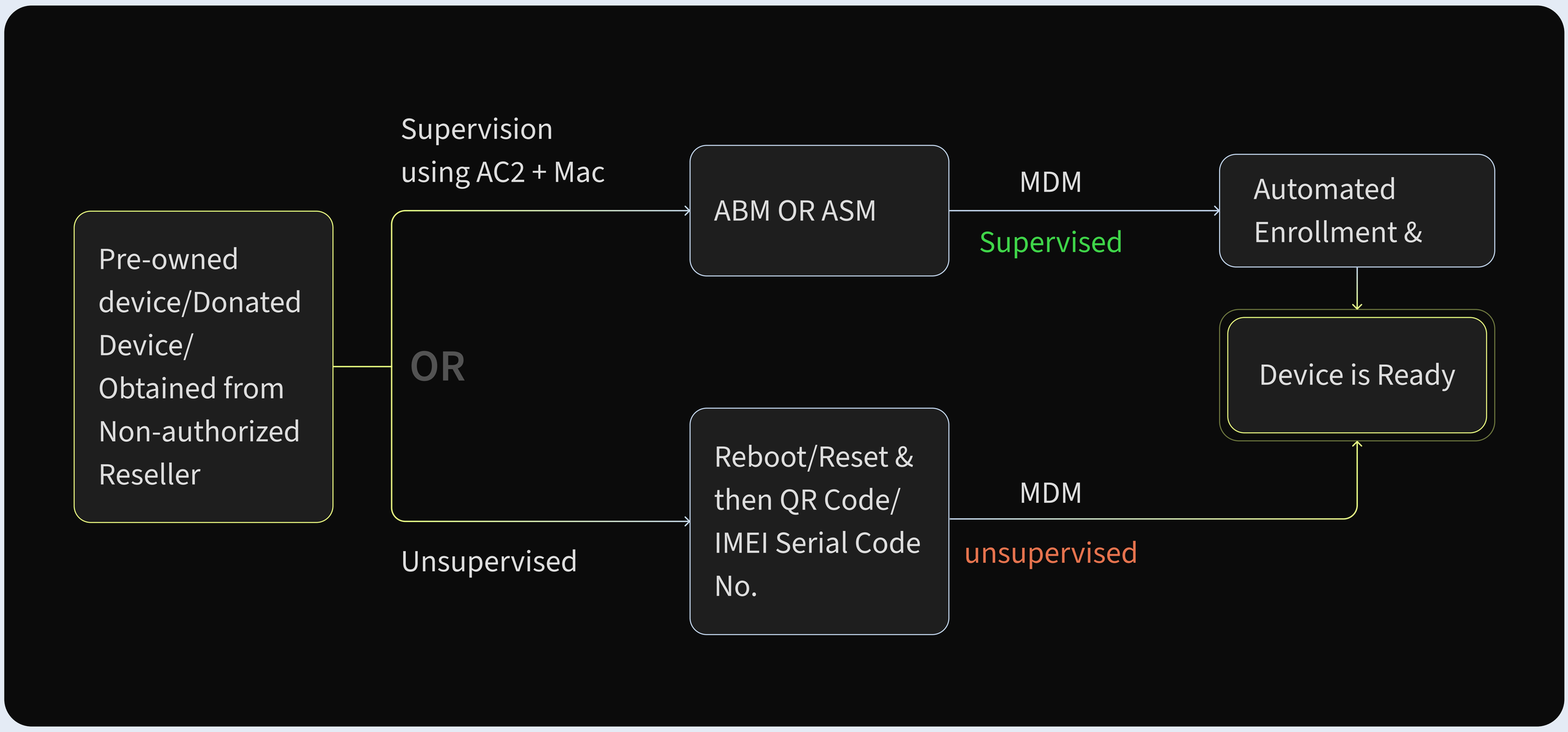
Mac computers are also supervised if they:

- Are running on macOS 11 or later and are added to DEP
- Are upgraded to macOS 11 or later, and the enrollment in MDM was approved by a local administrator account



Unsupervised devices

Device owned by the organization but is not enrolled into DEP/ Apple Business Manager. The organization can push applications and other settings but cannot have complete control over the device. Ideal for corporate-owned personally-enabled (COPE) device mode of operation.



Apple Device Management: Important Concepts

Apple Configurator 2

Apple Configurator 2 is a macOS application developed by Apple which allows organizations to configure, manage, and deploy multiple iOS and macOS devices simultaneously. It is a powerful tool for organizations that must manage and deploy a significant number of Apple devices. Apple Configurator 2 provides a way to customize devices, enforce security measures, and streamline the deployment process to ensure devices are ready for productive use in various institutional settings where device customization and management are essential.

From an MDM perspective, it’s most important for supervising unsupervised devices.

APNs

APN stands for Apple Push Notification. It’s a cloud-based service that allows app developers to send push notifications to users’ iOS, iPadOS, watchOS, and macOS devices. APN acts as the intermediary between the app server and the user device. When an app wants to send a push notification, it communicates with APNs, which then deliver the notification to the intended device. This allows apps to engage users, provide updates, or alert them about new content, events, messages, or any other relevant information.

APN also handles the security and encryption aspects of push notifications, ensuring the data being sent is secure and private. It’s a crucial part of the Apple ecosystem that enables real-time communication between apps and users, enhancing user engagement and app functionality.

Apple ID

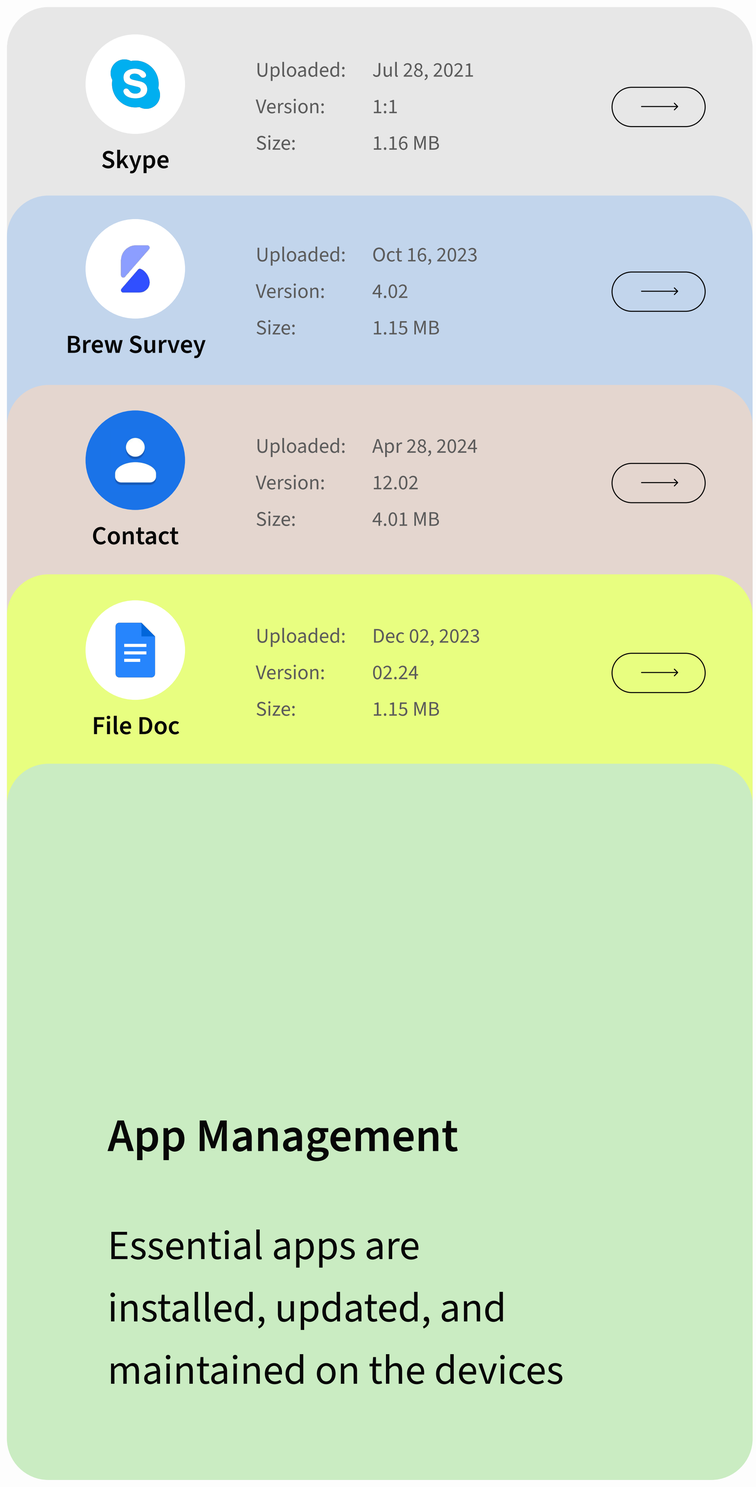
An Apple ID is a user’s key to accessing many Apple services. It is tied to an individual and allows them to purchase apps, store files in iCloud, sync data across devices, and use various Apple features. An Apple ID typically includes the user’s email address and password. While personal Apple IDs are often associated with users’ private email addresses, they can also be used for professional purposes, depending on individual preferences.

Managed Apple ID

A Managed Apple ID is a type of Apple ID created and managed by an organization, such as a business, educational institution, or government agency. Managed Apple IDs offer a range of advantages, including centralized control for organizations. They enable tailored configurations, app distribution, and security settings. With managed IDs, institutions can maintain data privacy, simplify user management, and create a cohesive ecosystem across devices, enhancing efficiency and security in various deployments.

Apple Device Lifecycle Management

The Device Lifecycle Management framework for Apple comprises the following components, each ensuring the security, integrity, and reliability of using Apple devices in an enterprise environment.



Inventory Monitoring

Devices are monitored for performance and compliance

App Management

Essential apps are installed, updated, and maintained on the devices

Deployment

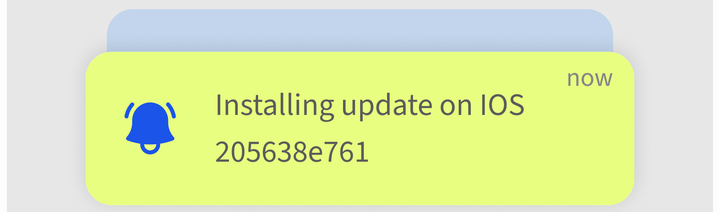
Devices are purchased and shipped to users

Policy Configuration

Devices are equipped with the right usage and security policies

Security

Security protocols are enforced as per organizational needs



Maintenance

Devices are troubleshot, updated, and retired

Scalefusion

Scalefusion Apple Device Management: An Overview

Scalefusion Apple Device Management is essential for IT administrators overseeing Apple devices in enterprise environments. Its user-friendly interface simplifies device management without detailed feature discussions. Ensuring smooth operations and optimal security, this versatile platform streamlines any security oversight.

Scalefusion is an indispensable tool for organizations that want to make the most of their Apple devices, providing a straightforward solution for efficient and secure device management. It stands out for its simplicity and effectiveness in meeting diverse administrative needs, contributing to enhanced organizational efficiency and security.

Apple Device Enrollment and Provisioning

Automated Device Enrollment

One of the best practices for deploying and managing a large number of Apple devices within an organization is automated device enrollment, which is available for supervised Apple devices. Only the devices purchased through Apple, its authorized reseller, or carrier are automatically added to the Apple DEP. For devices obtained from other procurement channels, supervision needs to be done manually. Once supervised, the devices are added first into the Apple Business or School Manager portal. After this, Scalefusion can take over for additional configuration and control.

Organizations can ensure a seamless out-of-the-box enrollment experience for Apple devices via automated device enrollment.

Ideal for: Company-owned devices

Manual Device Enrollment

For devices that cannot be supervised, either due to the mode of purchase or due to the nature of ownership (pre-owned/donated/ employee-owned), device enrollment cannot be automated. When a device is manually enrolled, a user can remove management from the device at a time.

The devices must be set up manually using various manual enrollment methods.

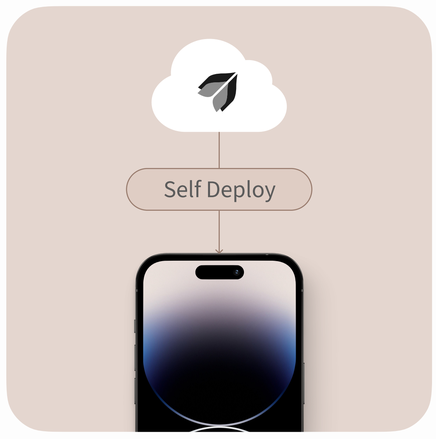
Ideal for: Company-owned devices that are not supervised, employee-owned devices

QR-code based enrollment

IMEI/serial#-based enrollment

Enrollment via SSO

Enrollment via browser



Enrollment via directory services

User-initiated Device Enrollment

Users can enroll their personal Apple devices on the Scalefusion platform using Managed Apple IDs. The organization’s policy settings can be installed on the device, initiating a data separation on devices. While the work and personal data are segregated, policies restricting data transfer between personal and managed apps can be controlled. Since Apple Business Manager’s policies still drive the device configuration, VPP is available.

Ideal for: Employee-owned devices

Policy Configuration via Device Profiles

Device profiles offer a convenient method to bundle a shared set of policies before deploying them across multiple devices. Any modifications administrators make within the device profile automatically reflect on all devices assigned to that profile.

For effective Apple device management, Scalefusion makes it mandatory to have at least one device profile to apply necessary policies. IT administrators have the flexibility to create numerous device profiles, aligning them with the organization's structure. These policies encompass comprehensive configurations that govern the usage and security parameters of Apple devices. Once enrolled, Apple devices can be grouped and subgrouped based on their usage, deployment scenario, and use case, and appropriate policies can be applied. Exchange and email settings, as well as parental control for macOS, can be configured and applied via device profiles.

Apple App Deployment and Management

While diverse methods and tools are available for deploying and managing applications on Apple devices in an enterprise, Apple’s very own VPP (Volume Purchase Program) stands out for bulk app purchases and app distribution.

Here are different ways to distribute, publish, and manage apps on Apple devices used within the enterprise environment:

Deploy VPP Applications

For organizations enrolled in the Apple VPP, Scalefusion streamlines the distribution of VPP applications. The Volume Purchase Program enables silent installations without user interaction, eliminating the need to sign in to an iTunes account on the device.

Deploy iTunes Applications

Search and deploy iTunes Applications on Apple devices. You can remotely install, uninstall, or update applications.

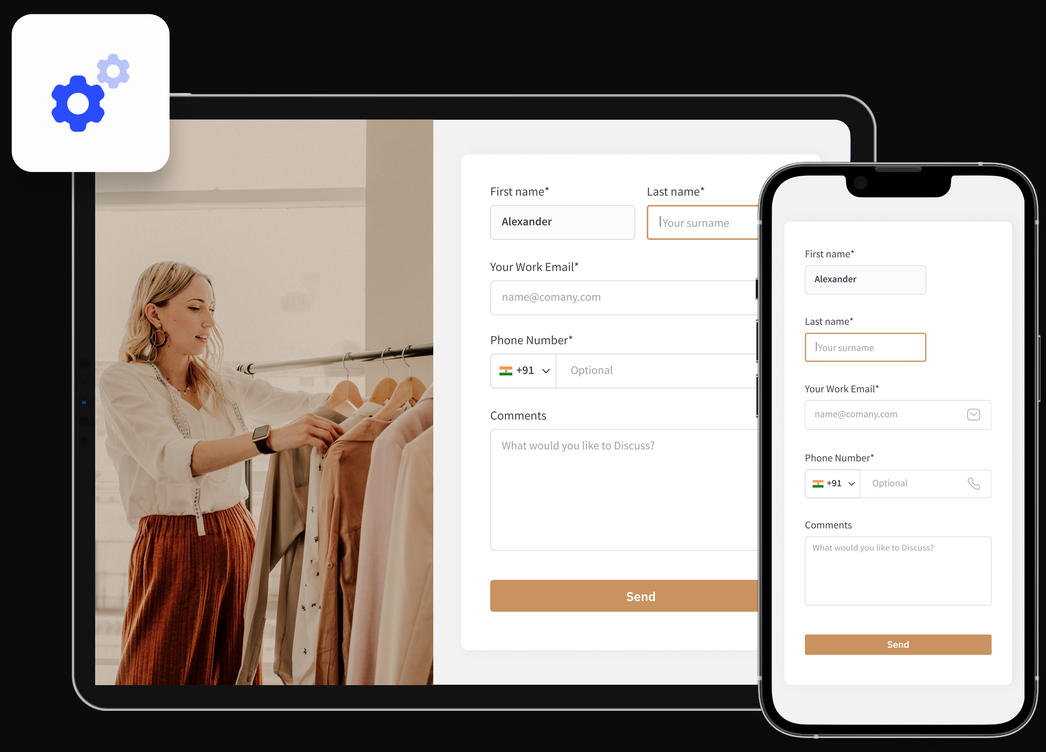
Deploy Enterprise or Custom Applications

When dealing with in-house applications, Scalefusion facilitates remote installation of native apps on Apple devices. Either upload the IPA file to our servers or, if self-hosted, upload the plist file (iOS), PKG, or DMG files (macOS) and install it via the Scalefusion dashboard.

iOS Device Management Modes

Single-App Kiosk Mode

For supervised iOS devices deployed for kiosk usage, setting one application to run becomes important. Scalefusion extends a device management mode where only one application can be set to run continuously, known as single-app mode.



Autonomous Single-App Kiosk Mode

While single-app mode offers the flexibility to restrict the device to a single application, it may only be suitable for some situations. Instances such as time-limited assessments, surveys, or on-demand data collection may necessitate running applications in single-app mode for a specific duration and then exiting that mode.

Scalefusion MDM addresses such scenarios by introducing support for Autonomous Single App Mode (ASAM). This feature allows you to select a subset of permitted applications, empowering them to enter single-app mode as needed autonomously, providing greater adaptability to diverse usage requirements.

Compliance Alerts and Task Automation

Leveraging Scalefusion Workflows, IT administrators can automate repetitive tasks according to device groups and policy configurations. The Workflows feature empowers IT teams to streamline routine tasks, enabling pre-planned execution and minimizing the time dedicated to recurring device management responsibilities. These tasks may encompass security checks and compliance measures, safeguarding devices against potential threats efficiently.

Scripting

For macOS devices, Scalefusion simplifies device management for IT admins through its GPT-powered AI tool, AirThink AI. Using AirThink AI, IT admins can easily create custom scripts tailored to their unique requirements, streamlining the device inventory process. These scripts can be scheduled to run automatically at specified times, removing the necessity for manual intervention. IT admins can configure dynamic scripts based on devices or users, eliminating the requirement to create separate scripts for each. It helps enhance efficiency and minimize complexity.

Driving Apple Device Security

Essential Security Settings

IT admins can implement passcode policies, enhance security settings for browsers, control media sharing, manage connections to other Apple devices through AirDrop and Bluetooth, regulate iCloud and App Store access, and limit users from accessing the camera and taking screenshots.

Certificate Management

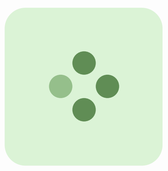
Scalefusion enables the installation of Digital Certificates that can be seamlessly integrated with enterprise Wi-Fi configurations. By implementing this feature, all managed devices that undergo Wi-Fi configuration are automatically equipped with the necessary certificate payload.

Lost Mode Support

IT admins can mark the device as lost, preventing further usage of the device even on restart. At the time of marking the device in lost mode, the admins can also specify a message to be displayed on the lock screen, a footnote message, and a phone number to appear on the device.

Data Security on BYO Devices

For Bring Your Own (BYO) devices, IT admins can restrict personal apps from accessing work apps and vice versa. Furthermore, admins can remotely lock stolen or misplaced devices and ensure the security of business data by initiating a remote wipe-off using the Scalefusion dashboard.



Custom Payload

Scalefusion offers support for Active Directory and LDAP payloads specifically for iOS devices. This enables IT admins to implement the mentioned policies on managed devices seamlessly. IT admins have the flexibility to configure custom payloads, allowing for the deployment of personalized components such as calendar and email settings, network configurations, certificates, and device restrictions. To simplify the process, IT admins can utilize the advanced XML editor to effortlessly push the Custom Payload directly onto managed profiles through the dashboard.

Lock Screen Settings

Scalefusion offers IT administrators the ability to control the lock screen settings on their managed iOS devices. IT admins have the power to allow or restrict notifications, passcode usage, and Siri access on the lock screen. They can also choose to allow or restrict users from utilizing Touch ID to unlock their devices. Once a setting is enabled, users will no longer have the ability to change it.

Driving Apple Device Security

mac OS

Leveraging macOS Security

macOS comes equipped with built-in volume encryption through FileVault, eliminating the need for additional software to secure folders, disks, or volumes on a Mac. FileVault, a Scalefusion offering, empowers IT admins to utilize macOS's Full Disk Encryption program, securing the disk and requiring a password for boot access, preventing unauthorized data access. This ensures data safety in case of device loss, with recovery possible even if users forget their password.

Scalefusion simplifies FileVault policy deployment across managed macOS devices, ensuring universal disk encryption. It also acts as an Escrow agent, securely storing and presenting recovery keys to IT admins when needed.

Additionally, Firewall and Gatekeeper settings can be configured for Macs to bolster the device and data security further.

Managing Content

Enterprise Content Files

Scalefusion Content Management allows IT admins to bypass iCloud and push files and content material directly to devices. Files are stored in an encrypted format on the disk; most file types can be viewed without leaving Scalefusion MDM.

Content Management allows IT to streamline access to business documents for the remote workforce and frontline employees. IT can push content files, videos, and presentations and enforce security policies to keep devices and data safe and secure.

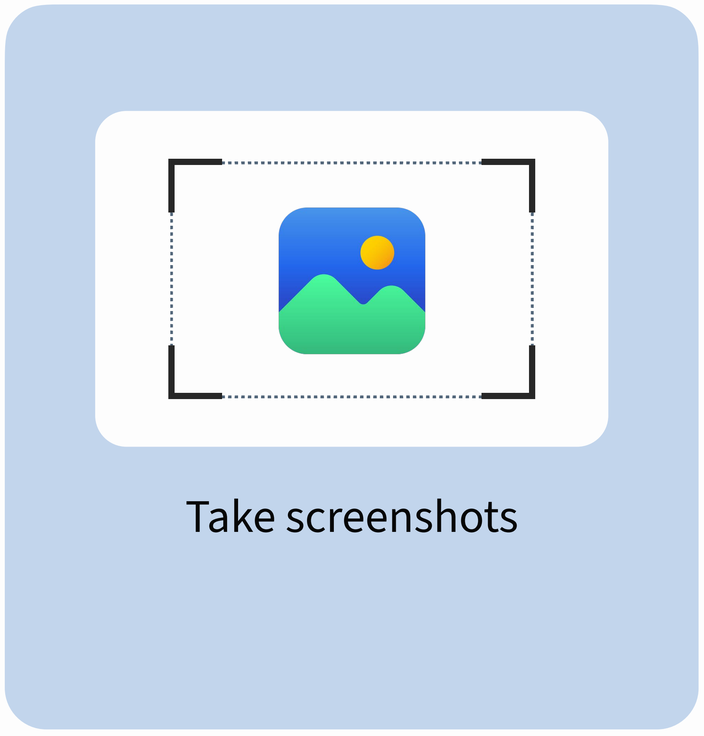
Web Content Filtering

Scalefusion provides IT administrators with the capability of managing the browsing experience on Apple devices via controls that regulate access to websites and apply content-filtering policies and restrictions. IT administrators can compile a master list of allowed websites, ensuring users can only access those specified sites and eliminating unnecessary browsing. Additionally, IT admins have the flexibility to block specific websites as needed.

With Scalefusion’s native browser ProSurf, IT teams can further apply browser restrictions to ensure safe browsing and reduce the risks of compromising data security and user privacy while browsing.

Remote Support

Scalefusion enables IT teams to reduce device downtime and promptly address device issues using the Remote Cast feature. IT administrators can easily cast screens of iPhones and iPads, enabling close monitoring and resolution of device-related issues. Furthermore, administrators can capture screenshots, record screen sessions, and conveniently raise tickets directly to their preferred ITSM tool, seamlessly integrated within the Scalefusion dashboard.



Take screenshots

Record screencast sessions

Raise context-aware ITSM tickets

Delivering OS Updates

Apple regularly introduces numerous features and essential bug fixes through OS updates. However, it can often trigger compatibility issues with apps, potentially leading to crashes or malfunctions post-update. Using Scalefusion MDM, IT admins can opt for a cautious approach, preferring a controlled rollout of OS updates following in-house testing on enterprise applications. Scalefusion enables deferring OS updates for a maximum delay of 90 days.

For macOS, IT admins can detect and patch the updates by major, minor, firmware, critical, or security and configuration. They choose the option to show the obsolete updates, which are updates that have been superseded.

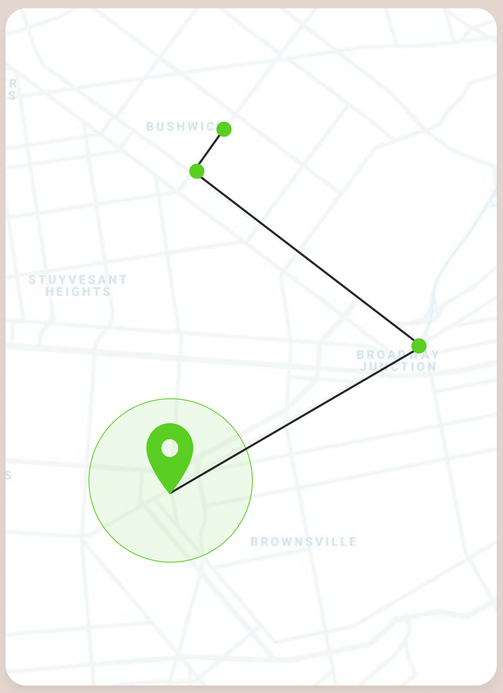
Device Inventory Monitoring and Reporting

Managing a vast device inventory across diverse geographical locations poses a challenge for enterprise IT. Tracking each device individually becomes strenuous. Scalefusion MDM provides a comprehensive 360-degree view of the entire device inventory, detailing individual device information like battery level, last seen, and OS version. IT administrators can effortlessly generate contextual reports for various device parameters, encompassing device availability and vital statistics such as battery history, available storage, and utilized storage. This ensures a streamlined approach to device management, making it easier for IT teams to stay informed and proactive across the entire inventory.

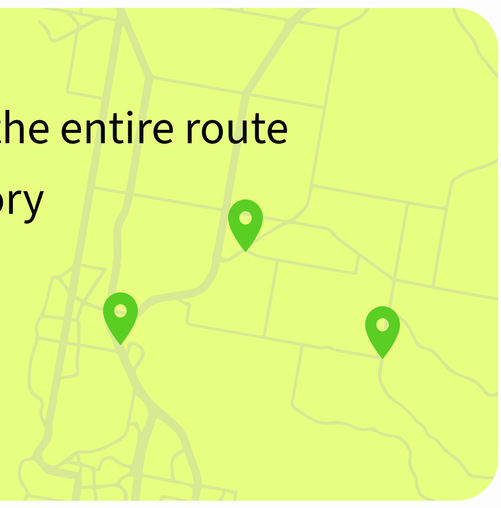
Location Tracking and Geofencing

Enhancing management, troubleshooting, and security for remote and frontline workers becomes possible through the utilization of Apple device location tracking. IT administrators can monitor device locations, access route histories, enforce a constant 'GPS ON' policy, and oversee multiple Apple devices concurrently. Additionally, administrators can establish an operational radius, enabling them to track movements in and out of designated areas to optimize the efficiency of frontline employee operations in the field.

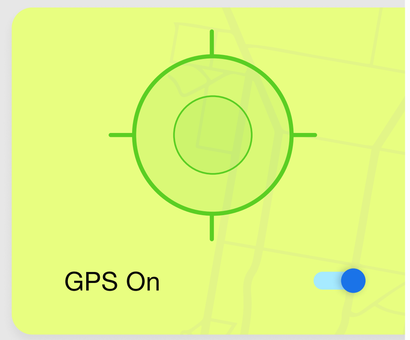
Track location accurately



Get the entire route history

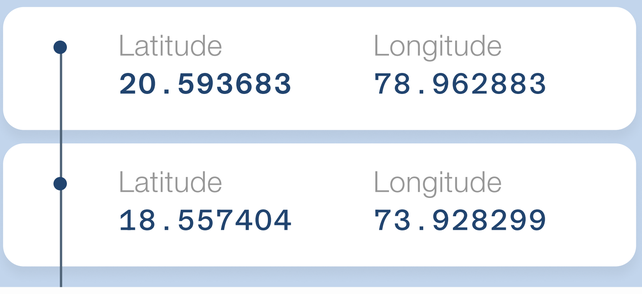


Enforce ‘GPS always ON’ on select devices

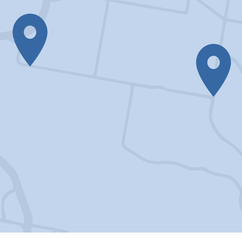


Track date, time, latitude & longitude

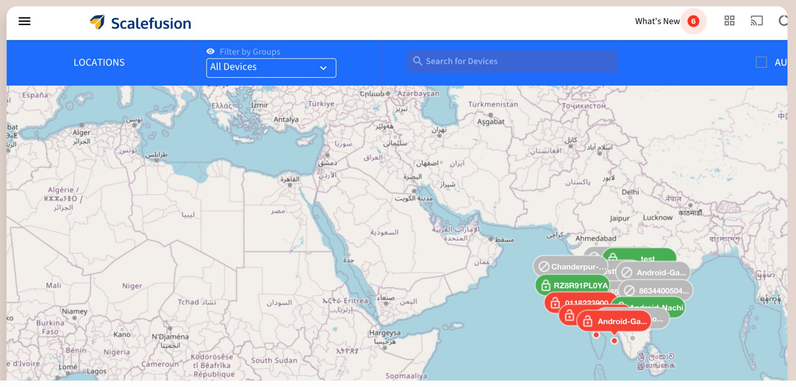
Obtain detailed location reports



Choose the frequency of collecting location and details



Simultaneously monitor multiple devices



Scalefusion OneIdP: UEM-Integrated Identity and Access Management

Enhance enterprise security and simplify user identity and access management with Scalefusion OneIdP. Integrate your existing directory or create your own on the .oneidp domain. Authenticate users and authorize access to devices, data, and applications seamlessly. Ensure robust identity governance with single sign-on (SSO) to enable your employees to access work apps, devices, and systems with a single set of credentials. Efficiently manage user lifecycles and extend access permissions based on device management status. You can also set access conditions for trusted locations, Wi-Fi networks, and IP addresses and deny access to work apps and devices via unidentified networks and locations.

Scalefusion

Case Study

Successful Deployment of Scalefusion Apple MDM for Wittichen Supply Company

Company Name:	Wittichen Supply
Industry:	Distribution
Platform:	iOS

Seeking to optimize its operations, Wittichen aimed to launch its Warehouse Management System (WMS) promptly and sought a powerful Mobile Device Management (MDM) solution to manage its iPod touch devices efficiently. Its goal was to streamline device setup, management, and deployment while overcoming the challenges of manual efforts and the integration of an in-house app.

In line with their WMS initiative, Wittichen's priority was securing, deploying, and managing its iPod Touch devices across 25 remote locations. The organization's significant challenge lay in the excessive man-hours required for device provisioning, security, and management, along with the integration of an in-house app for bin location maintenance and inventory cycle counting. The company sought an MDM solution that could alleviate these hurdles and ensure a seamless implementation of their WMS.

Leveraging Scalefusion as their chosen solution, Wittichen Supply Company successfully tackled its Apple device management challenges while experiencing a range of impactful benefits. The user-friendly setup and intuitive interface of Scalefusion facilitated an effortless device management experience for Wittichen. This led to streamlined device onboarding and swift configurations, significantly reducing the number of support calls related to misconfigurations and diminishing the burden of manual efforts.

Using Scalefusion's seamless deployment capabilities allowed Wittichen to effortlessly manage and configure 50 iPod Touch devices distributed across 25 remote locations. This translated to a substantial increase in operational efficiency and a notable enhancement in employee productivity.

With Scalefusion's robust security features, Wittichen experienced heightened device and data security, bolstering its overall IT infrastructure. Additionally, Scalefusion's efficiency contributed to Wittichen's WMS being operational sooner than anticipated, resulting in a faster return on investment and an accelerated realization of operational improvements.

Editor’s Note

Navigating the intricate world of Apple device management is imperative for enterprises choosing Apple devices. We hope this e-book offers a blueprint for seamless Apple device deployment, configuration, and enhanced data security.

To witness this e-book in action, you can get started with your device management journey by engaging with our Apple experts. Schedule a demo or reach out to our sales team now to catalyze efficiency and maximize ROI from using Apple devices for your business. Your next step begins with a click—contact our sales team and redefine your enterprise mobility.

Scalefusion

Seamlessly Manage Your Apple Devices with Scalefusion

Know someone who might benefit from this Ebook?

Book a Demo | Sign Up for Free | Share it across!