Apple at Work

Deployment and Management

Simple to deploy. At any scale.

Apple makes it easy for IT teams to administer devices, manage their configuration, distribute apps and content, and secure corporate data. With Apple Business Manager, devices can be distributed directly to employees and used right out of the box, all without manual configuration. And with flexible deployment models across all Apple platforms, IT can get employees up and running faster than ever with the best tools for the job.

Management made easy
Apple devices have a built-in mobile device management (MDM) framework, making it easy for IT to deploy devices, distribute apps and books, configure settings, and ensure the security of each device. Paired with a third-party MDM tool, IT teams can remotely manage and update devices over the air. And if devices ever go missing, IT teams can even remotely and securely erase them.

MDM supports configuration for apps, accounts, and data on each device. This includes integrated features such as password and policy enforcement. Controls remain transparent to employees while ensuring their personal information stays private. And IT maintains necessary oversight without disrupting the productivity employees need to succeed.

Whether a business uses a cloud-based or on-premise server, MDM solutions are available from a wide range of vendors with a variety of features and pricing for ultimate flexibility. And each solution utilizes the Apple management framework in iOS, iPadOS, tvOS, and macOS to manage features and settings for each platform.

Zero-touch deployment
Apple Business Manager is a web-based portal for IT administrators to deploy iPhone, iPad, iPod touch, Apple TV, and Mac, all from one place. Working seamlessly with a mobile device management solution, Apple Business Manager makes it easy to automate device deployment, purchase apps and distribute content, and create Managed Apple IDs for employees.

With Apple Business Manager, every iPhone, iPad, and Mac can be set up and configured automatically—eliminating the need for IT teams to handle each device individually. IT can also purchase and distribute apps for employees and enable employees to use Apple services with a Managed Apple ID.

Flexible deployment models

iOS, iPadOS, macOS, and tvOS support flexible security policies and configurations that are easy to enforce and manage. Through them, organizations can protect corporate information and ensure that employees meet enterprise requirements, even if they are using devices they've provided themselves—for example, as part of a bring your own device (BYOD) program.

With iOS 13, iPadOS 13.1, and macOS 10.15, Apple devices support a new user enrollment option specifically designed for BYOD programs. User enrollments provide more autonomy for users on their own devices, while increasing the security of enterprise data by storing it on a separate, cryptographically protected APFS volume. This provides a better balance of security, privacy, and user experience for BYOD programs.

IT teams can also choose to establish a higher level of control on organization-owned devices with supervision and device enrollment, which is available when an organization purchases devices from Apple or a participating Apple Authorized Reseller or carrier.

This enrollment method provides additional device management controls that are not available for other deployment models, including advanced security features and non-removable MDM. And IT can enforce or defer software updates across supervised devices to ensure compatibility with internal applications.

Organization-owned devices can be provided to a single user, shared among employees for common tasks, or configured as a purpose-built device for a specific use or for a single app.

Find out more about deployment and management.

apple.com/business/it

help.apple.com/deployment/macos

help.apple.com/deployment/ios

support.apple.com/guide/mdm