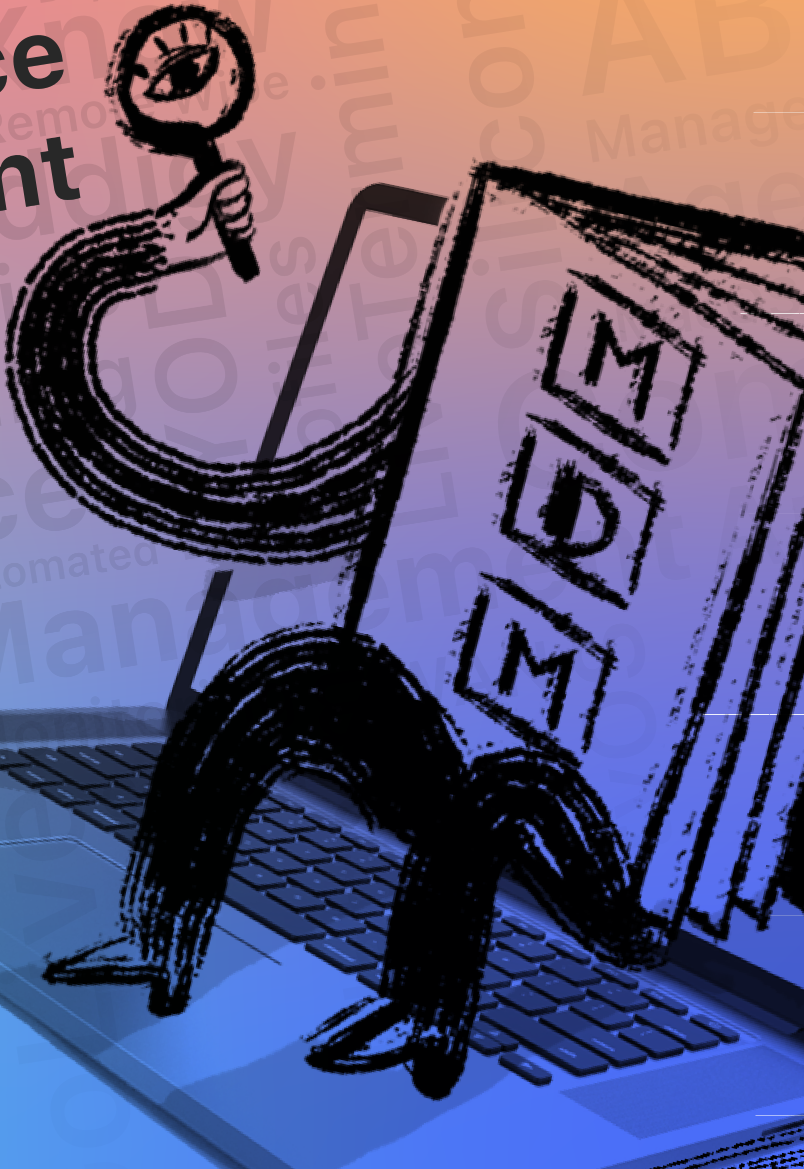
Addigy

ebook

The ABCs of Apple MDM:

Everything You Need to Know About Apple Device Management



Despite Windows being the dominant desktop operating system (OS) worldwide, Apple macOS has gained market share over the years, and Mac adoption in the enterprise continues to grow. Fifty-five percent of businesses are now Mac-friendly, according to a report published by Parallels.

Apple devices are connected to nearly every business's IT infrastructure in some way or another — and managing and monitoring them is vital to keeping employees productive and safeguarding sensitive corporate data from bad actors.

IT admins must be prepared to provide Apple users with the same level of device management as Windows users. In this eBook, you'll find definitions for all the terminology you'll need to know to start managing macOS, iOS, iPadOS, and tvOS devices in your managed networks.

Guide

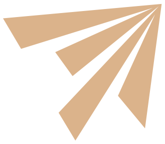
A

↘ Addigy Community

The Addigy Community is an arena of open-source device information queries (Device Facts) and scripts that Addigy users can leverage to create robust monitoring and remediation workflows. A managed third-party app catalog offers an array of custom solutions that can enhance servicing capabilities. The Community makes it possible for IT admins to network and grow their shared knowledge base.

↘ Addigy Identity

Addigy Identity simplifies users' authentication and onboarding at the macOS login window. With Addigy Identity, users can use the same authentication they use across your environment on their macOS systems as well. No extra configuration on the Identity provider side is necessary.



↘ Agent

The Addigy agent is a lightweight agent that runs on macOS devices. The Addigy agent is responsible for ensuring devices remain managed and healthy.

↘ AirDrop

AirDrop allows Apple users to transfer files to one another through close-range wireless communication.

↘ Apple Business Manager (ABM)

ABM enables automated device enrollment, giving organizations a fast, streamlined way to deploy corporate-owned Apple devices and enroll in MDM without physically touching or manually preparing each device.

↘ Apple Configurator

Apple Configurator enables IT admins to create MDM configuration profiles for Apple devices.

↘ Apple Device Management Platform

An Apple Device Management Platform allows IT professionals to securely and wirelessly configure Apple devices. They can also use the platform to wipe or lock devices remotely, monitor compliance with organizational policies, update software and device settings, and more. IT admins and MSPs use these platforms to manage Apple devices on their networks.

A
B
C
D
F
G
I
L
M
P
Q
R
S
T
U
X
Z

↘ Apple MDM Push Certificate

An Apple MDM Push Certificate is required for MDM vendors to manage Apple devices.

↘ Apple School Manager (ASM)

Apple School Manager enables IT admins to remotely enroll new devices into an inventory through Automated Device Enrollment and deploy shared software purchased through the App Store, via Apps and Books.

↘ Apple Silicon

Apple Silicon is the next generation processor line for Mac computers, replacing Intel chips. The first version, referred to as M1, is a 5nm 9-core System-on-a-Chip (SoC) integrated GPU.

↘ Apple T2 Security Chip

The Apple T2 Security Chip is Apple's second-generation, custom silicon for Mac. The chip offers a Mac several capabilities, including encrypted storage, secure boot capabilities, and enhanced image signal processing.

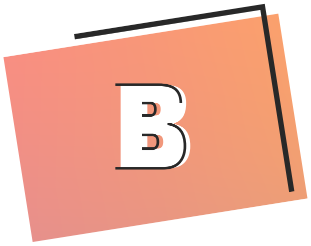
↘ Automagically

When something happens automatically and seems like magic.z

↘ Automated Device Enrollment

(formerly known as DEP – Device Enrollment Program)

Automated Device Enrollment is vital for IT admins looking to save time and effort when performing Apple device management tasks and deliver a truly zero touch deployment experience for users.



↘ Big Sur

Big Sur is the current major release of macOS. It's the successor to macOS Catalina.

↘ Bring Your Own Device (BYOD)

BYOD is an IT policy that allows employees to access corporate data, systems and networks through their personal devices instead of corporate-owned devices.

A
B
C
D
F
G
I
L
M
P
Q
R
S
T
U
X
Z

A
B
C
D
F
G
I
L
M
P
Q
R
S
T
U
X
Z

C

↘ Catalina

Catalina is a release of macOS; it's the successor to macOS Mojave.

↘ Configuration Profiles

IT admins with little to no experience dealing with Apple devices should first know that Apple makes it incredibly easy to set up devices in a variety of ways using MDM Configuration Profiles. Configuration Profiles contain device settings, custom app settings, user account information, and credentials that can be loaded onto any Apple device.

↘ Custom App Configuration

Custom App Configuration can save IT admins time, secure their fleets, and ensure that the Mac users on their networks are operating on machines that meet and stay compliant with security policies.

D

↘ Device Fact

Device facts will give IT admins even more power to monitor the current state of your fleet of devices and further leverage remediations when... devices are not properly secured. These new facts include being able to quickly determine the status of firmware security on Mac devices, passcode states on iOS devices, the type of enrollment methods for each device, and more.

F

↘ FileVault

FileVault is built-in disk encryption for macOS. Using Apple MDM, administrators are able to protect their fleet's hard drives, adding an extra layer of security to their data.

↘ Find My

Find My can help an end user locate a Mac computer, iPad, or iPhone using Bluetooth signals. If an Apple device with sensitive company data goes missing, the Find My app can quickly locate and secure the device, wherever it is. If the company uses an MDM solution to manage Apple devices, its IT team can deactivate or wipe enrolled devices remotely, even if a BYOD policy is in place.

G

↘ Gatekeeper

Gatekeeper enabled helps prevent users from installing or inadvertently executing malware in macOS devices.

↘ GoLive

GoLive has long been a core feature in the Addigy platform, providing IT admins with a single page to manage a singular device with ease and launch various remote control utilities such as Addigy Live Terminal, Splashtop, and Addigy Remote Control. GoLive also provides real-time device information such as Gatekeeper status, FileVault status, IP address, uptime, machine users, installed software, available updates, speed test results, and much more. GoLive is perfect for fixing one-off issues on an Apple device.

I

↘ iCloud

Allows end users to automatically back up their data and settings to the... cloud This stores everything from the organization of their home screen to their preferences within apps.

↘ Identity Lifecycle Management (ILM)

ILM refers to a system of software and business practices that manage individual access to devices, information, and identity.

↘ iOS

Apple's mobile operating system.

↘ iPadOS

A mobile operating system for Apple's iPad line of tablet computers.

L

↘ LiveDesktop

LiveDesktop allows an IT admin to create a secure, remote live session with an end user's Mac computer in just a few clicks.

↘ LiveTerminal

LiveTerminal allows an IT admin to securely and remotely connect to Mac computers via a command line.

A B C D F G I L M P Q R S T U X Z

M

↘ MacOS

The primary operating system for Mac computers.

↘ Managed Lost Mode

Managed Lost Mode remotely locks a device and shows the device's last known location.

↘ Mobile Device Management (MDM)

MDM is a process where IT admins protect corporate data by monitoring and managing employee devices. Many IT admins use a third-party solution or platform to implement policies that monitor and secure devices connecting to their systems and networks.

↘ Monitoring

Monitoring is checking on the performance of a device connected to a network.

↘ Monterey

macOS Monterey is the latest of Apple's operating systems for Mac. It's the successor to macOS Big Sur and due to arrive in the fall of 2021.

↘ Multi-factor Authentication (MFA)

An authentication method that requires a user to present two or more pieces of evidence to an authentication mechanism before granting access to an application or website.

P

↘ Policies

IT admins use MDM solutions to enforce desired configuration settings and security policies on devices.

↘ Privacy Preferences Policy Control (PPPC)

MDM allows administrators to grant or deny certain privacy permissions on macOS devices. PPPC permissions control access to disks, camera, mics, and more on individual devices.

↘ Public Software Catalog

Public Software Catalog is a collective list of maintained software titles the Addigy Community most commonly uses. Within 7-days of an update or patch becoming available,...

A
B
C
D
F
G
I
L
M
P
Q
R
S
T
U
X
Z

Addigy will package, verify, and update the title in the catalog. Deployment of titles is easy, with just a few clicks by an administrator.

Q

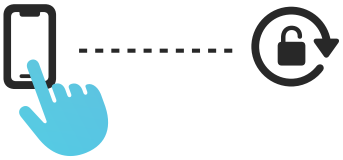
↘ Quality Assurance Standards

One of the main distinguishing factors for Apple device users is that all software applications must go through the Apple Store's rigorous evaluation process, ensuring that everything on the App Store meets Apple's quality assurance standards. For business users, this attention to device security and updates doesn't go unnoticed.

R

↘ Remote Lock

Remote Lock allows an IT admin to remotely lock a device.



↘ Remote Wipe

The remote wipe feature on an MDM solution allows an IT admin to erase data on a device that's been stolen or lost.

S

↘ Secure Enclave

A dedicated secure subsystem integrated into Apple's system on chips (SoCs).

↘ Self Service

Self Service, also known as MacManage, is a native Swift application designed to provide the Apple experience a device user expects. Self Service allows end users to install their own applications, request support, and get notifications for maintenance.

↘ System on a Chip (SoC)

An integrated circuit that integrates most components of a computer system. M1, Apple's first chip designed specifically for the Mac, is an example of a SoC.

T

↘ Touch ID

New Mac computers with Touch ID are **encrypted by default when you put a password on the device. Set it up, create an account, and the hardware inside the device** encrypts the data that's on it at rest.

↘ Trust Access

With Trust Access, an IT admin can **grant secure network access to devices enrolled in the company's MDM solution.** With an authenticated Trust Access certificate, end users can securely access resources without going through a new authentication process every time they return to that application or server.

↘ tvOS

Apple's OS for the Apple TV digital media player.

U

↘ User Authentication

A verification process in which someone who is attempting to access applications is who they claim to be.

↘ User Enrollment

A deployment option for personal devices that enter an organization through a BYOD program. While remote management capabilities are more limited in a device that goes through User Enrollment, IT admins still **retain certain key functions like applying user password settings and installing Wi-Fi security and SSID settings.** User Enrollment also creates a partition between a company and personal data, preventing information crossover.

X

↘ XProtect

XProtect is the anti-malware program that's been running under the hood of every Mac computer since the release of Mac OS X 10.6 Snow Leopard in 2009. This program is part of the security architecture of Apple computers. It helps flag potential malware before it's downloaded onto devices and alerts users to potential risks.

A B C D F G I L M P Q R S T U X Z

Z

↘ Zero-Day Support

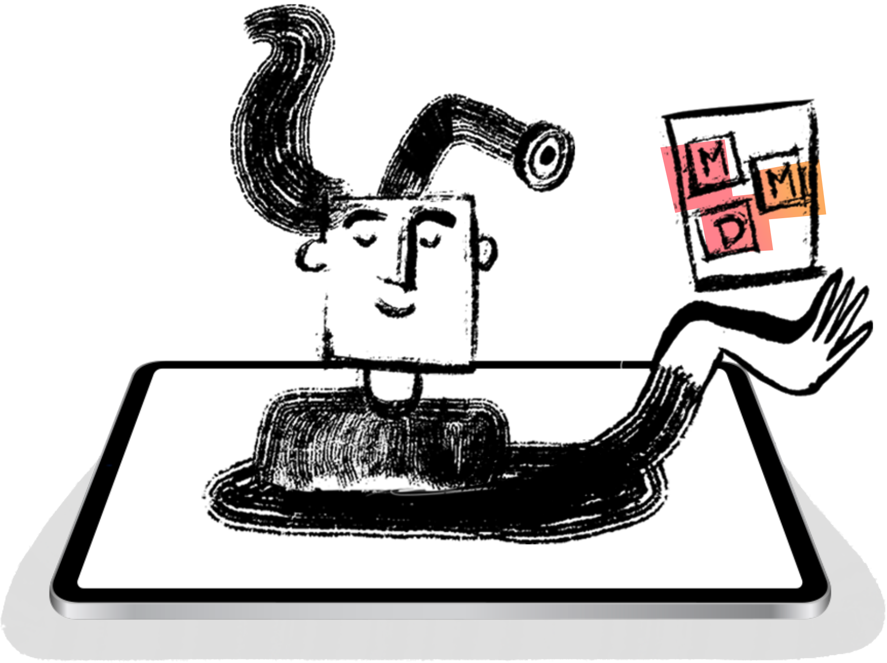
When a vendor's solution provides zero-day support, it supports devices when they become available.

Not having zero-day support could disrupt MDM workflows and leave an IT infrastructure vulnerable to cyberattacks.

↘ Zero-Touch Deployment

With Apple School Manager and Apple Business Manager, enrolled devices are tied to an IT admin's organization by their serial numbers, making it easy for admins to remotely support these devices from the first time they boot up and connect to the internet.

...



A
B
C
D
F
G
I
L
M
P
Q
R
S
T
U
X
Z

Summary

Ignoring Apple devices could prove to be disastrous for IT professionals in the long run. Today, there are simply too many end users using these devices, many of which are unsupported, for work-related purposes. Addigy can help.

Addigy is the most powerful Apple Device Management platform, enabling MSPs and IT teams to effortlessly manage macOS, iOS, iPadOS and tvOS devices. Our cloud-based multi-tenant offering makes managing multiple environments a breeze – whether you're managing 100 devices or 10,000.

Addigy simplifies Apple device management, allowing you to automate onboarding and deployment while ensuring your fleet is secure. Addigy lets you manage devices in real-time, launch remote control access, initiate a LiveTerminal session, remotely monitor devices and automatically respond to alerts and remediate issues, and so much more. Visit addigy.com/demo to request a free demo.

addigy.com | © 2021 Addigy. All Rights Reserved.

Addigy