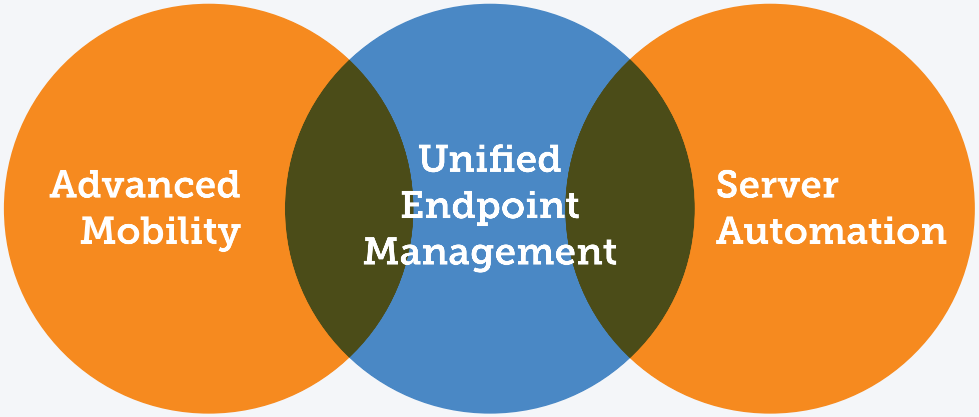
BETTER TOGETHER

Managing Your Apple Devices as an Ecosystem

Today, you'd be hard-pressed to find someone who doesn't use multiple devices for work. Users have phones, tablets and computers to stay more connected and productive than ever. Many organizations choose to manage these devices in order to ensure they are set up correctly, provide access to corporate resources, and ultimately ensure security and compliance. The question is how do you manage the various platforms you have in your environment?

Some organizations have separate teams purchasing and managing mobile devices (e.g., a Telecom team) and another (IT team) purchasing and managing computers — resulting in multiple management tools within the same organization. However, Microsoft, Google and Apple are all pushing for a unique experience across each of their desktop and mobile platforms. This puts the multiple management tools model at odds with the interconnected platform vision, which has spawned the notion of "unified endpoint management" (UEM), where all devices are managed by a single management tool. This might sound great, but begs the question, "what is universal across Microsoft, Apple and Google?"



The reality is desktop operating systems — Windows, macOS and Chrome OS — have little in common. All have a unique workflow to provision, encrypt, deploy, secure, update and support devices. The same "uniqueness" also applies to the mobile platforms: iOS, Windows Mobile and Android. This is where UEM fails; no one management tool is designed to support everything.

So, you as an organization have to choose:

- ☑ **Manage your devices by platform type (i.e., desktop or mobile).**
- ☑ **Attempt to manage your devices with a unified tool.**
- ☑ **Manage your devices by ecosystem (Apple, Microsoft, Google).**

This e-book breaks down these choices facing you and your IT staff, and how it impacts you and your users.

1 Approaching Management Through the Lens of an Ecosystem.

Defining Device Management Models

Let's start by examining the various types of device management models and what they mean.

Whether you manage your devices separately by device type or attempt to put them all in one unified tool, you are forced to support the lowest common denominator. The lack of commonalities across various device types coupled with unique and frequent upgrade cycles, means there is no one-size-fits-all approach to device management. The reality is that unified management tools aren't designed to support every device type and platform, and organizations are often relegated to a "master of none" toolset.

Option 1: Devices Managed by Type

Device Type	Apple	Microsoft	Google	Management
Computer	macOS	Windows	Chrome OS	Client Management
Mobile	iOS	Windows Mobile	Android	EMM/MDM Tool
TV	tvOS	—	Chrome OS	EMM/MDM Tool

Option 2: Devices Managed by a Single Tool

Device Type	Apple	Microsoft	Google	Management
Computer	macOS	Windows	Chrome OS	UEM
Mobile	iOS	Windows Mobile	Android	
TV	tvOS	—	Chrome OS	

Instead of focusing on the individual devices you manage, what happens when you focus on the ecosystems (i.e., platform or brand) you manage? When you organize vertically by ecosystem, you start to see commonalities.

Windows and Windows Mobile have commonalities, and Microsoft provides first-party management tools with Intune and SCCM. Chrome OS and Android are moving closer together, and both can be managed by Google's native management tools in G Suite. And, because Apple is known for creating an integrated IT and user experience across all of its device types, we will use it to best illustrate the value of managing devices by ecosystem.

Apple's operating systems are converging, and by design, are part of their own ecosystem. iOS and macOS share a common management framework, and this has been extended to tvOS. To get the most out of the Apple ecosystem, these devices can be managed together with a purpose-built management tool, such as Jamf.

Option 3: Devices Managed by Ecosystem

Option 3	Apple	Microsoft	Google
Desktop	macOS	Windows	Chrome OS
Mobile	iOS	Windows Mobile	Android
TV	tvOS	—	Chrome OS
Management Tool	Jamf	Intune/SCCM	G Suite Management

Efficiency Gains for IT

By choosing to manage devices by ecosystem rather than device type or unified tool, you optimize all management tasks without compromising their functional benefits. Let's explore the different ecosystem workflows for Apple, Microsoft and Google.

			Microsoft		Google	
	mac OS	iOS		Windows 10 Mobile		
Provisioning	Device Enrollment Program		Dynamic Provisioning via Azure AD		Manual Enrollment into G Suite	No Device Enrollment Program equivalent
Encryption	FileVault	Enabled with password	BitLocker		Encryption via cloud storage	Built-in encryption on newer devices, turned off by default
Management Framework	MDM via Apple Push Notification Service		SCCM + MDM via Windows Push Notification Service	MDM via Windows Push Notification Service	Chrome Management	MDM via Google push notifications
Settings Management	Configuration profiles		Group policy object	Configuration policy	Chrome Policy	Android (formerly Android for Work)
Software Licensing	Volume Purchase Program		Windows Store for Business		Chrome Web Store	Google Play Volume Purchase (US & Canada only)

As you can see, these ecosystem workflow differences require different ways to provision devices, apply settings and deploy software. And, this lack of universal workflows alone should be argument enough that unified endpoint management is not ideal for managing multiple ecosystems.

However, if you approach management by ecosystem, you can achieve the best of both worlds — efficient management and security for your IT team balanced with a delightful user experience. Let's look at how Apple's ecosystem shares management commonalities across its operating systems — macOS, iOS and tvOS.

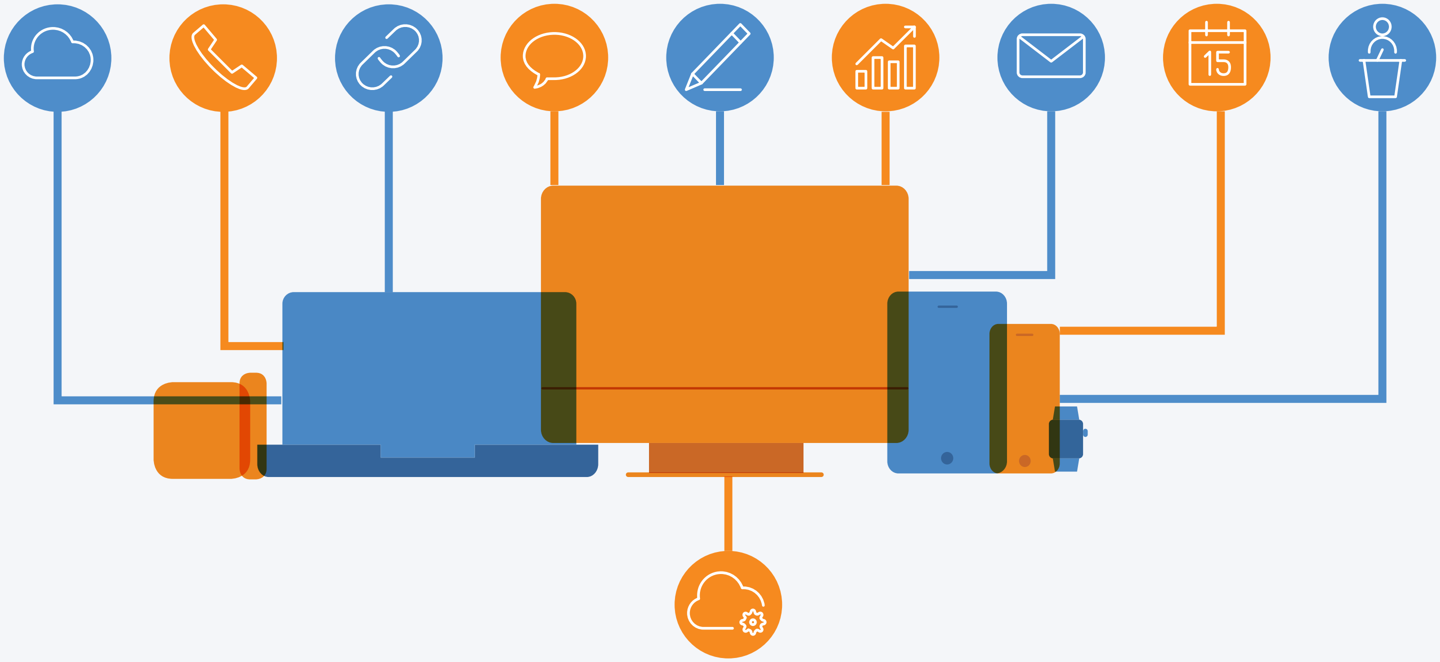
2 Starting With the Apple Ecosystem

Why Apple First: The Interconnected Experience

Apple continues to build an interconnected ecosystem. In fact, they are the leading example of a blended desktop and mobile experience. Apple embraces a consistent user experience across their entire ecosystem. iMessage, FaceTime and other Continuity features work across all Apple devices. For example, users can unlock their Mac from their Apple Watch, create a presentation on their Mac and continue editing the presentation on their iPad, then share the presentation wirelessly to their Apple TV. And, with enhancements to virtual personal assistants, like Siri, the Apple ecosystem is expected to become even more interconnected through voice commands.

The “seamlessness” of the Apple ecosystem creates an incredible user experience, and it also caters to IT in an enterprise setting. Apple has specific enterprise programs to help streamline deployment and create an out-of-box experience for users. Apple’s Device Enrollment Program (DEP) and Volume Purchase Program (VPP), combined with mobile device management (MDM), result in consistent management of Mac, iPad, iPhone and Apple TV devices. These management features are exclusive to the Apple ecosystem and need to be properly supported in a management tool.

Apple Ecosystem for End User



Apple Ecosystem for IT

The Apple Ecosystem Management Framework

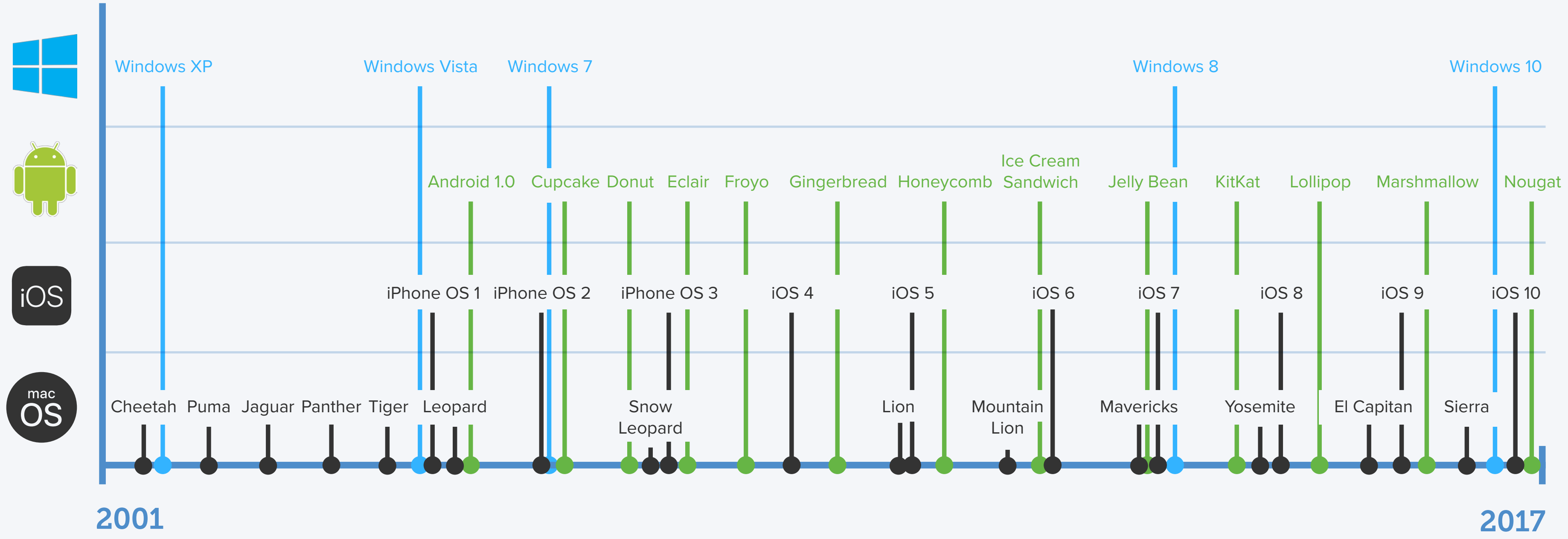
MDM is Apple's built-in management framework that allows IT to configure, secure and manage Mac, iOS and Apple TV devices. Based on configuration profiles, MDM allows IT to more easily and consistently build and deploy Apple devices to users. Configuration profiles tell the devices what settings to turn on or off, and how to behave.

Some profiles can be the same across all devices, meaning you can configure one Wi-Fi or email and deploy it to all of a user's Apple devices. Security settings and restrictions are also applied by profiles and allow you to turn off the camera, enforce a passcode, turn on encryption, restrict iCloud and block specific apps. These profiles all ensure consistent device settings and security across devices.

Keeping Pace with Ongoing Updates

Ensuring a seamless experience for your users is an ongoing process — one that includes continually supporting new features and capabilities on your devices. Apple, like other technology providers, have regular upgrade cycles for their operating systems, so it is critical from both a security and functionality standpoint to ensure your users can upgrade to the latest releases.

With every new release, macOS, iOS and tvOS become more integrated with each other, and Apple users are quick to upgrade to the latest features. Why? The upgrade process is simple and they want to take advantage of the latest capabilities. In fact, statistics show that 86 precent of iPhone and iPad users are on iOS 10, compared to only 7 percent who are on the latest Android operating system. However, because Apple and Microsoft upgrades are delivered differently, they need to be managed differently.



While new operating systems and features enhance the user experience, users only benefit from the latest and greatest if and when all of their Apple devices are fully supported. If you subscribe to the UEM model, you are reliant on your vendor's ability to support multiple and competing maintenance cycles. Per the graphic, UEM providers have a lofty set of expectations to meet, and often choose (or are forced by resource or time constraints) to cater to the lowest common denominator. As a result, support for the latest platform updates are often delayed by months, quarters, or worse, never supported.

In addition to diminishing the user experience, when UEM software can't immediately adopt the latest platform updates, organizations using those tools are exposed to security vulnerabilities and broken workflows. The best way to keep users productive and your organization protected is through a purpose-built solution that immediately supports updates to each platform's specific ecosystem. This isn't a luxury, but rather a baseline requirement for successfully and securely managing your devices.

Apple Hardware Purchasing Under One Roof

Apple's centralized hardware enrollment portal, known as the Device Enrollment Program (DEP), enables zero-touch deployment, meaning IT can pre-configure devices and allow users to simply unwrap their new device, turn it on, and go through the Setup Assistant process. Their device is automatically enrolled into management and ready for use. This Apple-exclusive deployment and enrollment process is available for macOS, iOS and tvOS. Managing this process with a tool dedicated to the entire Apple ecosystem is simple and avoids the need to implement the multiple, redundant workflows if macOS, iOS and tvOS devices are managed by different tools.

Things get messy fast if an organization uses different tools to manage different Apple device types. While DEP can support multiple MDM servers, IT administrators are then required to manually separate orders in the DEP portal and assign Mac and iOS devices to the corresponding MDM server. The DEP portal does not show a list of purchased devices, so the process of assigning devices requires IT to enter the (lengthy) serial number or order number in the DEP portal, which is tedious and prone to errors. If assignment of devices to an MDM isn't completed in the DEP portal before the device is delivered to the user, then the device isn't properly setup.

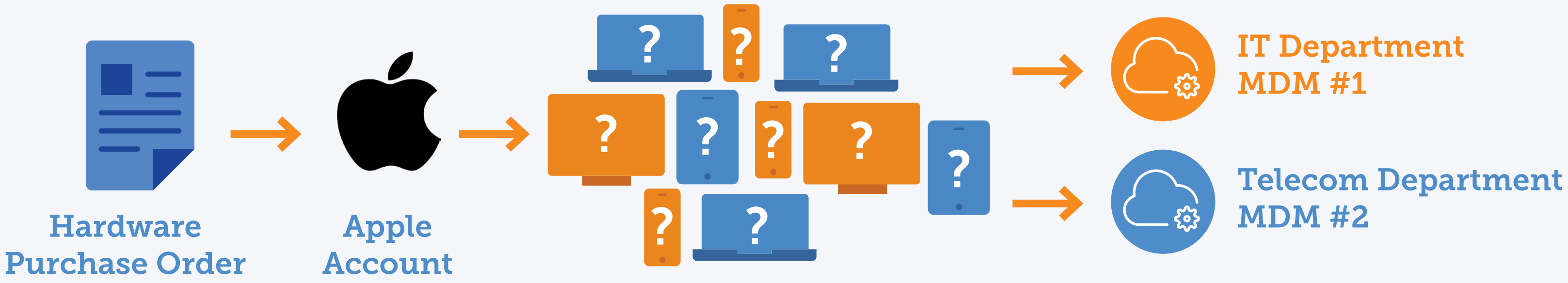
Organizations can eliminate the need to place separate orders with separate account numbers for Mac, iPad, iPhone and Apple TV devices by keeping your DEP account linked to a single ecosystem-specific MDM solution. This equates to an automated management experience for IT.

What is DEP and how did we get here?

Imaging has been the deployment standard for years. However, mobile devices were never built for imaging. Beginning with mobile, Apple created a more modular, modern deployment approach — the Device Enrollment Program.

Taking a cue from iOS, macOS is also moving away from imaging. The factory-installed version of macOS that comes pre-installed on your new Mac is already free from adware or add-on software, which means IT admins can simply build on top of the pre-installed OS with MDM.

DEP with multiple MDM vendors



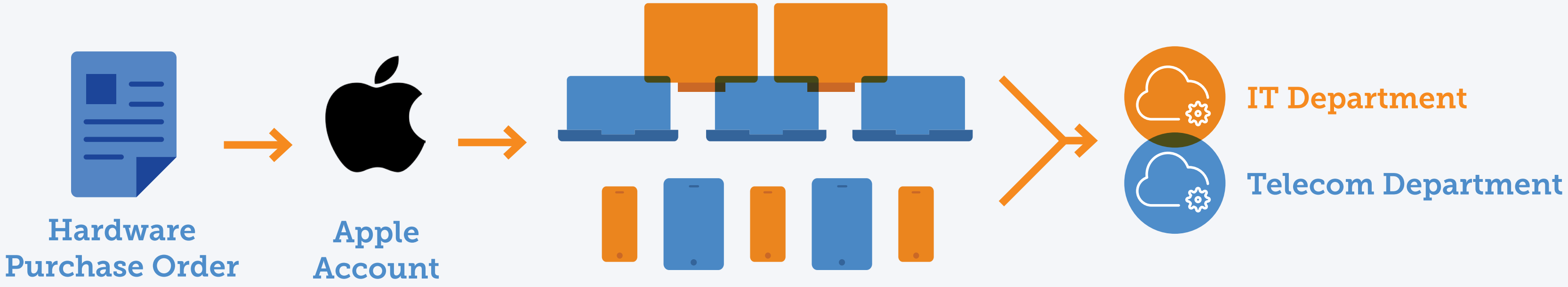
Hardware Purchase Order

Apple Account

IT Department MDM #1

Telecom Department MDM #2

DEP with 1 MDM vendor

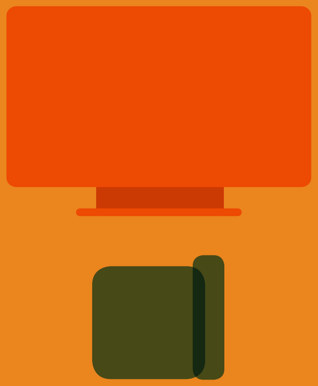


Hardware Purchase Order

Apple Account

IT Department

Telecom Department



What’s new with Apple TV?

Apple TV can now also be deployed and configured automatically via DEP and your MDM. If you’re wondering which side of the aisle would manage tvOS — desktop or mobile — it really doesn’t matter, as long as all of your Apple management is under one solution.

Apple Software Licensing and App Purchasing Under One Roof

What sets Apple apart from others on the market is its ecosystem of apps. Apps are core to enabling user productivity, and Apple has a rich App Store. However, downloading apps from the App Store traditionally required an Apple ID. This all changed with the Volume Purchase Program (VPP).

VPP is a streamlined method for purchasing and managing apps in bulk, and it's the only method to distribute App Store apps. Leveraging a single ecosystem management solution streamlines deployment and management of these apps. Furthermore, keeping purchasing, assignment and distribution all linked to a single ecosystem management solution reduces complexity and avoids potential loss of data.

Why should you use VPP with a single Apple management solution?

Purchase IT purchases all Apple apps in one central location regardless of the device / operating system.

Assign App assignments are easier with a single VPP account because all available purchases are linked to one central location versus multiple VPP accounts. Apple IDs are not required for device-based assignments.

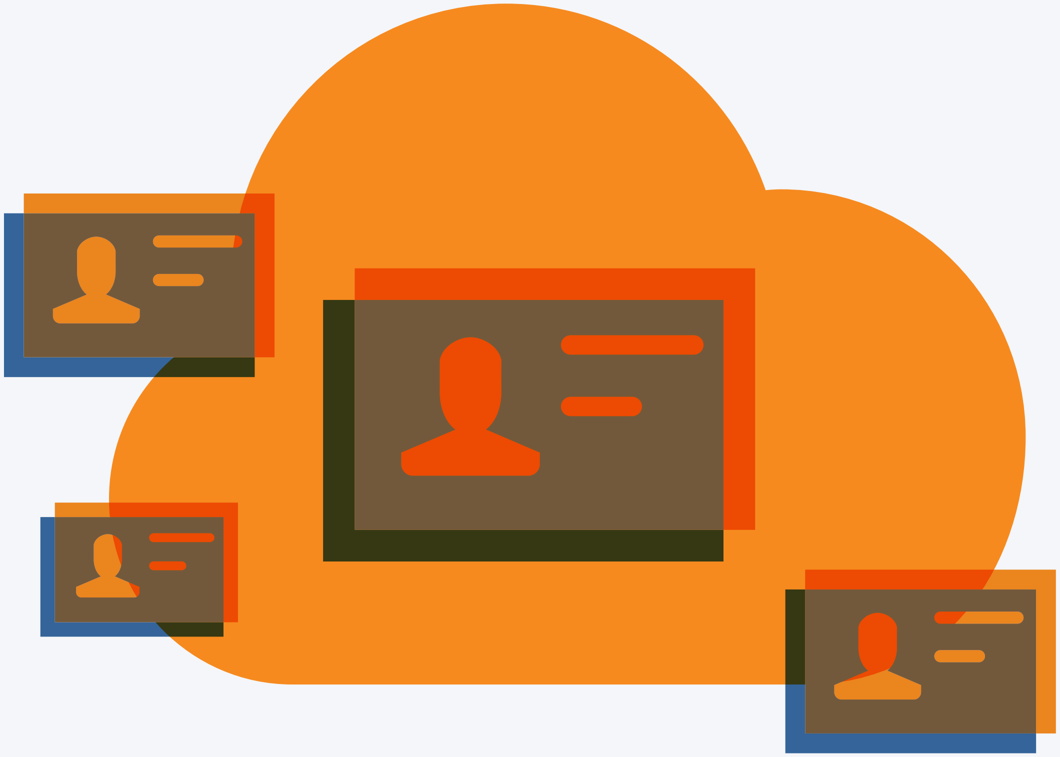
Distribute VPP apps are all listed in your single MDM and ready to be deployed to users.

Renew VPP tokens need to be renewed annually. If an IT administrator uploads the wrong VPP token to the wrong MDM solution, there is a risk of accidentally revoking all previously distributed apps. Keeping one VPP token with one MDM server reduces this risk.

What about Apple IDs?

Apps can leverage iCloud to sync mobile, desktop and even Apple TV operating systems. This allows the user to start utilizing an app on their phone and then pick up right where they left off on their computer.

This app hand-off and sync is possible because of a user's Apple ID. If your information security team approves of iCloud, you can allow your users to use their own Apple IDs and still deploy apps via device-based assignments.



Apple User Resources Under One Roof

Users demand the same seamless technology, support and service experience regardless of what device they use, and this expectation doesn't stop once the device is in their hands. There are many ways to extend the consumer Apple ecosystem experience. One way do so is through a managment app.

A management app enables IT to curate assets and provide users with an easy way to obtain resources and services, such as apps, printers, troubleshooting shortcuts and documentation. Anything loaded in the app is IT-approved, so instead of sending you a ticket, employees go directly to the app and immediately download the needed items — saving time for both you and your users.

Segmenting your Apple devices in separate management solutions forces end users to interact with different apps for Mac and iOS, ultimately creating confusion for where to go for what device. Streamlining ecosystem management with one solution gives you a common app for all Apple platforms. Users gain a consistent experience with a portal that has one brand, name, look and feel across both macOS and iOS.

Help them install or submit:

- ☑ App Store apps
- ☑ Email configurations
- ☑ E-books, guides and videos
- ☑ In-house apps
- ☑ VPN configurations
- ☑ Single Sign-on (SSO) integration
- ☑ Third-party software
- ☑ Basic maintenance
- ☑ Printer mapping and drivers
- ☑ Password resets
- ☑ Software and OS upgrades
- ☑ Hardware requests

3 Where Ecosystems Intersect

Reporting Tools as your Single Pane of Glass

The need for a holistic view into your environment is undeniable. Commonly referred to as a single pane of glass, you want the status of all endpoints, the ability to generate reports for senior management, and get a 360-degree view into your inventory. While UEM providers pitch this as the core reason for one universal tool, the lack of up-to-date support for the latest platform features overshadows the value of what you get with one window into your world.

Instead, look to proven, purpose-built business intelligence / reporting tools for your single pane of glass. Rather than reporting from your device management tool alone, aggregate the data into a BI or IT service management tool (e.g., Domo, Splunk, Tableau and ServiceNow), which is designed to show dashboard data. This lets each ecosystem management tool do what its designed to do best — manage devices. All device data can then be sent to a reporting / BI tool.

Devices Managed by Ecosystem

Option 3	Apple	Microsoft	Google
Desktop	macOS	Windows	Chrome OS
Mobile	iOS	Windows Mobile	Android
TV	tvOS	—	Chrome OS
Management Tool	**MDM (Jamf)**	**Intune/SCCM**	**G Suite Management**
Reporting Tool	**BI Tool: ServiceNow, Splunk, Tableau, etc.**		

The Power of "And"

When you mange by ecosystem, it's important to consider a management solution that fits seamlessly into your existing IT infrastructure. Services such as identity access management, directory services and network access, which may already be in your environment, are becoming platform agnostic and should extend across your managed ecosystems. Identity management, network access control and directory services can easily work with Apple, Microsoft and Google devices, but are not directly built into most device management solutions.

Instead, rely on purpose-built service providers to handle identity management, directory services and network access to do what they do best instead of hoping a unified tool can do it all. An integration-friendly ecosystem device management tool that can connect to existing IT services is better for organizations in the long run because it leverages what's best about the platforms while fitting into a broader IT strategy.

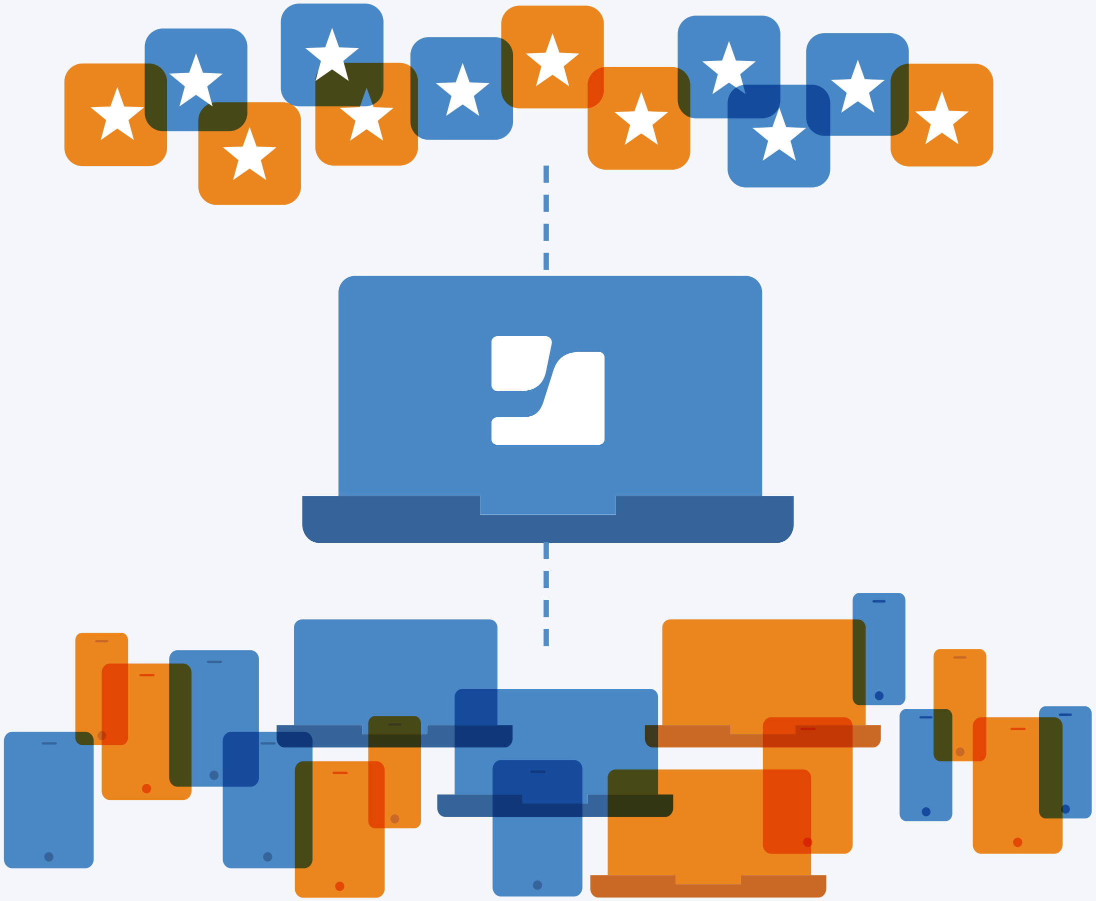
Devices Managed by Ecosystem

Device Type	Apple	Microsoft	Google
Computer	macOS	Windows	Chrome OS
Mobile	iOS	Windows Mobile	Android
TV	tvOS	—	Chrome OS
Management Tool	**MDM (Jamf)**	**Intune/SCCM**	**G Suite Management**
Reporting Tool	BI Tool: ServiceNow, Splunk, Tableau, etc.		
Identity Management	Okta, Ping, One Login, etc.		
Directory Services	Active Directory, Open Directory, JumpCloud, etc.		
Network Access	Cisco, Aruba, Wandera, etc.		

Jamf Integrations

Jamf’s platform is able to integrate with third-party tools, such as ServiceNow, RobotCloud, Tableau, Splunk and even SCCM to share your Apple inventory data. This gives you a better reporting for all your device and better management for your Apple devices.

Jamf builds solutions that extend and connect. From cross-industry integrations to specific solutions, Jamf integrates with more than 200 providers to ensure we work the way you need us to work.



4

Conclusion

Embrace the Apple Management Standard Across Your Apple Ecosystem

The power of Apple devices cannot be denied. And, the more computer and mobile teams unite to manage Mac, iPad, iPhone and Apple TV devices under one management solution, the better your management experience will be and the more you will empower your users.

The right solution for your Apple platform provides your team with zero-day support and streamlined workflows to implement DEP, VPP and leverage MDM profiles to customize the device experience for all of your users.

Jamf is the tool trusted by those who trust Apple. As the standard in Apple device management, Jamf makes it easy for you and your organization by offering a simplified cost structure, one contract for all your Apple device management needs, one upgrade schedule and one number to call for expert Apple advice.

Industry-best management capabilities are only the start. Jamf offers the whole product experience, meaning our services don’t stop once you become a customer. If anything, they only get better. From our world-class support model that provides you with a designated Jamf expert, to our educational courses that show you everything you need to know about our tool, to the 47,000-plus members of the Jamf Nation community who are ready to talk Apple management at a moment’s notice, you will not find a better Apple management provider out there. We stake our reputation on it.

jamf

Put us to the test by requesting a free trial of the best Apple management solution the industry has to offer.

Start Trial