vmware

GET STARTED

Workspace ONE Unified Endpoint Management for iOS and iPadOS

Upgrade Your Employee Experience

Studies show organizations that leverage great technology for their workforce provide a more positive experience for their employees and therefore have an advantage over the competition in recruiting and retaining top talent[1] and achieving peak user productivity. Companies that embrace the latest technologies from Apple have taken a great strategic step toward achieving that competitive edge. And VMware Workspace ONE® Unified Endpoint Management (UEM) has helped make millions of Apple iOS and iPadOS devices part of enterprise mobility initiatives worldwide, facilitating a multitude of use cases with management of iOS and all other device platforms in a single comprehensive, powerful solution.

Workspace ONE UEM enables IT to configure iPhones and iPads over the air with security policies, apps, a unified app catalog, VPN, and other resources for BYOD, corporate-owned, shared, and kiosk devices. Integrations with key Apple services like Apple Business Manager, Apple School Manager, and AppleCare simplify the execution of enterprise mobility strategies.

1. Randstad North America, Inc. "Hiring and Developing Digital Leaders." 2018

VMware: A Global Leader

Top analysts recognize Workspace ONE as a global industry-leading platform for unified endpoint management because it covers more use cases with extensive capabilities for iOS and other deployments, including

- Device activation and configuration
- App management and user enablement
- Security and data loss prevention
- User privacy and employee experience

Workspace ONE Unified Endpoint Management (UEM) from VMware helps IT easily and effectively deploy and manage Apple iOS and all other device types using a single comprehensive solution. Workspace ONE UEM is an industry leader helping to make iOS an integral part of enterprise mobility initiatives worldwide.

Device Activation and Configuration

To meet the demands of today's fast-paced and distributed organizations, IT must get Apple devices up and running quickly and have full visibility into all devices connected to corporate resources. Workspace ONE UEM supports User Enrollment for BYO environments and Custom Automated Enrollment to streamline and customize deployments of corporate-owned iOS devices.

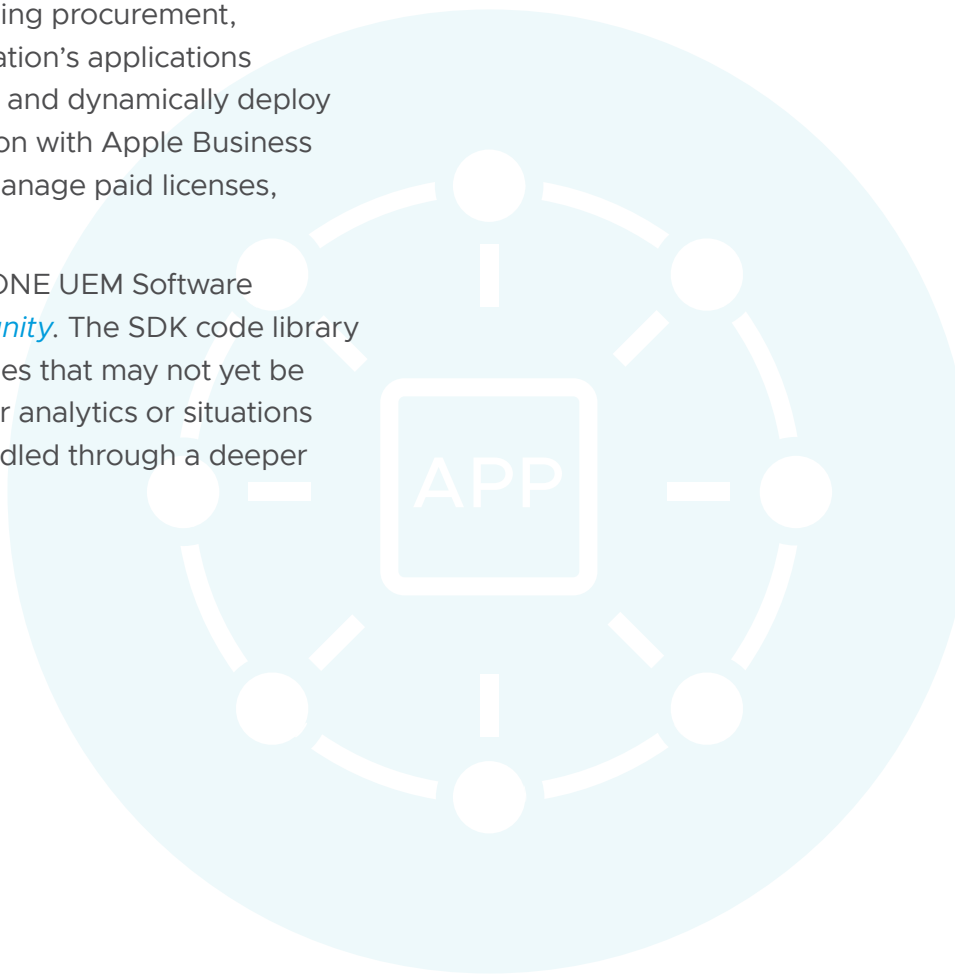
Devices can be shipped directly to office locations, remote employees or field teams, and security policies, Wi-Fi settings, email and more can be automatically installed over the air after users authenticate with corporate credentials or a token. With pre-set and customizable configurations, employees are far more likely to have a great experience as their devices are quickly onboarded out of the box with zero IT assistance, and they're able to access resources like email and corporate networks on their new devices within minutes.

Get iOS and iPadOS devices up and running quickly with out-of-the-box configurations and automated, over-the-air device activations to ensure a positive initial employee experience.

App Management and User Enablement

Workspace ONE UEM empowers IT to manage the full app lifecycle spanning procurement, deployment, management, and security. Admins can sync in their organization's applications whether they are publicly hosted on the App Store or internally developed and dynamically deploy them with custom configurations for a seamless user experience. Integration with Apple Business Manager takes this one step further by allowing admins to automatically manage paid licenses, version updates, and the deployment of iOS Custom Apps (formerly B2B).

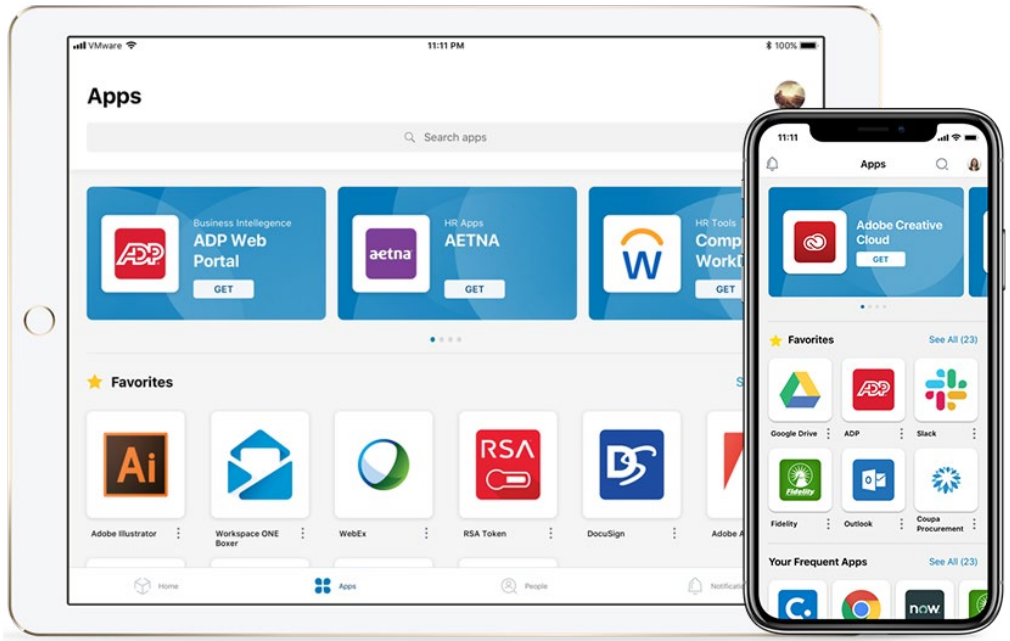
Companies can also develop their own applications using the Workspace ONE UEM Software Development Kit™ (SDK) or using standards set by the *AppConfig Community*. The SDK code library can be used to enable additional app configurations and security capabilities that may not yet be available as part of the native platforms. Certain use cases such as granular analytics or situations where an MDM profile installation on the device is not possible can be handled through a deeper integration with the SDK.



Easy and Secure Access to Apps

Apps of any type can be deployed by Workspace ONE UEM through a silent automated installation or on demand by users from a unified app catalog. The built-in single sign-on (SSO) in the unified app catalog and the per-app tunneling capabilities in Workspace ONE UEM make it easy for users to securely access all the apps and resources they need to do their work. And to ensure apps are always up to date, admin-configured compliance policies can be set to send push notifications and ultimately withhold services (for example, possible loss of email access) until users update to the latest app versions.

Deliver a superior employee experience by enabling SSO access to our self-service unified catalog of approved apps and services.



Security and Data Loss Prevention

Workspace ONE UEM provides security throughout the lifecycle of a device with comprehensive certificate lifecycle management, a service that can renew certificates automatically or manually. On top of that, VMware Workspace ONE® Tunnel encrypts traffic from individual applications to the back-end systems they talk to with "least privilege access" through the VMware Unified Access Gateway,™ which proxies and protects the application. These are just a couple of the ways Workspace ONE UEM improves the security posture of your IT environment, but these powerful protections are just the beginning.

Zero Trust Conditional Access

From there we enforce context-based, zero trust conditional access. The Workspace ONE® Access identity layer queries UEM to determine device compliance and can also pick up on user behavioral anomalies and other attributes to assess the security risk at the moment of access. For example, built-in intelligence understands if a user is accessing from an uncommon location, or if there has been an unusual spike in download activity. And through Trust Network integrations with the most popular endpoint protection providers, Access can enhance its contextual risk assessment with real-time threat data.

Once the security risk is understood, the Workspace ONE Access layer can take any of several actions. If everything checks out, the user can be granted full access to corporate resources. Alternatively, multi-factor authentication can be enforced, or a device that's out of compliance may be automatically remediated. Or, if the risk is unacceptable, access may be denied completely. If it's a corporate-owned device, it can even be remotely wiped.

With workers accessing apps and other corporate resources from every imaginable location, using every type of device, it's easier than ever for hackers to target assets that are outside the organization's hardened perimeter. **Zero trust conditional access** is security made to protect organizations in today's decentralized IT landscape.

Data Loss Prevention

Configurable features for system settings, encryption, data protection, apps, network connections, device controls, and more are built in. Restrictions can be set to disable the device camera, and disallow sharing sensitive work data between apps, syncing with unknown devices and more to prevent data leakage. Corporate-owned devices can be supervised for higher levels of control, which is especially useful for high-security and education use cases. Supervision enables IT to disable app removal, restrict configurable settings, and prevent iCloud backups, among other things.

Protect corporate resources with automated certificate lifecycle management, Workspace ONE Tunnel to encrypt data in use, zero trust conditional access for today's decentralized work force, and configurable data loss prevention.

BYO and User Privacy

Of course, many enterprises are moving away from corporate-owned devices and toward BYO mobility models because the cost/benefit analysis makes a lot of sense in most cases. In order for a BYO program to succeed, companies must provide a good employee experience—and that starts with respecting the employee's personal privacy. With User Enrollment, Workspace ONE supports the option to use Managed Apple IDs through Apple Business Manager, keeping work data completely separate from the device owner's personal data. This type of enrollment ensures that IT can only access relevant business-related apps and information while users are free to privately operate their devices for personal pursuits.

The User Enrollment partition allows admins to manage apps and data deployed via MDM, and that separation is so complete that IT can't even collect device-identifiable information like UDID, serial number, or IMEI. Admins also cannot wipe the device, clear the passcode, or require complex alphanumeric passcodes.

We're All About the Employee Experience

In order for privacy to have a truly positive impact on the employee experience, users must fully trust their device's privacy status. And that means understanding it in detail and knowing when something changes. So we built Workspace ONE Privacy Guard, a set of enterprise-ready privacy tools built into the Workspace ONE platform that helps customers manage privacy policies and clearly communicate them to employees. Our privacy SDK makes it easy for developers to build the same privacy experience into internally built mobile apps. In addition, Workspace ONE Privacy Guard creates a new role in the Workspace ONE console, "Privacy Officer," which provides access to view system settings that affect users and has full editing rights around privacy.

Make sure your employees are comfortable with your BYO program by respecting their personal privacy and making certain they KNOW their privacy is protected.

Workspace ONE privacy notices mitigate device management fears by informing employees of what information on the device admins are capable of seeing and how the information is used.

With incomparable levels of automation, self-service, intelligent security, and trustworthy user privacy, Workspace ONE makes mobility programs with iOS and iPadOS easier to manage—and more successful—than ever.

Join us online:

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Copyright © 2020 VMware, Inc. All rights reserved.
This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.
VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: FY20-5718-WKSPONE-UEM-FOR-IOS-IPADOS-EBOOK-WEB-USLET-20200309 3/20