omnissa™

Omnissa Workspace ONE Unified Endpoint Management for iOS and iPadOS

GET STARTED →

Upgrade the employee experience

Organizations that leverage advanced, user-friendly, and reliable technology for their workforce are able to deliver a more positive employee experience. A superior employee experience can give businesses **an advantage in recruiting and retaining top talent,** and a head start in achieving peak employee productivity. Organizations that embrace the latest technologies from Apple have taken a great strategic step toward achieving these benefits by providing their people with a **choice of devices** that they prefer over other options.

Omnissa Workspace ONE® Unified Endpoint Management (UEM) has helped manage the successful deployment of millions of Apple iOS and iPadOS devices for thousands of customers worldwide, facilitating an array of use cases with modern management of all types of devices and platforms in ONE powerful solution.

Omnissa: a global leader

Workspace ONE UEM from Omnissa helps IT easily and effectively deploy and manage iPhones, iPads, Macs, and virtually all other device types using a single comprehensive solution. There is no need to utilize multiple tools to manage Macs, mobile and rugged devices, IoT, and PCs—Workspace ONE helps you get it all done from a single pane of glass.

Analysts all over the world recognize Workspace ONE as an industry-leading platform for unified endpoint management because it covers more use cases (BYO, corporate-owned, shared devices, and more) with extensive capabilities for iOS, including:

- Device activation and configuration
- App management and user enablement
- Security and data loss prevention
- Support for Declarative Device Management and OS updates
- User privacy and employee experience

Workspace ONE UEM helps IT easily and effectively deploy and manage iPhones, iPads, Macs and many other device types using a **single comprehensive solution.**

Device activation and configuration

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

Devices can be shipped directly to office locations, remote employees, or field teams. Security policies, Wi-Fi settings, email, and more can be automatically installed and configured over the air after users authenticate with corporate credentials or a token. With pre-set and customizable configurations, employees will 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 within minutes.

Declarative device management and OS updates

Workspace ONE supports Apple's Declarative Device Management (DDM) for iOS, streamlining your IT team's ability to apply OS updates. Workspace ONE allows admins to specify their desired OS version, and set the date and time to have their iOS fleet updated while users are continually notified weeks in advance so they can update their devices when it's convenient.

Omnissa Workspace ONE

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 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 ABM 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 thier own applications using the Omnissa 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 platform. 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.

Shared iPads

The Shared iPad capability is designed to enable multiple users to employ a single device, usually in a shift work setting. It utilizes Managed Apple IDs and separates data with an encrypted partition for each device user. Workspace ONE personalizes the device for each user, ensuring a positive employee experience every time.

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. Built-in single sign-on (SSO) 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 if desired (for example, withholding access to email) until users update to the latest app versions.

Workspace ONE Intelligent Hub

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

Security for iOS and iPadOS

Certificate lifecycle management

Deliver a seamless, consumer-like end-user experience across shared devices by giving workers access to only the apps, content, and settings they need to stay productive and engaged.

Per-app VPN

Omnissa Workspace ONE® Tunnel encrypts traffic from individual applications to their back-end systems with “least privilege access” through the Omnissa Unified Access Gateway,™ which proxies and protects the application.

Zero trust conditional access

From there we enforce context-based, zero trust conditional access. The Omnissa 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, Access 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 if it was lost or stolen.

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

Many enterprises are choosing BYO mobility models because the cost/benefit analysis makes sense for their business. For BYO programs to succeed, companies must provide a strong 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 ABM, keeping work data separate from the 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. The separation is so complete that IT can't even collect device-identifiable information, like UDID, serial number, or IMEI, and cannot wipe the device, clear the passcode, or require complex alphanumeric passcodes. This level of privacy can ensure a high acceptance rate for your BYO program.

We're ALL ABOUT the employee experience

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. Workspace ONE® Privacy Guard 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, 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.

Workspace ONE privacy notices mitigate device management fears by informing employees of what exactly admins can see and how the information is used.

Workspace ONE Privacy Guard

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

Add on fully integrated remote support

Omnissa Workspace ONE® Assist is an optional solution that allows admins to remotely view iOS devices and other device types directly from the console for troubleshooting purposes. Issues are more likely to be corrected the first time when support personnel can see the user's screen and take direct action, and the employee experience is positive when problems are resolved the right way, right away. Assist helps minimize downtime and reduce IT support costs by eliminating the need for in-person assistance. The solution also ensures privacy and trust by notifying users when their screens are visible and allowing them to accept or reject certain requests and end the session at any time.

omnissa™

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.

Dive into all Workspace ONE has to offer.

LEARN MORE →