VMWARE WORKSPACE ONE

Edition Comparison Table

VMware Workspace ONE™ is the simple and secure enterprise platform that delivers and manages any app on any smartphone, tablet or laptop. By integrating app access management, unified endpoint management, and real-time application delivery, Workspace ONE engages digital employees, reduces the threat of data loss, and modernizes traditional IT operations for the mobile-cloud era.

Workspace ONE editions make it simple for organizations to license the right amount of technology based on user and endpoint requirements. Most organizations will license or subscribe to a mix of Standard, Advanced and Enterprise, which all work together, to create a single digital workspace platform across their entire organization.

		STANDARD EDITION	ADVANCED EDITION	ENTERPRISE EDITION
ACCESS MANAGEMENT				
Access Portal	Application portal for mobile and desktop platforms to install or launch into various applications on the endpoint device. Includes VMware AirWatch® App Catalog and Workspace ONE App Portal.	●	●	●
Federated Single Sign-On (SSO)	Federate active directory to third party or internally developed apps using one of the federation standards. Includes password form-fill feature for SSO. *Functionality limitations for per device licensing mode.	●*	●*	●*
Multi-Factor Authentication	Multi-factor authentication for accessing applications with supporting mobile application VMware Verify. *Functionality limitations for per device licensing mode.	●*	●*	●*
One-touch SSO	Ability to leverage mobile application management with certificate and biometric authentication for seamless application authentication. *Functionality limitations for per device licensing mode.	●*	●*	●*
Conditional Access Control	Application access control policy to restrict access to applications based on user authentication strength, device platform, network range and application. *Functionality limitations for per device licensing mode.	●*	●*	●*
Risk-based Conditional Access Control	Conditional access control plus additional risk-based access policy capabilities including device risk and compliance such as managed and compliant devices, device passcode, geofencing, OS version, application whitelist, blacklist, etc. *Functionality limitations for per device licensing mode.		●*	●*
Identity Provider (IDP)	Ability to serve as the identity database for user accounts. *Functionality limitations for per device licensing mode.	●*	●*	●*
Mobile Email Management	Email server ActiveSync access control integration via direct server APIs PowerShell, Office 365 and Google Apps.	●	●	●
Secure Email Gateway (SEG)	In-line gateway solution to provide access control to work email server to encrypt data and attachments.		●	●
VMware PIV-D Manager	Ability to enforce two-factor authentication through a Derived Credential client certificate using VMware PIV-D Manager.		●	●

		STANDARD EDITION	ADVANCED EDITION	ENTERPRISE EDITION
SECURE APPS AND DATA				
VMware Boxer	Secure containerized email, calendar and contacts solution. Includes VMware Boxer® and VMware AirWatch® Inbox.		•	•
VMware Browser	Intranet browsing application to secure access to web applications.		•	•
VMware Content Locker	Aggregate and view files across on-premises and cloud-based file repositories. Includes mobile content management, file editing and annotation while protecting from data loss with cut/copy/paste/ open-in restrictions. Combines VMware® Content Locker Standard and Content Locker Advanced features.		•	•
Socialcast	Enterprise social networking platform and team chat and collaboration.	Add-on	Add-on	Add-on
Mobile Application Management	Ability to install, track inventory, configure and assign applications—internal, public, web, native, etc.—to users and devices.	•	•	•
Container and SDK with DLP Protection	App containment via stand-alone mobile app management and VMware AirWatch® Software Development Kit™ (SDK).	•	•	•
App Wrapping	Ability to add security policies and management capabilities into an app that is already developed.		•	•
Per-App VPN Tunneling	Per-app VPN solution for connecting applications (VMware or third- party) to corporate intranet services. Includes VMware AirWatch® Tunnel™ and VMware NSX® integration.		•	•
UNIFIED ENDPOINT MANAGEMENT				
Mobile Device Management (MDM)	Ability to configure device policies, settings and device configurations across phones, tablets and laptop devices.	•	•	•
Special-purpose Device Management (OEM)	Special technology to manage shared, kiosk and rugged devices. Includes additional OEM specific device management APIs and legacy platform support including Android OEM, Samsung Knox, Windows CE, Windows Mobile, QNX, etc.	•	•	•
Wearable and Peripheral Management	Ability to manage wearable devices and peripheral devices such as smart glasses, printers or other accessories.	•	•	•
Remote Diagnostics and Support	Remote troubleshooting, diagnostic and support tools to remotely execute and terminate processes, capture logs, remote screen viewing and control.	•	•	•
Advanced Desktop Management	Includes custom scripting, BitLocker encryption, desktop/Win32 app management, Windows 10 Enterprise polices (incl. Credential Guard, Device Guard).		•	•

		STANDARD EDITION	ADVANCED EDITION	ENTERPRISE EDITION
UNIFIED ENDPOINT MANAGEMENT				
Telecom Management Tools	Telecom management features to track data, call and message consumption and automate actions and compliance.		●	●
IT Compliance Automation Engine	Ability to build compliance policies with automated remediation workflows, such as application whitelist/blacklist, GPS and geofencing, OS version control, and compliance escalation.	●	●	●
VIRTUAL APPS AND DESKTOPS				
Virtual Apps and Desktops (Horizon)	Ability to deliver virtual applications or desktops to devices.			●
LICENSING				
Number of Licensed Devices	Maximum number of devices allowed under management or SDK app managed.	Per-Device License: 1 Per-User License: 5	Per-Device License: 1 Per-User License: 5	Per-Device License: 1 Per-User License: 5
Workspace ONE Portal Access	Maximum number of devices that may access the Workspace ONE portal through a browser without being managed.	Per-Device License: 1 Per-User License: Unlimited	Per-Device License: 1 Per-User License: Unlimited	Per-Device License: 1 Per-User License: Unlimited

* When licensing Workspace ONE in a device-license model, the SSO and Access Control technology is restricted to only work on managed devices and from managed applications. Organizations looking to enable access to enterprise applications across devices not managed by AirWatch or allowing access to enterprise applications from any web browser, must license Workspace ONE in a per-user license model. In addition, VMware Verify is not available in a device-based license.

For more information on Workspace ONE, please visit: vmware.com/go/workspaceone.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2017 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. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: 45711-vmw-comparison-wkspc1-editions 07/17