

# VMWARE WORKSPACE ONE

## Edition Comparison Table

VMware Workspace ONE™ is an intelligence-driven digital workspace platform powered by VMware AirWatch® technology. Workspace ONE integrates access control, application management and multi-platform endpoint management to simply and securely deliver and manage any app on any device. The editions below are available as a cloud service (on premises deployment options are also available).

		STANDARD EDITION	ADVANCED EDITION	ENTERPRISE EDITION	ENTERPRISE for VDI EDITION
<b>INTELLIGENCE AND AUTOMATION</b>					
<b>Reports</b>	Design custom reports with device, application and user data.	●	●	●	●
<b>Configurable, Historical Dashboards</b>	Delivers insights into device and app usage over time to enable optimized resource allocation and license renewals.			●	●
<b>App Analytics</b>	Measure app adoption and engagement across environment and quickly discover the apps that are used the most, easily quantifying ROI of app deployments.			●	●
<b>Decision Engine for Automation</b>	Automate processes with defining rules that take actions based on a rich set of parameters.			●	●
<b>Mobile Flows</b>	Surfaces context-based actions and notifications, empowering users to complete tasks across backend business systems without leaving VMware Boxer™.			●	●
<b>ACCESS MANAGEMENT</b>					
<b>Access Portal</b>	Application portal for mobile and desktop platforms to install or launch into various applications on the endpoint device. Includes AirWatch App Catalog and Workspace ONE App Portal.	●	●	●	●
<b>Federated Single Sign-On (SSO)</b>	Federate active directory to third party or internally developed apps using one of the federation standards. Includes password form-fill feature for SSO. <i>*Functionality limitations for per device licensing mode.</i>	●*	●*	●*	●*

		STANDARD EDITION	ADVANCED EDITION	ENTERPRISE EDITION	ENTERPRISE for VDI EDITION
<b>ACCESS MANAGEMENT</b>					
<b>One-touch SSO</b>	Ability to leverage mobile application management with certificate and biometric authentication for seamless application authentication. On Android, SSO requires the VMware Tunnel app, which can be used with any Workspace ONE edition. <i>*Functionality limitations for per device licensing mode.</i>	●*	●*	●*	●*
<b>Conditional Access Control</b>	Application access control policy to restrict access to applications based on user authentication strength, device platform, network range and application. <i>*Functionality limitations for per device licensing mode.</i>	●*	●*	●*	●*
<b>Identity Provider (IDP)</b>	Ability to serve as the identity database for user accounts. <i>*Functionality limitations for per device licensing mode.</i>	●*	●*	●*	●*
<b>Mobile Email Management</b>	Email server ActiveSync access control integration via direct server APIs PowerShell, Office 365 and Google Apps.	●*	●*	●*	●*
<b>Multi-Factor Authentication</b>	Multi-factor authentication for accessing applications with supporting mobile application VMware Verify. <i>*Functionality limitations for per device licensing mode.</i>	●*	●*	●*	●*
<b>Secure Email Gateway (SEG)</b>	In-line gateway solution to provide access control to work email server to encrypt data and attachments.	●**	●	●	●
<b>VMware PIV-D Manager</b>	Ability to enforce two-factor authentication through a Derived Credential client certificate using VMware PIV-D Manager.		●	●	●
<b>Unified Access Gateway (UAG)</b>	Direct authentication requests to the appropriate server and discard unauthenticated requests to provide secure access to resources.	UAG Standard	UAG Advanced	UAG Enterprise	UAG Enterprise
<b>SECURE APPS AND DATA</b>					
<b>Workspace ONE Web</b>	An intuitive, secure browser that provides instant access to intranet sites and web apps. Includes the ability to lock devices into kiosk mode.		●	●	●
<b>Workspace ONE Content</b>	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.		●	●	●
<b>Workspace ONE Boxer</b>	Enable employees with a secure, better-than-native email experience with exciting productivity features for mail, calendar and contacts.		●	●	●

		STANDARD EDITION	ADVANCED EDITION	ENTERPRISE EDITION	ENTERPRISE for VDI EDITION
<b>SECURE APPS AND DATA</b>					
<b>Workspace ONE Send</b>	Enable the secure pass back and forth of Microsoft Intune protected Word, Excel, or PowerPoint attachments between the Microsoft Office 365 apps and the Workspace ONE productivity apps.	●	●	●	●
<b>Mobile Application Management</b>	Ability to install, track inventory, configure and assign applications - internal, public, web, native, etc - to users and devices.	●	●	●	●
<b>Container and SDK with DLP Protection</b>	App containment via stand-alone MAM and AirWatch Software Development Kit (SDK).	●	●	●	●
<b>App Wrapping</b>	Ability to add security policies and management capabilities into an app that is already developed.		●	●	●
<b>VMware Tunnel</b>	Per-app VPN solution for connecting applications (VMware or third party) to corporate intranet services. Includes VMware Tunnel™ and VMware NSX® integration. On Android, SSO requires the VMware Tunnel app, which can be used with any Workspace ONE edition.		●	●	●
<b>UNIFIED ENDPOINT MANAGEMENT</b>					
<b>Mobile Device Management (MDM)</b>	Ability to configure device policies, settings and device configurations across phones, tablets and laptop devices.	●	●	●	●
<b>Special-purpose Device Management (OEM)</b>	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.	●	●	●	●
<b>Wearable and Peripheral Management</b>	Ability to manage wearable devices and peripheral devices such as smart glasses, printers or other accessories.	●	●	●	●
<b>Advanced Desktop Management</b>	Includes custom scripting, BitLocker encryption, desktop / Win32 app management, Windows 10 Enterprise policies (incl. Credential Guard Device Guard).		●	●	●
<b>Telecom Management Tools</b>	Telecom management features to track data, call and message consumption and automate actions and compliance.		●	●	●
<b>IT Compliance Automation Engine</b>	Ability to build compliance policies with automated remediation workflows, such as application whitelist/blacklist, GPS and geofencing, OS version control, and compliance escalation.	●	●	●	●

		STANDARD EDITION	ADVANCED EDITION	ENTERPRISE EDITION	ENTERPRISE for VDI EDITION
<b>UNIFIED ENDPOINT MANAGEMENT</b>					
<b>AirLift for Windows 10</b>	A server-side co-management connector to Microsoft System Center Configuration Manager (SCCM) that de-risks and speeds transition of traditionally high pain-point PC management tasks to Workspace ONE modern management for Windows 10.	•	•	•	•
<b>VMware Workspace ONE Advanced Remote Management</b>	Remotely support and troubleshoot corporate-owned devices with advanced remote management and control tools.	Add-on	Add-on	Add-on	Add-on
<b>VIRTUAL APPS AND DESKTOPS</b>					
<b>Virtual Apps (Horizon)</b>	Ability to deliver virtual applications to devices.			•	•
<b>Virtual Desktops (Horizon)</b>	Ability to deliver virtual applications and/or desktops to devices.				•
<b>Number of Licensed Devices</b>	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	Per-Device License: 1 Per-User License: 5
<b>Workspace ONE Portal Access</b>	Maximum number of devices that may access the Workspace ONE portal through a browser without being managed.	Per-User License: Unlimited	Per-User License: Unlimited	Per-User License: Unlimited	Per-User License: Unlimited

\* When licensing Workspace ONE in a device-license model, the SSO, MFA, 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 Workspace ONE UEM (AirWatch) or allowing access to enterprise applications from any web browser, must license Workspace ONE in a per-user license model.

\*\* SEG included in Workspace ONE Standard is limited to native mail clients.

**For more information on Workspace ONE, please visit: [vmware.com/products/workspace-one](http://vmware.com/products/workspace-one).**

