VMware Workspace ONE Deployment – Standard

AT A GLANCE

VMware delivery specialists provide product implementation and onboarding services in the Americas and EMEA for a variety of VMware products.

KEY BENEFITS

- Skilled resources available to supplement customer teams
- Experts in VMware technologies
- Wide variety of assistance available

SKU

VA-PS-WOS-DEP

VA-PS-ELA-WOS-DEP

WDS-WOSDS-1TCT0-C1S

WDS-WOSDS-1TCT0-A1S

WDM-WOSDS-1TCT0-C1S

WDM-WOSDS-1TCT0-A1S

WDP-WOSDS-1TCT0-C1S

WDP-WOSDS-1TCT0-A1S

Service Overview

This service provides for technical support related to the VMware AirWatch® ("VMware") Enterprise Mobility Management™ and VMware Workspace ONE® offerings as set out below in the services description (the "Services" or Professional Services"). The Workspace ONE solution allows customers to activate, profile, and track mobile devices and usage.

The deployment will include implementation of a Workspace ONE environment with integration supported by components installed on-premises in the Customer's data centers. This project will be organized into four phases: 1) Initiate, 2) Plan, 3) Execute, 4) Close.

The implementation scope includes:

- Review of associated pre-requisites
- Implementation of VMware AirWatch® Enterprise Mobility Management™ servers
- Implementation of VMware AirWatch® Secure Email Gateway™
- VMware Workspace ONE® Access™ installation/configuration
- Unified Application Catalog and VMware Workspace ONE® Launcher™
- Directory Services Integration
- Personal Information Management (PIM) – email, contacts and calendar
- Security policies – enrollment restrictions, compliance policies, privacy policies, terms of use
- Application management – public, internal, Volume Purchase Program application
- Mobile Device Management enrollment strategy

Service Assumptions

1. VMware will assist with the installation/configuration of one environment under this datasheet. The environment type (SaaS or On-Premises) will be implemented based on the license type purchased by the Customer.
2. VMware will deliver the Remote Professional Services using global resources. VMware makes no commitment, representation, or warranty regarding the citizenship or geographic location of the Consultant(s).
3. VMware will assist with up to four different device types/operating systems for configuration and setup (iOS, Android, Mac and Windows) of up to five devices of each operating system. Rugged Android, Rugged Windows Mobile/CE devices and printers are out-of-scope. Any additional device roll-out beyond the five devices are out-of-scope.

4. VMware will integrate only one corporate e-mail infrastructure via one Email Management integration (PowerShell, AirWatch Secure Email Gateway v2 AirWatch Secure Email Gateway on VMware Unified Access Gateway™).
5. Advanced PC Management (Mac/Windows scripting and product provisioning) is out-of-scope.
6. Alignment of all AirWatch Enterprise Mobility Management configurations and policy design with Customer's requirements is the responsibility of the Customer. VMware will provide recommendations and assistance.
7. Unified Access Gateway (Content, Tunnel, Browsing) integration is out-of-scope. One can purchase the associated service offering to incorporate Unified Access Gateway into the scope.
8. Procurement and installation of hardware for any components that will be installed on-premises is the responsibility of the Customer. VMware may provide recommendations.
9. Configuration of software other than VMware is the responsibility of the customer.
10. VMware will provide implementation services for various levels of integration, listed in the Service Deliverables section, for Workspace ONE Access. A maximum of five (5) units are available for additional integrations. These units are calculated based on the Integration Unit Valuation Matrix table below the Service Deliverables table.
11. Third Party Web Applications: Any SAML 2.0 compliant web applications can be integrated with Workspace ONE Access. The Customer is required to work independently with the service provider to provide VMware with all required integration details or SAML meta-data. These include, but are not limited to the following:
    - Login Redirection
    - Assertion Consumer Service URL
    - Recipient Name
    - Signing Certificates
    - Audience
    - Assertion Lifetime
    - Attribute Mapping
    - Application Parameters
12. Internally Developed Web Applications: Any SAML 2.0 compliant internal application can be integrated with Workspace ONE Access. The Customer is required to provide VMware with all required integration details or SAML meta-data. These include, but are not limited to the following:
    - Login Redirection
    - Assertion Consumer Service URL
    - Signing Certificates
    - Audience
    - Assertion Lifetime
    - Attribution Mapping
    - Application Parameters
13. Native Application On-Touch SSO Integration: native applications supporting SAML single-sign-on can be configured to accept Identity Provider initiated SSO through

VMware managed devices. The Customer is required to work independently with the service provider to provide VMware with all required integration details including attributes to be passed via VMware.

14. VMware cannot guarantee that individual third party SAML endpoints will integrate successfully with Workspace ONE Access given unforeseen Customer or service configurations or limitations.
15. Workspace ONE Access for App Catalog will be implemented with Workspace One licensing.
16. Customer-specific customization for Workspace ONE Access is out-of-scope.
17. Includes High Availability for VMware (Device Services, Console, Secure Email Gateway v2 or AirWatch Secure Email Gateway on Unified Access Gateway, VMware AirWatch® Cloud Connector™, Enterprise Notification System v2, and Workspace ONE Access) for up to 16 servers.
18. Installation of Disaster Recovery (DR) is out-of-scope. One can purchase the associated service offering to incorporate Disaster Recovery into the scope of a deployment.
19. Certificate Authority integration can be included for the use of One Touch Single Sign-On with Workspace ONE Access. Certificate usage for Wi-Fi, VPN, email authentication is out-of-scope. One can purchase the associated service offering to incorporate certificate usage for authentication into the scope of a deployment.
20. Review of the console will be provided throughout the configuration; however formal training is out-of-scope.
21. Implementation of derived credentials is out-of-scope.
22. The scope of Service Deliverables listed in Section 6 below will be determined mutually by the parties during Phase 1 (Initiate) and Phase 2 (Plan). Service Deliverables not identified and scheduled prior to Phase 3 (Execute) will be considered out-of-scope.
23. Services or products that have been deprecated or reached end of life are out-of-scope.
24. Certain features may require the purchase of a Workspace ONE Deployment Add-On bundle. Please contact your VMware representative for further information.
25. Pre-requisites must be completed for all installation components before any installation activities will be performed.
26. VMware and the Customer will work closely together to ensure that project scope remains consistent, and issues are resolved in a timely manner. VMware will not provide a project manager as a role under this datasheet.
27. All work will be delivered remotely via screen-share. On-site travel is out-of-scope.
28. All work, documentation and deliverables will be conducted during VMware local business hours and will be provided in English.
29. Any feature not listed in Services Deliverables is out of scope, unless discussed and agreed to with the Product Deployment Team prior to purchase.
30. The staffing for this datasheet assumes all work will be completed within a maximum of 12 weeks after the initiation of Phase 3 (Execute). Should the duration of the engagement be extended, or should the product scope materially change, a project change request may be issued.
31. The period of performance is limited to 12 months from purchase date. Federal and Public-Sector customers who exceed this limit may contact their VMware representative for further clarification.

32. The scope of the services is deemed complete upon ONE of the following criteria - whichever comes first:
    - Upon completion of all deliverables within scope of the engagement as agreed upon in the Design Sign-off Form.
    - After 12 weeks from the date the project is moved to Phase 3 (Execute) as agreed upon in the Design Sign-off Form.
    - After 12 months from purchase date.
    - If the services were purchased using PSO credits the services expire the same time the credits expire, unless a credit extension is requested. Work with your Account Executive to determine a plan for all remaining credits on the account and request an extension.

Estimated Schedule

The Professional Service typically takes 4 – 6 weeks to fully deliver with the pre-defined scope and will consist of meetings every 3 - 5 business days, each being 2 - 4 hours in length, scheduled based on the agenda outlined for the next meeting. This is a target schedule but could vary depending on the availability of the assigned consultant. The estimated timeline for the engagement is outlined in the following table. The tasks defined each week can shift based on Customer readiness and availability of both the Customer and VMware. VMware will perform the Professional Services according to a schedule agreed by both parties.

Change Management

For Project Change Request, Customer and VMware will follow the project change request process in accordance with 2(c) of the General Terms and Conditions.

Responsibilities

All VMware and Customer responsibilities are listed in the Service Deliverables section. The ownership is defined as follows:

- **Primary Owner = VMware**: VMware is responsible for delivery of the component, with minimal assistance from the Customer's project team.
- **Joint**: VMware and the Customer's project team are jointly responsible for delivery of the component.
- **Primary Owner = Customer**: Customer is responsible for the delivery of the component, with recommendations from VMware as needed.

Service Deliverables

The following is a list of all the potential deliverables that the Customer may select. Items will be listed on the project schedule as agreed to by Customer and VMware during Phase 1 (Initiate) and Phase 2 (Plan).

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
Phase 1 (Initiate)				
1.1	Introduction meeting		Joint	

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
1.2	Review datasheet		Customer	Understand service assumptions and scope
1.3	Register for My Workspace ONE ID	My Workspace ONE access	Customer	Required to access resources and training
1.4	Provide Pre-Installation Requirements	VMware Recommended Architecture Guide, Pre-Installation Requirements Worksheet	VMware	Firewall configuration, server prep, load balancer configuration
Phase 2 (Plan)				
2.1	Plan Meeting		Joint	
2.2	Perform business requirements and solution design	Solution Design PowerPoint and Design and Implementation doc	VMware	Scope definition
2.3	Perform architectural review	VMware Recommended Architecture Guide, Visio diagram	VMware	
2.4	Review of technical pre-installation requirements	Pre-Installation Requirements Worksheet	VMware	Pre-requisite clarified with Customer network, database, server and security teams, hardware sizing and architecture
2.5	Review Best Practices Guide		VMware	Configuration best practices
2.6	Download and setup any required software/tools		VMware	
2.7	Summarize pre-work, next steps and requirements for Phase 3 (Execute)	Customer action items	VMware	
Customer requirements to proceed to Phase 3 (Execute)				
2.8	Procure virtual and/or physical servers		Customer	Servers accessible and software pre-requisites completed
2.9	Configure networking/firewall and service accounts for integration		Customer	Networking rules provisioned
2.10	Complete and return Pre-Installation	Installation Pre-Requisites	Customer	

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	Requirements Worksheet			
2.11	Send Design and Implementation doc for review and customer sign off	Design and Implementation doc and Plan Phase Completion Acknowledgment form	VMware	
2.12	Sign and return Plan Phase Completion Acknowledgment form	Plan Phase Completion Acknowledgment form	Customer	Scope of project cannot be modified without agreed change control
Phase 3 (Execute)				
Step 1: Installation				
AirWatch Enterprise Mobility Management				
3.1	Confirm completion of pre-requisites	Pre-Installation Requirements Worksheet	VMware	
3.2	Installation of VMware Enterprise Mobility Management server(s)	VMware Installation Guide	VMware	If Customer has necessary licensing
3.3	Installation of AirWatch Cloud Connector		VMware	
Identity Management and Unified Application Catalog (Workspace ONE Access)				
3.4	Configuration of Workspace ONE Access and Unified App Catalog		VMware	
Productivity Applications				
3.5	Installation of AirWatch Secure Email Gateway v2 (SEG v2) or AirWatch Secure Email Gateway on Unified Access Gateway, or Configuration of PowerShell		VMware	
Step 2: Configuration				
AirWatch Enterprise Mobility Management				
3.6	Configure Organizational Group structure (up to 5)		Joint	
3.7	Register email domain for auto-discovery		Joint	

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
3.8	Assistance configuring Directory Services integration: • Assist with creating up to 5 users • Assist with creating up to 5 administrators • Assist with adding one user group		Joint	
3.9	Assist with creating one of each desired profiles for up to three device Operating Systems		Joint	Profiles may be limited based on device operating system
3.10	• Assist with creating up to three of each of the following policies, one for each device Operating System (if applicable): • Enrollment Restriction Policy (i.e., # of devices, Ownership Types, etc.) • Compliance Policy (i.e., Comprised Status, Encryption, Application List, etc.,) • Privacy Policy (i.e., Collect GPS Data, Allow Full Wipe, etc.) • Terms of Use (i.e., Platforms, Geographies, etc.)		Joint	
3.11	Advanced Windows 10 Management: Windows 10 Management: • Work Access Enrollment • Azure Active Directory Enrollment • Agent Enrollment • Integration with Microsoft Business Store • Assist with installation of up to a total of 3 internal applications (.exe – 1 unit, zip – 1 unit, .msi – 1 unit)		Joint	

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	• Assist with configuration of up to 3 VMware Applications for Windows 10 • Profiles: Passcode, Wi-Fi, VPN, Restrictions, Data Protection, Firewall, Anti-virus, Encryption, Windows Updates, Windows Licensing, Kiosk, Windows Hello, Application Control, Personalization • Assist with the distribution and execution of up to two client scripts from the Workspace One® UEM console • Configuration of up to 2 CSPs via VMware Policy Builder • Assist with up to two Baselines configuration			
3.12	MacOS Management • Integration with Apple Business Manager • Assist with macOS specific enrollment method for up to 5 devices: Intelligent hub, Device staging enrollment, Apple Business Manager – DEP • Review Staging and Provisioning section of Workspace ONE UEM Admin Console • Assist with installation of up to a total of 3 internal applications using the Software Distribution feature: dmg – 1 unit, pkg– 1 unit, mpkg – 1 unit	macOS Management	Joint	Associated Licenses are required to be purchased Deploy macOS applications via the software distribution module on the Workspace ONE UEM console Incorporate a functional script in the Workspace ONE UEM console

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	• Assist with the distribution and execution of up to five client scripts from the Workspace ONE UEM console • Profiles: Passcode, Network, VPN, Exchange Web Services, LDAP, Dock, Restrictions, Software Update, Parental Controls, Directory, Secure and Privacy, Disk Encryption, Login Items, Login Window, Energy Saver, Time Machine, Finder, Accessibility, Printing, AirPlay Mirroring, AirPrint, Firewall, Firmware, Custom Attributes, Custom Settings			
Workspace ONE Access and Unified Application Catalog				
3.13	Complete Workspace ONE Access Configuration: • Sync with Active Directory users and groups • Configure the Unified Application Catalog. • Enable User AD Password change • Integration with Workspace ONE UEM (AirWatch Compliance)	Identity and Access Management	Joint	Integration with Customer's endpoints for single sign-on
3.14	Configure the following for Application Management functionality: • Internal Application (one per device type) • Web Application (one per device type) • Application Store integration		Joint	Configuration of application management policies

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
3.15	Assist with setup, association, and installation of Volume Purchase Program applications (sToken or License-Based). This will include: • Upload of sToken/redemption codes • Register up to 10 devices for up to 3 deployment types with Volume Purchase Program Terms of Use • Register using app catalog and automatic • Install application on same devices as Auto/On-Demand		Joint	Configuration of Volume Purchase Program applications
3.16	Assist with SAML Integration of the following: • Workspace ONE UEM Admin Authentication • Workspace ONE UEM User Authentication • One Standard SAML Application	Identity and Access Management	Joint	Standard Enterprise Web Applications: These commonly used enterprise web applications can be configured using integration units. These applications have been thoroughly tested with Workspace ONE Access. The list, which is subject to continuous updates can be found *here*. The Customer is required to work independently with the service provider to provide VMware with all required integration details or SAML meta-data.
3.17	Assist with VDI Integration of one of the following: • VMware Horizon® View™ • Horizon Cloud Hosted • Horizon Cloud on Azure	Identity and Access Management	Joint	

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	• Citrix Xenapps and Xendesktops			
3.18	Configure the following Authentication Methods: • Directory • iOS Mobile SSO • Android Mobile SSO • Windows Kerberos Authentication (SSO for Windows 10) • Certificate Authentication (SSO for Windows 10 and Mac OS) • One additional Authentication adapter for MFA (includes VMware Verify)	Identity and Access Management	Joint	
3.19	Setup of one Network Range for an Authentication Policy	Identity and Access Management	Joint	
3.20	Setup of one Application Specific custom Authentication Policy	Identity and Access Management	Joint	
Productivity Applications				
3.21	Configuration of Personal Information Management (email, contacts, calendar)	VMware Mobile Email Management Guide	Joint	Integration with Customer email solution
Step 3: Deploy				
3.22	Define Enrollment/Registration Strategy for new devices	Enrollment Strategy	Joint	Defined enrollment methodology
3.23	Assist with enrolling up to 5 devices for identified device types	VMware Platform Guide	Joint	Successfully enrolled devices
Phase 4 (Close)				
4.1	Implement Monitoring and Maintenance		Customer	

LEARN MORE

Visit *vmware.com/services*.

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
4.2	Customer Support Transition	VMware delivers software related services completion materials and contact information for support/Customer Support Representative.	VMware	Transition to support meeting
4.3	Customer receives Customer Acceptance Form		VMware	

Integration Unit Valuation Matrix

UNITS	INTEGRATION TYPE	COMMENTS
1	• Each Additional Authentication Method • Each Standard Application (excludes Office 365)	Standard Enterprise Web Applications: These commonly used enterprise web applications can be configured using integration units. These applications have been thoroughly tested with Workspace ONE Access. The list, which is subject to continuous updates can be found here. The client is required to work independently with the service provider to provide VMware with all required integration details or SAML meta-data.
2	• Each Non-Standard Application	Excludes Office 365
3	• Each Additional VDI Integration: Citrix, Horizon View, Horizon Cloud • ThinApp Integration • Office 365	Office 365 Integration refers to direct federation with Workspace ONE
4	• Workspace ONE as a Trusted IDP for a Third party IDP • Native Application One Touch SSO Integration	With testing for up to 3 applications

This service must be delivered and accepted within the first 12 months of purchase, or the service will be forfeited. Pricing for this service excludes travel and other expenses. For detailed pricing, contact your local VMware representative.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.