VMware Workspace ONE Deployment – Advanced

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-WOA-DEP

VA-PS-ELA-WOA-DEP

WDS-WOADA-1TCT0-C1S

WDS-WOADA-1TCT0-A1S

WDM-WOADA-1TCT0-C1S

WDM-WOADA-1TCT0-A1S

WDP-WOADA-1TCT0-C1S

WDP-WOADA-1TCT0-A1S

Service Overview

This service provides for technical support related to the VMware AirWatch® 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.

VMware will provide implementation services for one (1) of the following options. Please review the associated Appendix for the respective service for additional details.

A. Workspace ONE Deployment - Advanced – General

B. Workspace ONE Deployment - Advanced – Windows 10 Jump Start

Estimated Schedule

The Professional Service typically takes 5 - 7 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.

APPENDIX A – Workspace ONE Deployment – Advanced - General

Service Overview

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, VPP application
- VMware Unified Access Gateway™ integration (Content, Tunnel, Browsing)
- Mobile Device Management enrollment strategy
- Advanced Desktop Management (scripting, product provisioning, desktop/win 32 app management, Win10 enterprise policies) for Mac and Windows devices.

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 or AirWatch Secure Email Gateway on Unified Access Gateway).
5. 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.
6. Procurement and installation of hardware for any components that will be installed on-premises is the responsibility of the Customer. VMware may provide recommendations.
7. Configuration of software other than VMware is the responsibility of the customer.

8. 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.
9. 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
10. 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
11. Native Application On-Touch Single Sign-On 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.
12. VMware cannot guarantee that individual third party SAML endpoints will integrate successfully with Workspace ONE Access given unforeseen Customer or service configurations or limitations.
13. Workspace ONE Access for Application Catalog will be implemented with Workspace One licensing.
14. Customer-specific customization for Workspace ONE Access is out-of-scope.
15. For any Windows 10 functionality not included in the Workspace One product that the customer wants to include using scripts, it is the responsibility of the customer to provide these scripts for execution through Workspace One.
16. For any internal Windows 10 applications, it is the responsibility of the customer to provide the configuration necessary to install the applications. This includes the

installation commands, uninstallation commands, and criteria for when to call the installation complete on devices.

17. Includes High Availability for VMware (Device Services, Console, AirWatch Secure Email Gateway v2 or AirWatch Secure Email Gateway on Unified Access Gateway, Unified Access Gateway, VMware AirWatch® Cloud Connector™, Email 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 DR 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.

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	
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	Hardware sizing and architecture
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	Customer action items	VMware	

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	requirements for Phase 3 (Execute)			
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	Stage required OVA files		Customer	If Applicable
2.10	Configure networking/firewall and service accounts for integration		Customer	Networking rules provisioned
2.11	Complete and return Pre-Installation Requirements Worksheet	Installation Pre-Requisites	Customer	
2.12	Send Design and Implementation doc for review and customer sign off	Design and Implementation doc and Plan Phase Completion Acknowledgment form	VMware	Scope of project cannot be modified without agreed change control
2.13	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 AirWatch 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 VMware Secure Email Gateway on VMware Unified Access Gateway, or		VMware	

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	Configuration of PowerShell			
3.6	Installation of Email Notification Service v2 (ENS v2) server (if applicable)		VMware	If using VMware Boxer™
3.7	Installation of Unified Access Gateway (Content, Tunnel, Browsing)		VMware	
Step 2: Configuration				
AirWatch Enterprise Mobility Management				
3.8	Configure Organizational Group structure (up to 5)		Joint	
3.9	Register email domain for auto-discovery		Joint	
3.10	Assistance configuring Directory Services integration: • Assist with creating up to five (5) users • Assist with creating up to 5 administrators • Assist with adding one user group		Joint	
3.11	Assist with creating one (1) of each desired profiles for up to three (3) device Operating Systems		Joint	Profiles may be limited based on device operating system
3.12	Assist with creating up to three (3) 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.,) • Email Compliance Policy (i.e., Unmanaged Devices, Compromised		Joint	

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	Devices, Encryption, etc.) • Privacy Policy (i.e., Collect GPS Data, Allow Full Wipe, etc.) • Terms of Use (i.e., Platforms, Geographies, etc.)			
3.13	Assist with configuration of App Wrapping/SDK	VMware SDK Technical Implementation Guide	Joint	
3.14	Configure Data Loss Prevention • Application Containerization Controls • "Open in" Controls • Email Attachment Management • Authentication • Single Sign-on • Integrated Authentication • Compromised protection • Network Access Control	Data Loss Prevention	Joint	Configuration of DLP policies
3.15	Assist with configuring Telecom plans and settings	VMware Telecom Guide	Joint	Configuration of Telecom plans and policies
3.16	Windows 10 Management: • Work Access Enrollment • Azure AD Enrollment • Agent Enrollment • Integration with Microsoft Business Store • Bulk Provisioning • Out of Box Enrollment: Dell Factory Provisioning or Windows Auto-Pilot in conjunction with Azure AD* • Silent, script-based enrollment via a GPO	Windows Desktop Management	Joint	Purchase of Professional Add-On is required for additional / Professional Windows 10 configuration *Configured in conjunction with Dell Command suite

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	• Assist with installation of up to a total of 3 internal applications (.exe – 3 units, zip – 2 units, .msi – 5 units) • 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, Dell OEM Updates*, Dell BIOS Configuration* • Assist with the distribution and execution of up to two client scripts from the Workspace One UEM console • Configuration of up to 5 CSPs via VMware Policy Builder • Assist with up to two Baselines configuration			
3.17	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, Zero-touch enrollment using DEP, Workspace ONE UEM and 3rd party cloud-based Directory that supports LDAP*, Assist with implementing bootstrapping for macOS device	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 * It is customer's responsibility to provide the scripts

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	enrollment using DEPNotify ** • 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 – 4 units, pkg– 3 units, mpkg – 3 units • 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, Kernel Extension Policy, Privacy Preferences, Proxies, Mobility, Managed Domains • Integration with Apple Business Manager • Assist with the distribution and execution of up to five client scripts from the Workspace One UEM console			for DEP enrollment with the cloud-based directory ** The pkg package for the bootstrapping has to be owned by customer. It is customer's responsibility to create/customize the package. If customer chooses other 3rd party utility instead of DEPNotify, we cannot guarantee it would work.

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
3.18	Assist with installation of up to three internal applications using the Software Distribution feature		Joint	
3.19	Assist with the distribution and execution of up to three client scripts from the AirWatch console		Joint	If Associated Licenses are purchased
Workspace ONE Access and Unified Application Catalog				
3.20	Complete Workspace ONE Access Configuration: • Sync with Active Directory users and groups • Configure the Unified Application Catalog. • Enable User Active Directory Password change • Integration with Workspace ONE UEM (AirWatch Compliance)	Identity and Access Management	Joint	Integration with Customer's endpoints for single sign-on
3.21	Configure the following for Application Management functionality: • Internal Application (one per device type) • Web Application (one per device type) • App Store integration		Joint	Configuration of application management policies
3.22	Assist with setup, association, and installation of Volume Purchase Program applications (sToken or License-Based). This will include: • Upload of sToken/redemption codes		Joint	Configuration of Volume Purchase Program applications

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	• 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			
3.23	Assist with SAML Integration of the following: • Workspace ONE UEM Admin Authentication • Workspace ONE UEM User Authentication • One Standard SAML Application • 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.	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.
3.24	Assist with VDI Integration of one of the following: • VMware Horizon® View™ • Horizon Cloud Hosted • Horizon Cloud on Azure • Citrix Xenapps and Xendesktops	Identity and Access Management	Joint	
3.25	Configure the following Authentication Methods: • Directory • iOS Mobile SSO • Android Mobile SSO • Windows Kerberos Authentication (SSO for Windows 10)	Identity and Access Management	Joint	

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	• Certificate Authentication (SSO for Windows 10 and Mac OS) • One additional Authentication adapter for MFA (includes VMware Verify)			
3.26	Setup of one Network Range for an Authentication Policy	Identity and Access Management	Joint	
3.27	Setup of one Application Specific custom Authentication Policy	Identity and Access Management	Joint	
Productivity Applications				
3.28	Configuration of Personal Information Management (email, contacts, calendar)		Joint	Integration with Customer email solution
3.29	VMware Tunnel™ configuration		Joint	
3.30	VMware Browser™ configuration		Joint	Configuration of VMware Browser tunneling
3.31	Configuration of Content: • Content Repository integration • Editing and Annotation • Personal Content • VMware Workspace ONE® Content Sync		Joint	Configuration may be limited by Customer licensing
Step 3: Deploy				
3.32	Define Enrollment/Registration Strategy for new devices	Enrollment Strategy	Joint	Defined enrollment methodology
3.33	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	
4.2	Customer Support Transition	VMware delivers software related services completion materials and contact information for support/CSR.	VMware	Transition to support meeting

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
4.3	Customer receives CAF		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

APPENDIX B – Workspace ONE Deployment – Advanced – Windows 10 Jumpstart

Service Overview

This service provides for technical support related to the VMware AirWatch ("VMware") Enterprise Mobility Management (EMM) and Workspace ONE offerings as set out below in the services description (the "Services" or Professional Services"). The Workspace ONE solution allows customers to activate, configure, and manage devices and user access.

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, and 4) Close.

The implementation scope includes:

- Review of associated pre-requisites
- Implementation of AirWatch Enterprise Mobility Management servers
- Implementation of VMware gateway servers
- VMware Workspace ONE Access installation/configuration
- Unified Application Catalog and Launcher
- Directory Services Integration
- Security policies – enrollment restrictions, compliance policies, privacy policies, terms of use
- Application management – public and internal
- Unified Access Gateway integration (Tunnel)
- Enrollment strategy
- Advanced Desktop Management (scripting, product provisioning, desktop/win 32 app management, Win10 enterprise policies) for Mac and Windows devices.

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 assist with the configurations required to manage Window 10 devices. Assistance with the configuration required to manage any other device types/operating systems (iOS, Android, Chrome OS, or Mac) may require the purchase of additional services. Rugged Windows Mobile/CE devices and printers are out-of-scope. Any additional device roll-out beyond the pilot devices mentioned below are out-of-scope.
3. VMware will assist with the integration of only one corporate e-mail infrastructure for Email Management integration.
4. 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.
5. Procurement and installation of hardware for any components that will be installed on-premises is the responsibility of the Customer. VMware may provide recommendations.

6. Configuration of software other than VMware is the responsibility of the customer.
7. 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.
8. 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
9. 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
10. 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.
11. VMware cannot guarantee that individual third party SAML endpoints will integrate successfully with Workspace ONE Access given unforeseen Customer or service configurations limitations.
12. Workspace ONE Access for App Catalog will be implemented with Workspace ONE licensing.
13. Customer-specific customization for Workspace ONE Access is out-of-scope.
14. For any Windows 10 functionality not included in the Workspace ONE product that the customer wants to include using scripts, it is the responsibility of the customer to provide these scripts for execution through Workspace ONE.
15. For any internal Windows 10 applications, it is the responsibility of the customer to provide the configuration necessary to install the applications. This includes the

installation commands, uninstallation commands, and criteria for when to call the installation complete on devices.

16. Includes High Availability for VMware (Device Services, Console, Unified Access Gateway, Airwatch Cloud Connector, and Workspace ONE Access) for up to 16 servers.
17. Installation of Disaster Recovery (DR) is out-of-scope. One can purchase the associated service offering to incorporate DR into the scope of a deployment.
18. 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.
19. Review of the console will be provided throughout the configuration; however formal training is out-of-scope.
20. Implementation of derived credentials is out-of-scope.
21. 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.
22. Services or products that have been deprecated or reached end of life are out-of-scope.
23. Certain features may require the purchase of a Workspace ONE Deployment Add-On bundle. Please contact your VMware representative for further information.
24. Pre-requisites must be completed for all installation components before any installation activities will be performed.
25. 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.
26. All work will be delivered remotely via screen-share. On-site travel is out-of-scope.
27. All work, documentation and deliverables will be conducted during VMware local business hours and will be provided in English.
28. Any feature not listed in Services Deliverables is out of scope, unless discussed and agreed to with the Product Deployment Team prior to purchase.
29. 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.
30. 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.
31. 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.

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	
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	Hardware sizing and architecture
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	

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
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	Stage required OVA files		Customer	If Applicable
2.10	Configure networking/firewall and service accounts for integration		Customer	Networking rules provisioned
2.11	Complete and return Pre-Installation Requirements Worksheet	Installation Pre-Requisites	Customer	
2.12	Send Design and Implementation doc for review and customer sign off	Design and Implementation doc and Plan Phase Completion Acknowledgment form	VMware	Scope of project cannot be modified without agreed change control
2.13	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 AirWatch 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 VMware Secure Email Gateway on Unified Access Gateway, or Configuration of PowerShell		VMware	

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
3.6	Installation of Email Notification Service v2 (ENS v2) server (if applicable)		VMware	If using VMware Boxer
3.7	Installation of Unified Access Gateway (Content, Tunnel, Browsing)		VMware	
Step 2: Configuration				
AirWatch Enterprise Mobility Management				
3.8	Configure Organizational Group structure (up to 5)		Joint	
3.9	Register email domain for auto-discovery		Joint	
3.10	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	
3.11	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
3.12	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.,) • Email Compliance Policy (i.e., Unmanaged Devices, Compromised Devices, Encryption, etc.)		Joint	

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	• Privacy Policy (i.e., Collect GPS Data, Allow Full Wipe, etc.) • Terms of Use (i.e., Platforms, Geographies, etc.)			
3.13	Assist with configuration of App Wrapping/SDK	VMware SDK Technical Implementation Guide	Joint	
3.14	Configure Data Loss Prevention • Application Containerization Controls • "Open in" Controls • Email Attachment Management • Authentication • Single Sign-on • Integrated Authentication • Compromised protection • Network Access Control	Data Loss Prevention	Joint	Configuration of Data Loss Prevention policies
3.15	Assist with configuring Telecom plans and settings	VMware Telecom Guide	Joint	Configuration of Telecom plans and policies
3.16	• Windows 10 Management: • Work Access Enrollment • Azure Active Directory Enrollment • Agent Enrollment • Integration with Microsoft Business Store • Bulk Provisioning • Out of Box Enrollment: Dell Factory Provisioning or Windows Auto-Pilot in conjunction with Azure Active Directory* • Silent, script-based enrollment via a GPO	Windows Desktop Management	Joint	Purchase of Professional Add-On is required for additional / Professional Windows 10 configuration *Configured in conjunction with Dell Command suite

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	• Assist with installation of up to a total of 3 internal applications (.exe – 3 units, zip – 2 units, .msi – 5 units) • 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, Dell OEM Updates*, Dell BIOS Configuration* • Assist with the distribution and execution of up to two client scripts from the Workspace One UEM console • Configuration of up to 5 CSPs via VMware Policy Builder • Assist with up to two Baselines configuration			
3.17	• 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, Zero-touch enrollment using DEP, Workspace ONE UEM and 3rd party cloud-based Directory that supports LDAP*, Assist with implementing bootstrapping for	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 * It is customer's responsibility to

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	macOS device enrollment using DEPNotify ** • 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 – 4 units, pkg– 3 units, mpkg – 3 units • 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 & Privacy, Disk Encryption, Login Items, Login Window, Energy Saver, Time Machine, Finder, Accessibility, Printing, AirPlay Mirroring, AirPrint, Firewall, Firmware, Custom Attributes, Custom Settings, Kernel Extension Policy, Privacy Preferences, Proxies, Mobility, Managed Domains • Integration with Apple Business Manager • Assist with the distribution and execution of up to five client scripts from the Workspace One UEM console			provide the scripts for DEP enrollment with the cloud-based directory ** The pkg package for the bootstrapping has to be owned by customer. It is customer's responsibility to create/customize the package. If customer chooses other 3rd party utility instead of DEPNotify, we cannot guarantee it would work.

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
3.18	Assist with installation of up to three internal applications using the Software Distribution feature		Joint	
3.19	Assist with the distribution and execution of up to three client scripts from the AirWatch console		Joint	If Associated Licenses are purchased
Workspace ONE Access and Unified Application Catalog				
3.20	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
3.21	Configure the following for Application Management functionality: • Internal Application (one per device type) • Web Application (one per device type) • App Store integration		Joint	Configuration of application management policies
3.22	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		Joint	Configuration of Volume Purchase Program applications

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	• Register using app catalog and automatic • Install application on same devices as Auto/On-Demand			
3.23	Assist with SAML Integration of the following: • Workspace ONE UEM Admin Authentication • Workspace ONE UEM User Authentication • One Standard SAML Application • 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.	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.
3.24	Assist with VDI Integration of one of the following: • Horizon View • Horizon Cloud Hosted • Horizon Cloud on Azure • Citrix Xenapps and Xendesktops	Identity and Access Management	Joint	
3.25	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)	Identity and Access Management	Joint	

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
	• One additional Authentication adapter for MFA (includes VMware Verify)			
3.26	Setup of one Network Range for an Authentication Policy	Identity and Access Management	Joint	
3.27	Setup of one Application Specific custom Authentication Policy	Identity and Access Management	Joint	
Productivity Applications				
3.28	Configuration of Personal Information Management (email, contacts, calendar)		Joint	Integration with Customer email solution
3.29	VMware Tunnel™ configuration		Joint	
3.30	VMware Browser configuration		Joint	Configuration of VMware Browser tunneling
3.31	Configuration of Content: • Content Repository integration • Editing and Annotation • Personal Content • VMware Workspace ONE® Content Sync		Joint	Configuration may be limited by Customer licensing
Step 3: Deploy				
3.32	Define Enrollment/Registration Strategy for new devices	Enrollment Strategy	Joint	Defined enrollment methodology
3.33	Assist with enrolling up to 5 devices for identified device types	VMware Platform Guide	Joint	Successfully enrolled devices

LEARN MORE

Visit *vmware.com/services*.

ID	DESCRIPTION	TOOL/DELIVERABLE	PRIMARY OWNER	COMMENTS
Phase 4 (Close)				
4.1	Implement Monitoring and Maintenance		Customer	
4.2	Customer Support Transition	VMware delivers software related services completion materials and contact information for support/Customer Support Rep.	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 apps

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.