Workspace One Standard & Advanced – MSP

This Schedule sets out the additional terms and conditions applicable to the Customer's use of the Workspace One Standard and Advanced – MSP Services (the "**Services**"), details of which are stipulated in the Product Quotation. This Schedule is an attachment to and forms an integral part of the Customer's Rogers for Business Agreement (the "**Agreement**") with Rogers. The Customer agrees to be bound by the terms and conditions set out in the Agreement, which include without limitation this attachment and any other attachments to the Agreement. Capitalized terms used but not defined herein shall have the meanings ascribed to them in the Agreement.

1. **Description.** The Workspace One Enterprise Mobility Management solution ("Workspace One"), supplied by Rogers to the Customer, is an intelligence-driven digital workspace platform that simply and securely delivers and manages any app on any device by integrating access and control, application management and multi-platform endpoint management. All editions of this service are available as a cloud service.

1.1. **Product Features.** Workspace One is available in 1, 2 and 3 year terms (some of these terms may have the option of monthly billing) and contain the features described in Table 1 below:

Table 1 – Product Features

		STANDARD EDITION	ADVANCED EDITION
INTELLIGENCE AND AUTOMATION			
Reports	Design custom reports with device, application and user data.	●	●
ACCESS MANAGEMENT			
Access Portal	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.	●	●
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.	●*	●*
One-touch SSO	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.	●*	●*
Conditional Access Control	Application access control policy to restrict access to applications based on user authentication strength, device platform, network range and application.	●*	●*
Identity Provider (IDP)	Ability to serve as the identity database for user accounts.	●*	●*
Mobile Email Management	Email server ActiveSync access control integration via direct server APIs PowerShell, Office 365 and Google Apps.	●*	●*
Multi-Factor Authentication	Multi-factor authentication for accessing applications with supporting mobile application VMware Verify.	●*	●*
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.		●

Unified Access Gateway (UAG)	Direct authentication requests to the appropriate server and discard unauthenticated requests to provide secure access to resources.	UAG Standard	UAG Advanced
SECURE APPS AND DATA			
Workspace ONE Web	An intuitive, secure browser that provides instant access to intranet sites and web apps. Includes the ability to lock devices into kiosk mode.		●
Workspace ONE Content	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.		●
Workspace ONE Boxer	Enable employees with a secure, better-than-native email experience with exciting productivity features for mail, calendar and contacts.		●
Workspace ONE Send	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.	●	●
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 MAM and AirWatch Software Development Kit (SDK).	●	●
App Wrapping	Ability to add security policies and management capabilities into an app that is already developed.		●
VMware Tunnel	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.		●
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.	●	●
Advanced Desktop Management	Includes custom scripting, BitLocker encryption, desktop / Win32 app management, Windows 10 Enterprise polices (incl. Credential Guard Device Guard).		●
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.	●	●
AirLift for Windows 10	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.	●	●

VMware Workspace ONE Advanced Remote Management	Remotely support and troubleshoot corporate-owned devices with advanced remote management and control tools.	Add-on	Add-on
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
Workspace ONE Portal Access	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

* 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.

1.2. **Licensing Models.** The Workspace One solution is available under either a per-device or a per-user licensing model.

1.2.1. **Hosting Models.**

i) The Workspace One solution includes a SaaS/Cloud-based hosting model, which includes standard hosting and basic support* as part of the base product offering.
(*) Please refer to Support Model in Section 5 below for additional information

ii) The Customer has the option to purchase a private, multi-tenant cloud hosting model, for the additional amount as set out in the MDM Pricing Table.

iii) The Customer has the option to purchase a private, dedicated cloud hosting model, for the additional amount as set out in the MDM Pricing Table.

iv) The Customer has the option to purchase a UAT Environment, which requires a private cloud hosting model, for the additional amount as set out in the MDM Pricing Table.

1.3. **Deployment/Professional Services.** Workspace One Deployment and Professional Services are mandatory for Workspace One licenses, and are subject to a separate fee, as the license fees do not include deployment services. These deployment services are provided by Rogers and are considered additional services – these are excluded from the licensing cost. Once purchased, Deployments and Professional Services are not refundable.

1.4. **Tech Support.** Rogers will be offering the end to end Tech Support. The Workspace One solution support model is fully described in Table 2 below:

Table 2 – Support Models

	FEATURES	ACCESS
myAirWatch	Knowledge Base	Full Access
	Forums	Full Access
	Documentation	Full Access
Reactive Support	Support Channels	12x5 Web/Phone
	Support Channels - emergencies	24x7 Phone

	Support Requests via email	Unlimited

2. **Terms and Conditions.**

2.1. **Minimum Number of Licenses.** There is a twenty-five (25) license minimum initial purchase, and the Customer must always maintain a minimum of 25 licenses.

2.2. **Additional Licenses.** If the Customer wishes to add additional licenses during the Term of the Customer's original license order (the "Original Order"), the applicable term for such additional licenses will be the same as the remaining Term of the Original Order, so that all additional licenses are co-terminus with the Original Order.

2.3. **Maximum Number of Devices.** No limit.

2.4. **Early Termination.** Workspace One licenses are purchased for a 1, 2 or 3 year Term. If Customer wants to cancel, upgrade or downgrade Workspace One Services at any time before the end of a 1, 2 or 3 year Term, Customer will pay an amount equal to 100% of the remaining monthly fees for the terminated service that would have been payable to the end of the Term (collectively, the "Termination Fees"). Customer acknowledges that the Termination Fees are a reasonable estimate of Roger's liquidated damages and represent consideration for the Services and are not a penalty. Any upfront payments are not refundable.

2.5. **End of the Service.** In the event that no renewal notice has been provided in writing by Customer to Rogers at least 30 days prior to the end of the applicable Term, the Services will expire at the end of the Service Term and Rogers shall have no liability to Customer as a result of the expiration of the Services.

2.6. **Currency Fluctuation.** The pricing set out in the Product Quotation is subject to change for subsequent Product Quotations based on fluctuations in the conversion rate between United States dollars and Canadian dollars (the "Exchange Rate") Rogers may make changes to the pricing set out in a Product Quotation at any time if the Exchange Rate fluctuates +/- 2% within 30 days of the date of the Product Quotation.

2.7. AirWatch Hosted Services Policy found at www.air-watch.com/download/eula/.

3. **Workspace One Standard- Deployment Scope.** Rogers "Professional Services Engagement Team" will provide implementation services associated with the deployment of **VMware Workspace One Standard** licenses. Rogers will configure & setup the VMware Workspace One (AirWatch) Cloud portal Hosted in VMware/Rogers Shared Dedicated SaaS environment. Rogers will be implementing/installing applicable on premise components (Servers) in the Customer's infrastructure (on premise).

Rogers will work on the configuration, setup, installation and incident based day to day support & management of the VMware Workspace One SaaS EMM solution, allowing Customer resources to focus on other IT related projects.

Rogers is pleased to provide Customer with the following Services outlined below. Rogers will set up, configure/deploy, install and provide integration of the VMware Workspace One (Standard license) applicable components to the Customer infrastructure end points nodes. The activities include the following:

i) Project Kick-Off Call & Meetings
ii) IT Policy → Strategy & Policy Design Workshop
iii) Assessment Optional Add-On service "on premise Components"
iv) Environment Assessment
v) Customer Readiness
vi) VMware Workspace One (Standard License) AirWatch Cloud Portal Setup & Configuration
vii) Installation & Deployment of VMware Workspace One (Standard License) applicable On-Premise components integration with Workspace One Cloud portal.
viii) Device Enrollment & Activation testing
ix) Knowledge Transfer & Questions & Answer session
x) Steady State Support Transition
xi) Project Acceptance & closing

3.1. **In-Scope Services:** Rogers agrees to provide the Customer with technical resources to perform the following Services:

i) Understanding of the existing EMM/MDM Polices & Profiles (if they exist)
ii) IT Policy Strategy & Policy Design Workshop; based on the Customer's requirements and functionalities available in VMware Workspace One Standard licenses.
iii) AirWatch Cloud portal configuration & setup
iv) Activation and Enrollment of up to 5 five devices (Android & iOS combined)
v) Knowledge transfer session of VMware Cloud portal & Integrated Components – session of up to three (3) hours.
vi) Setup & Deployment of VMware Workspace One Standard Licenses

3.2. **Environment Assessment**. Environment assessment will consist of the following:

i) Analyze the current Enterprise Managed Mobility (EMM/MDM) domain policies and configuration - if any.
ii) Analyze the Customer's environment for integration with VMware Workspace One (Standard License) for applicable on premise components.
iii) Create assessment reports that include the following information:
    a) Recommended Workspace One, AirWatch portal configuration.
    b) VMware Workspace One Deployment setup of on premise components, architecture, design integration topology with Customer infrastructure (e.g. Mail Server, Active Directory, Intranet Browsing)
    c) Recommended IT policies

3.3. **Customer Readiness.** Customer readiness stage will consist of the following:

i) Review of VMware Workspace One assessment report:
    a) Recommended Workspace One Profiles and IT policies.
    b) Applicable components integration with Customer's environment → architecture design
ii) Workspace One on premise Servers requirements
    a) Minimum hardware requirements
    b) Operating system and third-party software
    c) Network and firewall/proxy requirements
    d) Permissions (e.g. local server(s), database, etc.)
    e) Ensure software & hardware are meeting minimum requirements for the deployment and proper function of the VMware Solution.

3.4. **VMware Workspace One on Premise applicable Components - "Server" Installation on Customer Hardware.** Installation will consist of the following on premise applicable components:

i) Verify all requirements (software & hardware) discussed during pre-deployment phase are completed.
ii) Enterprise System Connector - ESC

3.5. **VMware Workspace One – AirWatch UEM Management Console Configuration/Setup.** The following settings will be configured on the AirWatch (UEM) Management Console:

i) First time user login setup to the UEM Console (VMware) - Demonstrate Console Navigation
ii) Assist in the creation and uploading of Apple's APNs certificates - for iOS devices
iii) Assist with the setup of the default Organization Groups - "Group ID"
iv) Configure the Active Directory Server Connection Integration – Enterprise System Integration
    a) Test & create up to 5 users
    b) Add a group (if any)
v) Complete the Identity Manager Setup/Sync with the VMware portal.
vi) Create up to two (2) custom roles
vii) Create up to two (2) administrator accounts
viii) Create up to two (2) groups and associate properties with group(s)
ix) Configure the SMTP settings
x) Register email Domain for auto-discovery – Device Enrollment.
xi) Review IT policies best practices and create up to two (2) custom IT policies
xii) Create up to (3) of each of the following profiles for each device type (OS):
    a) Passcode
    b) Email
    c) Wi-Fi

d) VPN
e) Restriction (i.e., Siri, Encrypted, Backup, etc.)

xiii) Create up to (3) of each of the following policies, one for each device (OS):
a) Enrollment Restriction Policy (i.e., # o device, Ownership, Type, etc.)
b) Compliance Policy (i.e., Comprised Status, Encryption, Application List, etc.).
c) Comprised Device
d) Privacy Policy (i.e., Collect GPS Data, Allow Full Wipe, etc.)
e) Terms of use (i.e., Platforms, Geographies, etc.)

xiv) Assist Customer in Branding the portal (i.e., color schemes & logo).

xv) Assist with loading & pushing of the following Application types (if applicable)
a) Public Application
b) Internal Application
c) VPP Application

xvi) Complete Identity Manager Setup/Sync with AirWatch portal.

3.6. **Acceptance Testing.**

i) Add up to five (5) users to the VMware portal and activate up to two (2) devices against each account
ii) Test configured settings and verify functionalities
iii) Verify the profiles and settings associated with the devices are properly applied (e.g. Email/ActiveSync, IT policy, software configuration, etc.)
iv) Verify the devices are able to receive and send email messages and synchronize PIM information (calendar and contacts)

3.7. **Knowledge Transfer.** The knowledge transfer session will take place immediately following the completion of post-installation tasks. The knowledge transfer consists of the following:

i) Customer questions
ii) If time permits, the following topics may be covered:
a) High-level overview of VMware Workspace One UEM Management Portal
b) Review of VMware portal settings
c) Review VMware Workspace One on-premise Components (Servers) services.
d) Provide some quick troubleshooting tips and tricks on the VMware portal.

3.8. **Assumptions.** Rogers has made the following assumptions while defining the Scope of Work, estimated effort and drawing up the work plan and schedules. Any variation in these assumptions may have a direct impact on the effort and cost.

i) Rogers will assist with an initial deployment of up to five devices (iOS & Android combined).
ii) Rogers will publish ActiveSync email profile via the VMware portal.
iii) EMM configurations and policy designs are the responsibility of the Customer. Rogers can only provide recommendations and assistance.
iv) Procurement and installation of Software (OS) and hardware (VMs) is the responsibility of Customer. Rogers will provide recommendations and assistance where needed/requested.
v) Customer specific customization of Identity Manager is out of scope.
vi) Rogers requires remote access to the Customer's environment to perform the installation and deployment of on premise components such as "Servers" to integrate with the VMware SaaS environment with collaboration of Customer IT administrator.
vii) The Environment assessment session may not exceed three (3) hours in duration.
viii) The Knowledge transfer session may not exceed four (4) hours in duration.
ix) Project will be completed within the following time frames:
a) Total time spent by Rogers may not exceed more than (5) business days in duration during regular business days and hours. Also, the project must be completed within fifteen (15) days of the Effective Date where both parties agree to initiate the project.
x) Rogers reserves the right to subcontract all or some portions of the Services outlined on this document.
xi) Rogers is not responsible for project or service delays that are outside of Rogers' control.
xii) Pre-requisites must be completed for all configuration or installation components before any installation activities are performed.
xiii) Rogers is not responsible for the manufacturers' "VMware" features that do not work or third party software bugs in hardware, software, equipment or any other property utilized in the Customer's environment.
xiv) Deployment is deemed to be completed upon any of the following:

a) Completion of all service deliverables – shown below
b) Up to a maximum of 12 weeks after the kick---off call has occurred
c) Deployment activities not implemented due to reasons outside of Rogers scope (*)

(*) Validity of the PS engagement is good for one year. If after the year the Service has not been deployed, the Customer will have to pay for the Service again. No refunds/credits are accepted by Rogers

4. **Deliverables & Project Acceptance.** Deliverables shall be limited to the items listed below and shall be deemed received upon written confirmation of receipt from the Customer. The Customer will provide Rogers with written confirmation of receipt within 5 business days of final delivery. If such confirmation is not received within 5 business days, the Deliverables will be deemed accepted.

Table 3: Deliverables & Project Acceptance

Title	Description	Format
Project Kick Off	Project planning session to review the project scope, define Customer's success criteria, & desired outcomes. Project Kick-Off Meeting: • Identify and document the services to be delivered, timelines, escalation process and change control plans. • Define and document Customer's success criteria • Review and document the Customer infrastructure and environment • Establish and document project schedule & milestones	Session
Network Architecture	Network Architecture and Documentation	PDF
Policy Design & Strategy Workshop	EMM Policy Design Workshop • Review Current EMM/MDM Policy - if any • Review VMware Workspace One UEM polices • Determine polices relevant to desired management and user experience • Define Policies to be implemented and move into implementation stage	Session
Policy Configurations	Configure policies as signed off by Customer including - but not limited - to: • Compliance policy • Configuration policy i.e. passcode • Wi-Fi Policies • Management Policies for iOS, Android Devices • Mobile Application Management policy for whitelisting/blacklisting of apps • Conditional access policy • Other policies as defined in the policy workshop	Session
Portal Configuration, Setup & Deployment of on premise components "Servers"	Configure Setup, deployment, & integration of VMware Workspace One with AirWatch portal : • Configuration & Setup of VMware Workshop One policies in AirWatch Portal. • Complete full setup as defined • Configure, Setup of on premise components "Servers" & its integration with VMware Workshop One Airwatch portal. • UAT testing	Platform/PDF
Device Enrollment	Multi OS Devices Activation/Enrollment	
Scope of Service & Support Workshop	Knowledge transfer session: • Review of Scope of Service & Support documentation • Portal login, policy changes, application push add a new user, additional items as required. • How to troubleshoot Level 1 support issues and when to escalate, etc.	Session
Project Sign Off	Customer Sign Off on Project Deliverables and Customer Satisfaction Survey/Feedback on delivery of the project	PDF
EMM Managed Services	EMM Managed Services, Admin Help Desk, 5 x 12, Monday to Friday, 7 am to 9 pm EST / 4 am to 6 pm PST. Support for Severity 1 issues is available 24x7.	Support

4.1. **Out-of-Scope Items:** The following items are out of scope to this project:
i) VMware ThinApp integration is out of scope of this deployment.

ii) Secure Email Gateway – SEG & PowerShell environment integration is out of scope of this deployment.
iii) Email Notification Service (ENS) for iOS devices environment integration is out of scope of this deployment.
iv) VMware Tunnel Service environment integration is out of scope of this deployment.
v) VMware Content Locker "Standard" environment integration is out of scope of this deployment.
vi) On-going upgrading, Service Pack and Maintenance Releases upgrades for on premise Server(s)
vii) Citrix XenApp environment integration is out of scope.
viii) Certificate usage for authentication is out of scope of this deployment. One can purchase the associated service offering to incorporate certificate usage for authentication into the scope of a deployment separately.
ix) High Availability (HA) and Disaster Recovery (DR) is out of scope of this deployment. One can purchase the associated service offering to incorporate HA/DR into the scope of a deployment separately.
x) The scope of the project cannot be delivered in phases
xi) Items not implemented as part of the initial deployment will be considered out of scope.
xii) Device migration support & end user support will be handled by Customer technical staff – not Rogers
xiii) VMware Workspace One on-premises Servers, Monitoring and Support – will be handled by Customer IT staff
xiv) Rogers/VMware cannot guarantee that individual third party SAML endpoints will integrate successfully with VMware Identity Manager given unforeseen customer or service configurations or limitations outside of our product.
xv) Any Power shell scripts, or security certificates required for this project
xvi) Microsoft & other required licenses.
xvii) VMware Workspace One Product Training
xviii) Additional training unless specified above
xix) Project Management
xx) And any other item not mentioned as part of the In-scope section of this document

4.2. **Location.** The VMware Workspace One essential Setup, Configuration and Deployment Implementation is to be completed telephonically and via remote/on-site access (*)
(*) If Customer requires work to be done on-premises, an additional cost to travel and expenses will be added to the quote

4.3. **Customer Responsibilities.** Rogers and the Customer are responsible for the success of this project by collaborating on the execution of the Workspace One deployment services. The Customer agrees to the following responsibilities:

i) Be solely responsible for completing a backup of all existing data, software, and programs on supported product(s) before receiving the Services (including telephone support). ROGERS WILL HAVE NO LIABILITY FOR LOSS OF OR RECOVERY OF DATA, PROGRAMS, OR LOSS OF USE OF SUPPORTED PRODUCT(S) OR NETWORKS.
ii) Provide required resources, who have a working knowledge of the enterprise components to be considered during this Project ("Technical Contacts"). Rogers may request that meetings be scheduled with Technical Contacts.
iii) Is solely responsible to provide any hardware, software (inclusive of software licenses), third party services or equipment which are required to use the MDM Services.
iv) Acknowledges that Rogers is not responsible for project or service delays that are outside of Rogers' control.
v) Customer may need to perform work to integrate their environment with VMware Workspace One including, but not limited to:
    a) Mail server
    b) Firewall/Proxy
    c) Microsoft SQL Server
    d) Active Directory
    e) SMTP
    f) Certificate Infrastructure
    g) VPN Infrastructure
vi) Customer is responsible for enabling the Exchange Active Sync internally.
vii) Customer is responsible for providing hardware and software for VMware Workspace One, AirWatch portal and components installed on Customer premises.

viii) Customer must purchase the license in additional to professional services for setup, configuration and installation of on premise components.
ix) Customer is responsible for acquiring Apple APN certificates for use with Apple devices.
x) Customer is responsible for creating a Gmail Account for setting up Android-for-Work on the AirWatch portal.

4.4. **Workspace One Advanced – Deployment Scope.** Rogers will set up, Configure/Deploy, Install and provide integration of the VMware Workspace One (Advance license) applicable components to the Customer infrastructure end points nodes. In addition to the activities provided under the Standard License Deployment above, the Advance License Deployment includes the following activities:

4.4.1. **In-Scope Services:**

i) VMware Workspace One (Advance License) AirWatch Cloud Portal Setup & Configuration
ii) Installation & Deployment of VMware Workspace One (Advance License) applicable On-Premise components integration with Workspace One Cloud portal.
iii) Rogers agrees to provide the Customer with technical resources to perform the same Services as provided for under the Standard License, with the following additional Services being in-scope:
iv) Exploring the Existing EMM/MDM Polices & Profiles (if exist)
v) IT Policy Strategy & Policy Design Workshop; based on the Customer's requirement and functionality available in VMware Workspace One Advance license.
vi) Activation and Enrollment of up to 5 five devices (Android, iOS) Setup & Deployment of VMware Workspace One Advance License applicable
vii) On-premise optional Add-On services "Components/Servers".

4.4.2. **Optional Add-on Services "on premise components".**

i) Customer has the option of purchasing the following Add-On service "on premise components" applicable to their setup.
ii) Add-on services are excluded and will require additional payment.
iii) **Enterprise System Connector** - ESC
iv) **Secure Email Gateway** – SEG if applicable
v) **PowerShell integration**, if Customer mail platform is in 0365 or Customer wants Direct integration of mail platform
vi) **Email Notification Service (ENS)** if applicable
vii) **VMware Tunnel** Service if applicable to Customer situation
viii) **VMware Content Locker** "Standard" service if applicable to Customer situation

Table 4: On Premise Connectors Install Summary

No.	Name of the on premise Connector	Require = Yes	Require = No
1	Enterprise System Connector – ESC		
2	Secure Email Gateway – SEG or PowerShell Integration		
3	Email Notification Service -ENS		
4	VMware Tunnel		
5	VMware Content Locker		

4.5. **Environmental Assessment:**

i) Analyze Customer's environment for integration with VMware Workspace One (Advance License) for applicable on premise components.

4.6. **VMware Workspace One on Premise applicable Component's "Server" Installation on Customer Hardware.**

Installation will consist of the following on premise applicable components:

i) Verify all requirements (software & hardware) discussed during pre-deployment phase are completed.
ii) Enterprise System Connector - ESC
iii) Secure Email Gateway – SEG
iv) PowerShell integration, if Customer mail platform is in 0365 or Customer wants Direct integration of mail platform
v) Email Notification Service if applicable
vi) VMware Tunnel Service if applicable to Customer situation

vii) VMware Content Locker “Standard” service if to Customer situation

4.7. **VMware Workspace One- AirWatch UEM Management Console Configuration/Setup:** The following settings will be configured on the AirWatch (UEM) Management Console:

i) If applicable to Customer situation – Assist in configuring AirWatch Container
ii) If applicable to Customer situation - Assist with Configuring AirWatch Application Security Settings & Policies:
iii) Authentication
iv) Single Sign on
v) Offline Access
vi) Comprised Protection
vii) AirWatch App Tunnel
viii) Data\Loss Prevention (DLP)

4.8. **Out-of-Scope Items:** All of the out-of-scope line items from the Standard License deployment are also out of scope in this Advanced License deployment, except for the following line items which are in scope and **do not** apply to the Advanced License deployment:

i) Secure Email Gateway – SEG & PowerShell environment integration is out of scope of this deployment.
ii) Email Notification Service (ENS) for iOS devices environment integration is out of scope of this deployment.
iii) VMware Tunnel Service environment integration is out of scope of this deployment.
iv) VMware Content Locker “Standard” environment integration is out of scope of this deployment.

4.9. **Customer Responsibilities.** In addition to all of the Customer Responsibilities from the Standard License deployment, which also apply to this Advanced License deployment, the following additional Customer Responsibility applies:

i) Customer is responsible for creating a **Gmail Account** for setting up Android-for-Work on the AirWatch portal.