Service Description

VMware Workspace ONE®

Last Updated: 01 July 2022

vmware

As used in this Service Description, "VMware", "we", or "us" means VMware, Inc., a Delaware corporation, if the billing address for your order is in the United States, and VMware International Unlimited Company, a company organized and existing under the laws of Ireland, if the billing address for your order is outside the United States. Terms not defined in this Service Description are defined in the VMware Cloud Service Offerings Terms of Service ("Terms of Service") or elsewhere in the Agreement (as defined in the Terms of Service).

The VMware Privacy Notices describe how personal information may be collected, used, shared or otherwise processed by VMware as a data controller. The VMware Privacy Notices are available at https://www.vmware.com/help/privacy.html.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Rev. 01 July 2022

1. Introduction

VMware Workspace ONE® (the "Service Offering") is a platform made up of a set of services designed to deliver and manage any application on any device. Depending on the edition of the Service Offering in your order, your entitlement may consist of VMware Workspace ONE® UEM for device management, an access policy and identity management service powered by Workspace ONE® Access™ (previously known as VMware Identity Manager), and several sub-service components. See the Workspace ONE edition comparison guides, at the URLs listed below, for descriptions of the features of the various editions of the Service Offering:

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/workspace-one/vmw-workspace-one-edition-comparison-guide.pdf

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/workspace-one/workspace-one-editions-comparison.pdf

1.1 Service Portals

Depending on the edition of the Service Offering in your order, you may have access to the following end user or service consoles:

- **Workspace ONE My Apps Portal** provides access to applications and data. Users can leverage single sign-on (SSO) for access to software as a service (SaaS) and web applications, to request access to applications, and to customize their portal.
- **Workspace ONE Access Console** provides organization administrators the ability to brand the portal, generate reports and audit logs, configure applications, and manage access policies, directory sync and authorization configuration.
- **AirWatch Self-Service Portal** provides the ability to manage devices and personal file data.
- **Workspace ONE UEM Admin Console** provides the ability to manage users and devices.
- **Workspace ONE Cloud Admin Hub** provides an administrative platform allowing organization administrators access to Hub Services, Workspace ONE UEM, Workspace ONE Access, and VMware Horizon® Cloud Service™ directly from a single console with SSO, to discover new use cases across those services, and access to reports and dashboards powered by VMware Workspace ONE® Intelligence™.
- **Horizon Cloud Administrator Console** allows an admin to manage virtual applications and desktops.

1.2 On-Premises Components

Depending on the edition of Workspace ONE in your order, your entitlement may include access to certain VMware Unified Access Gateway™ components which may need to be installed in your on-premises environment. You will also have access to the VMware Enterprise Systems Connector™ used by Workspace ONE UEM.

1.3 Definitions

For purposes of this Service Description:

"Device" means any client hardware, such as a mobile device, that enables installing and running of the Service Offering on that client hardware.

"Enrolled Device" means any Device that has the Service Offering installed and that is enrolled in the Workspace ONE UEM console, and is being managed by the Service Offering.

"Named User" means your employee, contractor, or Third-Party Agent who has been identified and authorized by you to use the Service Offering in accordance with the Agreement.

"**Seat**" means an entitlement for one Named User, if your order is on a per-Named User basis, or one Device, if your order is on a per-Device basis.

"**User**" is defined in the Terms of Service.

"Third-Party Agent" means a third party delivering information technology services to you pursuant to a written contract with you.

1.4 Entitlements

You may purchase an entitlement to the Service Offering on a per-Named User basis or on a per-Device basis. A single order may include both models.

Per Named User Entitlement

If you have purchased your entitlement to the Service Offering on a per-Named User basis, the Service Offering can be used on the agreed number of Devices for each Named User. You may not enroll more Devices than the number of Devices permitted to all Named Users in the aggregate. If you exceed that number, you must pay for the extra Enrolled Devices. Each Named User may also access the Service Offering using web-only access, which will not constitute use of a Device by that user.

If you have purchased your entitlement to the VMware Workspace Security™ offerings on a per-Named User basis, those entitlements can only be used on an endpoint device that is assigned to a Named User. For more information see the VMware Carbon Black Cloud™ offering Service Description at:
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-carbon-black-cloud-service-description.pdf.

Per Device Entitlement

If you have purchased your entitlement to the Service Offering on a per-Device basis:

- You cannot use the Service Offering to access the Workspace ONE web-based portal from an unmanaged Device (that is, Devices that were never enrolled, or that have been unenrolled, in the Workspace ONE UEM console).
- The Service Offering can only be used with Devices being managed by Workspace ONE (that is, enrolled in the Workspace ONE UEM console).

1.5 Service Operations Data

In connection with providing the Service Offering, VMware collects and processes information (such as configuration, performance, and log data) from VMware's software or systems hosting the Service Offering, and from the customer's systems, applications, and Devices that are used with the Service Offering. This information is processed to facilitate delivery of the Service Offering, including but not limited to (i) tracking entitlements, (ii) providing support, (iii) monitoring and ensuring the performance, integrity, and stability of the Service Offering's infrastructure, and (iv) preventing or addressing service or technical issues. To the extent any of this data is considered personal data under applicable data protection laws, the data will be treated in accordance with VMware's Privacy Notice, including the VMware Products and Services Notice, available at: https://www.vmware.com/help/privacy.html.

1.6 Usage Data

The Service Offering collects data (such as configuration, performance, and usage data) directly from the machines and/or Devices involved in the use of the Service Offering, for the purposes of improving VMware products and services, and your and your users' experiences, as more specifically described in VMware's Trust and Assurance Center, at: https://www.vmware.com/solutions/trustvmware/usage-data-programs.html.

To the extent that any of this data is considered personal data under applicable data protection laws, the data will be treated in accordance with the VMware Privacy Notice, found at: https://www.vmware.com/help/privacy.html.

In connection with the collection of usage data, VMware and its service providers use cookies. Detailed descriptions of the types of cookies we use can be found in the VMware Privacy Notice, and policies linked from that Privacy Notice, found at https://www.vmware.com/help/privacy.html. More information on how to choose whether to accept certain cookies used by VMware websites and solutions can be found from that link.

1.7 Technical Documentation

Documents outlining Key Concepts with usage examples, a "Getting Started" guide, and "How To" guides for key features are available at https://docs.vmware.com/en/VMware-Workspace-ONE/index.html

1.8 Legal Terms

Use of the Service Offering is subject to the VMware Cloud Service Offerings Terms of Service ("Terms of Service") available through a link at the main VMware end user terms landing page, at https://www.vmware.com/download/eula.html.

If you have migrated or converted from a VMware AirWatch® product to Workspace ONE (whether as part of a VMware migration offering, purchase of support and subscription services for Workspace ONE, or receipt of a Workspace ONE product entitlement from VMware), your use of Workspace ONE (including the applicable Workspace ONE UEM functionality you already use pursuant to the AirWatch terms) is subject to the Terms of Service, and any legacy terms governing the Workspace ONE UEM functionality will not apply.

1.9 Additional Information

Your subscription to the Service Offering includes an entitlement to use the Workspace ONE Access service. You may use this entitlement to Workspace ONE Access only with the Service Offering.

You acknowledge that the Service Offering includes VMware Workspace ONE® Verify, VMware's multi-factor authentication solution included in Workspace ONE Access that is powered by a third-party service provider. If you opt to use Workspace ONE Verify, VMware, its affiliates and its third-party service provider will have access to your personal information, including the name, phone number and email address of individual users. VMware, its affiliates and service provider will use the personal information collected through Workspace ONE Verify to provide the multi-factor authentication service.

Information collected by VMware may be transferred, stored and processed by VMware in the United States or in any other country where VMware or its affiliates or its service providers maintain facilities.

Each edition of the Service Offering includes entitlements to use different functionality and included components. For your selected edition of the Service Offering, you may only use the functionality for that edition, as specified in the Workspace ONE edition comparison guide referenced above.

When a Device communicates with the Service Offering console, it results in transmission of data to and from the Device. That transmission may result in additional charges from your carrier or service provider. VMWARE DISCLAIMS ANY LIABILITY FOR, AND IS NOT RESPONSIBLE FOR, ANY CARRIER OR INTERNET SERVICE PROVIDER DATA COSTS OR CHARGES YOU MAY INCUR IN CONNECTION WITH YOUR USE OF THE SERVICE OFFERING.

2. Service Operations

The following sections outline VMware's roles and responsibilities in delivering the Service Offering. While specific roles and responsibilities have also been identified as being owned by you, any roles or responsibilities not contained in this Service Description are either not provided with the Service Offering or are assumed to be your responsibility.

2.1 Service Provisioning

VMware will provide the following provisioning services:

- Creating service "tenants" for your organization in the Service Offering with default authentication and authorization policies for you to log on to the service.
- Creating the initial administrative user account in the administrator console using default administrator privileges and system preferences.
- Making available the on-premises components entitled to you as part of the Service Offering.

You will be responsible for the following provisioning services:

- Installing the VMware Enterprise Systems Connector™ and any other on-premises components entitled to you as part of the Service Offering in your on-premises environment and configuring it and them with the Service Offering.

- Connecting the services to your directories to get users and groups in the services you are provisioning, and setting the basic configuration of the services you wish to provision.
- Creating any applications required for the provisioned services.
- Entitling end user access to the provisioned apps and services.

2.2 Monitoring

VMware will provide the following services with respect to monitoring:

- Monitor availability of the Service Offering.

You are responsible for the following services with respect to monitoring:

- Monitoring availability of the on-premises components made available with your entitlement and installed as part of the service.

2.3 Incident and Problem Management

VMware will provide incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Availability of the Service Offering.

Status of the services can be viewed from the status page - https://status.workspaceone.com/

You are responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- The Enterprise Systems Connector and any other products you have installed and integrated with the Enterprise Systems Connector in your on-premises environment.
- Any other on-premises components you have installed, that are entitled to you as part of the Service Offering.

2.4 Change Management

VMware will provide the following change management services:

- Processes and procedures to maintain the health and availability of the Service Offering.
- Processes and procedures to release new code versions, hot fixes, and service packs related to the Service Offering and the Enterprise Systems Connector.

You are responsible for:

- Installing and upgrading to new releases of on-premises components entitled as part of the Service Offering for new features and bug fixes.
- Administration of the features in the services that are provided to you.

2.5 Security

The end-to-end security of the Service Offering is shared between VMware and you. VMware will provide security for the aspects of the Service Offering over which we, as between you and VMware, have sole physical, logical, and administrative level control. You are responsible for the

aspects of the Service Offering over which you, as between you and VMware, have administrative level access or control. The primary areas of responsibility between VMware and you are outlined below.

VMware will use commercially reasonable efforts to provide the following:

- **Information Security:** VMware will protect the information systems used to deliver the Service Offering over which it has sole administrative level control.
- **Network Security:** VMware will protect the networks containing its information systems up to the point where you have some control, permission, or access to modify your networks.
- **Security Monitoring:** VMware will monitor for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of the Service Offering over which it has sole administrative level control. This responsibility stops at any point where you have some control, permission, or access to modify an aspect of the Service Offering.
- **Patching and Vulnerability Management:** VMware will maintain the systems it uses to deliver the Service Offering, including the application of patches VMware deems critical for the target systems. VMware will perform routine vulnerability scans to surface critical risk areas for the systems it uses to deliver the Service Offering. Critical vulnerabilities will be addressed in a timely manner.

You are responsible for addressing the following:

- **Information Security:** You are responsible for ensuring adequate protection of the information systems, data, content, or applications that you deploy and/or access with the Service Offering. This includes, but is not limited to, any level of patching, security fixes, data encryption, access controls, roles and permissions granted to your internal, external, or third party users, etc.
- **Network Security:** You are responsible for the security of the networks over which you have administrative level control. This includes, but is not limited to, maintaining effective firewall rules, exposing communication ports that are only necessary to conduct business, locking down promiscuous access, etc.
- **Security Monitoring:** You are responsible for the detection, classification, and remediation of all security events that are isolated with your Service Offering account, associated with virtual machines, operating systems, applications, data or content surfaced through vulnerability scanning tools, or required for a compliance or certification program in which you are required to participate, and which are not serviced under another VMware security program.

Security Updates and Maintenance

Some updates to the Service Offering may be required for security or stability reasons, including for issues that may affect all customers of the Service Offering. In most cases, a customer (including customers who have enrolled in the managed hosting service, discussed below) will be given a minimum of five business days' notice for production updates, three business days' notice for trials, and one business day notice for UAT, in advance of the update. However, critical security vulnerabilities updates may be implemented by VMware with no advance notice.

2.6 Hosting Services

Managed Hosting Service

The Workspace ONE managed hosting service is designed to provide the functionality of the Workspace ONE cloud service offering but allows the customer to control its own upgrade cadence for major version upgrades of Workspace ONE UEM.

The Workspace ONE managed hosting service can be purchased by eligible customers. For the managed hosting service, you can specify the data center region where your environment will be hosted, based on the then-current list of available data center locations. If you move your Service Offering instance from one data center to another, you may be required to re-enroll your Devices. With the managed hosting service (but not with the shared environment hosting service), you can schedule timing of software updates to the environment based on a list of available time slots. Managed hosting customers may delay or forego upgrades (subject to the remaining portions of this Section 2.6), but support is limited to supported versions of the Workspace ONE UEM service, as specified in the then-current VMware product lifecycle matrix, found at:
https://lifecycle.vmware.com/

VMware requires customers to be on supported versions of Workspace ONE UEM to maintain the functional integrity and security posture of the hosted platform; supported versions of Workspace ONE UEM are eligible to get critical security and application updates on an on-going basis.

Managed hosting customers will receive notifications 60 days and 30 days prior to a version of the Service Offering going out of support, and will be requested to schedule an upgrade to a supported version. Customers who have not scheduled updates to remain compliant with the VMware product lifecycle matrix (found at https://lifecycle.vmware.com/) will be directed to upgrade before receiving further support from VMware. VMware reserves the right to schedule an upgrade for a managed hosting customer that is on an unsupported version, and the right to proceed with the upgrade of the customer's environment to a supported version if the customer does not comply with the requirement to schedule the upgrade.

Managed hosting customers are also subject to VMware's processes regarding critical security upgrades, which may be implemented with minimal or no advance notice, as more particularly described above in Section 2.5.

Perpetual + Hosting

Customers that purchased perpetual licenses of the on-premises Workspace ONE Standard and Workspace ONE Advanced software offerings (the "Software") prior to January 2018 and that also purchased an entitlement to hosting those perpetual licenses prior to January 2018 would have been eligible to elect either a shared hosting environment or a managed hosting service, as described above, allowing the customer to use the Software in a production environment via Internet-based consoles. These services are included here, for clarity, and are not available to customers who do not meet eligibility parameters (i.e., purchasing both perpetual license and a hosting entitlement prior to January 2018). A customer enrolled in shared environment hosting or managed service hosting cannot migrate from one environment to the other during a Subscription Term. If a customer wants to change its hosting service entitlement, it must contact iVMware to determine available migration options. VMware does not guarantee that migration will be possible.

Eligible Workspace ONE perpetual license customers (as described above) may choose to operate one or more components of Workspace ONE in their on-premises environment, with the remaining Workspace ONE functionality operating in the Workspace ONE hosted environment. However, customers may not mix on-premises installation and VMware hosting services for the same component of Workspace ONE; for example, all instances of the Workspace ONE UEM console must be all on-premises or all in the VMware hosted environment. You must not use the Software, through the Service Offering, in a way that exceeds your license entitlements (e.g., user/device limitations, applicable third-party terms, etc.) as set forth your Order, and as set forth in the VMware End User License Agreement ("EULA") and the VMware Product Guide. If there is a conflict between the (i) Terms of Service, on the one hand and (ii) the EULA and the VMware Product Guide, on the other hand, then the Terms of Service will control with respect to the Service Offering. You can access the EULA and the VMware Product Guide from the main VMware end user terms landing page, at:
https://www.vmware.com/download/eula.html.https://www.vmware.com/download/eula/product-guides.html

Standard VMware support and subscription services ("SnS") must be purchased for each Workspace ONE perpetual license that is hosted. SnS must be kept current at all times during your hosting service subscription term. The provisions of the VMware End User License Agreement, and the VMware Product Guide continue to apply to the perpetual licenses (e.g., user/device limitations, etc.).

Hosting Services – Latest Mode

Customers that purchased a "latest mode" license as part of our Subscription Upgrade Program will forego the ability to control updates and will be upgraded to the latest version as per our standard hosted offering.

2.7 VMware Workspace ONE® Intelligence™

VMware Workspace ONE® Intelligence™ is included in Workspace ONE Enterprise, and is available as an add-on offering to customers that have purchased entitlements to the Workspace ONE Standard or Workspace ONE Advanced editions, on both a Named User and Device basis.

Workspace ONE Intelligence aggregates and analyzes data coming from multiple resources such as Workspace ONE UEM (device data) and Workspace ONE Access (user activity). Workspace ONE Intelligence has the following features:

- **Dashboards** to give the customer visibility into its entire workspace, and the ability to create custom dashboards.
- **Automation** to automate processes across the customer's environment by defining rules that take actions based on a rich set of parameters, and to create policies that take automated remediation actions based on context.
- **Reporting** (through the custom reports functionality) to provide the customer with secure access to its data, and the ability to create, schedule and download custom reports.

Workspace ONE Intelligence collects data directly from the mobile apps and/or Devices using the Service Offering, such as configuration, performance, usage and consumption data, to provide the Service Offering. To the extent that any of this data is considered personal data under applicable data protection laws, the data will be treated in accordance with the VMware Privacy Notice, found at https://www.vmware.com/help/privacy.html.

VMware collects data regarding use of the Service Offering ("Customer Data") and of the customer applications ("App User Data"). VMware has the right to use, reproduce, and distribute Customer Data and App User Data when it is aggregated with other information and not specifically identifiable to you or to any app user to publish reports (either for the general public or VMware customers) on various metrics of interest, for particular industry sectors, or otherwise. VMware also has the right to use Customer Data and App User Data for data analysis, benchmarking, and machine learning to run models so VMware can derive insights and add intelligence to automation functionality (e.g., anomaly detection, forecasting, or predicting future data, as well as recommending possible corrective actions).

In connection with your use of Workspace ONE Intelligence, you may elect to integrate and use an offering from a partner in the VMware Workspace ONE® Trust Network (each a "TN Partner"). If you elect to use a solution provided by a TN Partner (a "TN Solution") in combination with Workspace ONE Intelligence, data collected by the TN Solution ("TN Solution Data") will be sent to Workspace ONE Intelligence to provide the Workspace ONE Intelligence offering. VMware may use any TN Solution Data to improve our products and services, and other purposes as set forth in the Terms of Service. The TN Solution is considered Third-Party Content under the Terms of Service, and any data transferred between the TN Partner and VMware will be governed by each party's respective agreement with you.

2.8 Hub Services

Hub Services is a set of services provided by Workspace ONE Access that adds functionality to Workspace ONE. Hub Services provides a customer's users with a single destination to access the customer's corporate resources. Hub Services includes the Workspace ONE applications catalog, notifications, and people search features. Any customer that has purchased an entitlement to Workspace ONE, either as an on-premises software offering or as a cloud service offering, can use Hub Services. Customers that have purchased an entitlement to the Workspace ONE cloud service offering can utilize Hub Services through their existing Workspace ONE Access tenant. Hub Services is included in all editions of the Workspace ONE cloud service offering.

2.9 Workspace ONE Assist

The VMware Workspace ONE® Assist™ is an add-on offering that enables IT and help desk staff to remotely access and troubleshoot a covered Device, in real time, to support productivity. Workspace ONE Assist gives you the ability to accept, pause, and end a remote session at any time, for enhanced privacy. A separate agent is required to be installed on a covered Device, through Workspace ONE UEM, on the Android, Windows 10, MacOS, and Windows CE operating systems. The capabilities are embedded in the Workspace ONE Intelligent Hub application on iOS.

2.10 Mobile Flows

The VMware Workspace ONE® mobile flows feature is included in Workspace ONE Enterprise (hosted), as well as in the Workspace ONE Intelligence add-on.

Workspace ONE mobile flows helps employees perform tasks across multiple business back-end systems from a single app (like VMware Workspace ONE® Intelligent Hub), eliminating the need for end users to visit multiple websites or apps while performing business tasks. For example, an employee who receives approval requests from Concur in Workspace ONE Intelligent Hub can

approve/deny them directly from Workspace ONE Intelligent Hub without having to go to the Concur application.

NOTE: VMware plans to discontinue support for Mobile Flows at the end of August 2022.

2.11 Workspace Security

The VMware Workspace Security™ offerings include VMware Carbon Black Cloud™ platform functionality in combination with Workspace ONE and VMware Horizon Service capabilities. For details on the VMware Carbon Black Cloud offering, see the Service Description at: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-carbon-black-cloud-service-description.pdf.

The Service Description for the VMware Horizon Service can be found at: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/vmw-horizon-service-description.pdf

2.12 VMware Horizon for Application Virtualization

Workspace ONE Enterprise includes an entitlement for Horizon Cloud Service for application virtualization. The Service Description for the Horizon Cloud Service can be found at: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/vmw-horizon-service-description.pdf

2.13 VMware Advanced Monitoring powered by ControlUp (Optional Add-On)

VMware Advanced Monitoring powered by ControlUp ("VMware Advanced Monitoring") is a third-party solution that delivers a real-time monitoring and visualization engine for VMware Horizon that allows customers to have a unified console for monitoring, triggers and alerts, troubleshooting, and automation for their Horizon deployment. VMware Advanced Monitoring allows customers to monitor their entire VMware Horizon environment, detect anomalies, and proactively solve issues across their deployment. VMware Advanced Monitoring has an analytics engine that provides insights and reporting on the data that is collected from the customer's environment. VMware Advanced Monitoring is hosted by ControlUp, Inc., from its data centers. VMware Advanced Monitoring can be purchased as an add-on for Workspace ONE Enterprise.

VMware Advanced Monitoring entitlements can be purchased for terms of one month, or for 1, 2, or 3 years, for a separate fee. The fee is based on the number of Seats purchased, and is payable monthly, annually, or prepaid. You must purchase an equivalent number of Seats for VMware Advanced Monitoring as you have purchased for the applicable Workspace ONE service.

VMware will provide support for the VMware Advanced Monitoring offering. The Terms of Service will govern a customer's use of the VMware Advanced Monitoring, and will supersede any terms presented to the customer during the deployment and sign-in process for VMware Advanced Monitoring. If a customer uses the offering in an on-premise environment, then the VMware standard end user license agreement will govern that use. Notwithstanding anything in the Terms of Service, and other than as expressly set forth in this Section 2.13, VMware provides the VMware Advanced Monitoring offering without any indemnification or warranty whatsoever.

2.14 Experience Workflows (Optional add-on)

The Experience Workflows™ for VMware Workspace ONE® powered by Boomi add-on is an optional feature available for Hub Services. Experience Workflows helps employees perform tasks across multiple business back-end systems from VMware Workspace ONE® Intelligent Hub, eliminating the need for end users to visit multiple websites or apps while performing business tasks. For example, an employee who receives approval requests from Concur in Workspace ONE Intelligent Hub, can approve/deny them directly from Workspace ONE Intelligent Hub without having to go to the Concur application.

2.15 Mobile Threat Defense (Optional add-on)

VMware Workspace ONE® Mobile Threat Defense™ is an optional feature that helps organizations ensure their mobile devices are secure by analyzing device, operating system, application, web, and network data to identify security threats and vulnerabilities. Threats are visible to IT and security administrators through the Workspace ONE Mobile Threat Defense administrative console, where administrators can also define policies to automatically take remediation actions against vulnerable Devices. Workspace ONE Mobile Threat Defense integrates with Workspace ONE UEM to synchronize Devices across services, and perform remediation actions, and with Workspace ONE Intelligence to synchronize threat events that can be used to generate dashboards and reports for a single pane of glass into the management and security of mobile endpoints.

Workspace ONE Mobile Threat Defense is hosted by Lookout, Inc. in the AWS US-West Region. Threat data captured from Devices that have activated the Workspace ONE Mobile Threat Defense service may be used by Lookout, Inc for security research and to improve its ability to detect new threats. You consent to such processing by Lookout, Inc. for its purposes. Refer to the Lookout Privacy Notice at: https://legaldocs.lookout.com/en/enterprise-privacy-policy.pdf, the Workspace ONE Privacy Disclosure at https://www.vmware.com/help/privacy/uem-privacy-disclosure.html, and end user disclosures within the mobile app.

Committed term subscriptions to Workspace ONE Mobile Threat Defense are available for 1, 2, and 3 year terms. The fee is based on the number of Devices that will leverage the service. Fees can be paid monthly or annually. There is a minimum initial purchase of 25 entitlements (one entitlement per Device).

VMware will provide support for the Workspace ONE Mobile Threat Defense offering. The Terms of Service will govern a customer's use of Workspace ONE Mobile Threat Defense and will supersede any terms presented to the customer during the deployment and sign-in process for Workspace ONE Mobile Threat Defense.

2.16 VMware SaaS App Management™ by BetterCloud (Optional add-on)

VMware SaaS App Management™ by BetterCloud add-on is an optional feature available in the United States only. VMware SaaS App Management delivers a SaaS Management Platform (SMP) that helps organizations discover, manage, and secure SaaS apps across their environments with a single platform, eliminating the need for IT admins to use multiple consoles. The service is hosted by BetterCloud, in its United States-based data center.

VMware SaaS App Management includes three modules which are sold as separate offerings: Discover, Manage, and Secure. Customers have access up to 10 apps integrations, which can be out-of-the-box integrations available in the BetterCloud Integration Center, or custom integrations through the BetterCloud API. The offering also includes an implementation service package delivered by the BetterCloud professional services team to help customers succefully onboard.

Entitlements to the offering are sold on a per end user account/per month and must be licensed for the customer's entire user base. The number of entitlements to the SaaS App Management offering must equal the number of Workspace ONE entitlements (whether per Named User or per Device). Support for VMware SaaS App Management can be obtained from VMware, or directly from BetterCloud through in-product live chat with BetterCloud, or through web form or email to support@bettercloud.com.

3. Business Operations

This section summarizes processes for ordering, renewing, and terminating a subsubscription to the Service Offering.

3.1 Ordering

Subscription Ordering

You may order the Service Offering on a per-Named User basis or on a per-Device basis. A single order may include both models. You may purchase a subscription for a 1, 2, 3, 4, or 5-year term. You are entitled to use the Service Offering for up to the number of Named Users or Devices for which you have paid the applicable fees. If you enroll more Devices in the UEM Console than the number of Devices for which you have paid the applicable fees, or have more Named Users than covered by the fees you have paid, VMware reserves its right to bill you for any additional fees you have incurred, as well as any other right VMware has under the Terms of Service.

- Initial orders must be a 25-seat minimum, unless you are purchasing Workspace ONE Express, in which case your initial order must be a 10-seat minimum.
- You will receive a storage allocation with your subscription. Please refer to the Edition comparison matrix for more details. Additional storage can be purchased separately.
- You can transfer Service Offering entitlements from one Named User to another Named User, or from one Device to another Device, within your organization so long as you do not exceed the number of Named Users or Devices for which you have paid the applicable fees.
- Upon renewal of your subscription, you will be billed for the total number of Enrolled Devices and/or Users within your tenant environments.
- For Workspace ONE Express, Standard, and Advanced editions, the Subscription Term and applicable billing period will begin within 24 hours of the date the Service Offering has been provisioned. For Workspace ONE Enterprise, we will provision the Service Offering within 14 days of the date VMware books your Order. VMware can elect to delay the start of the billing period at its discretion.

Entitlement utilization (to confirm compliance with your order) is measured as set forth below:

Service Offering Component	Per-Device Order Compliance Unit of Measure	Per-Named User Order Compliance Unit of Measure
Workspace ONE UEM	Enrolled Devices	Named Users are entitled to "N" Enrolled Devices*
Workspace ONE Assist	Enrolled Devices	Named Users are entitled to "N" Enrolled Devices*
Workspace ONE Intelligence	Enrolled Devices	Named Users are entitled to "N" Enrolled Devices*

* "N" means the number of Enrolled Devices permitted per Named User.

Subscription Upgrade Program

As stated in the VMware Product Guide, if you receive your entitlement to the Service Offering under the Subscription Upgrade Program for Workspace ONE you agree to (i) relinquish your entitlements to any corresponding perpetual licenses for the on-premises Workspace ONE product and (ii) complete your migration to the Service Offering, within 90 days after the effective date of the relevant agreement (e.g., an Enterprise License Agreement ("ELA"), or an amendment to an ELA, etc.). Failure to complete your migration within 90 days will result VMware ceasing support of your on-premises Workspace ONE instance, and you will have no further access to upgrade and installer files for your on-premises instance of Workspace ONE. After you have completed your migration to the Service Offering, you must not use any license keys related to those perpetual licenses for the on-premises Workspace ONE product, and VMware will invalidate those license keys.

3.2 Suspension and Re-Enablement

During the time a SID is suspended by VMware (as specified in the Terms of Service), VMware will restrict access to the Workspace ONE UEM Console for subsequent orchestration. VMware will retain SIDs with configurations and data intact until the issue is resolved or your Subscription Term expires or is terminated. SID re-enablement will be initiated promptly upon resolution of the account issue that led to suspension; access to the Service Offering and traffic across IP addresses will be restored.

3.3 Termination

Termination of a SID due to expiration, termination, cancellation, or any other cause will result in loss of access to the Workspace ONE UEM Console, discontinuation of software updates, account services, support, and deletion of such environments, configurations, and data. Data from a terminated SID will be deleted within 90 days of a deletion request.