

OMNISSA CLOUD SERVICES GUIDE

September 2025

1. TERMS APPLICABLE TO ALL OMNISSA CLOUD SERVICES

The terms set forth in this Cloud Services Guide apply to all Cloud Services, as provided in the Omnissa General Terms (“**General Terms**”) and the Cloud Services Exhibit to the General Terms (“**Cloud Exhibit**”), available at <https://omnissa.com/legal-center/>. Terms used but not defined in this Cloud Services Guide have the meanings set forth in the General Terms and the Cloud Exhibit. Individual services may have additional or differing provisions for any of the terms included in this Section 1; refer to the individual service entries in Section 2.

1.1 SERVICE OPERATIONS DATA

In connection with providing a Cloud Service, Omnissa collects and processes information (such as configuration, performance, and log data) from Omnissa’s software or systems hosting the Cloud Service, and from Customer’s systems, applications, and devices that are used with the Cloud Service. This information is processed to facilitate delivery of the Cloud Service, including but not limited to (i) tracking entitlements, (ii) providing support, (iii) monitoring and ensuring the performance, operational integrity, security, and stability of the Cloud Service’s infrastructure, (iv) preventing or addressing service or technical issues, (v) providing Cloud Service-specific notices to customers, and (vi) preventing fraud; and for other legitimate operational business purposes. To the extent any of this data is considered personal data under applicable data protection laws the data will be treated in accordance with the Omnissa Products and Services Notice available at: <https://www.omnissa.com/trust-center/#privacy-notices>

1.2 USAGE DATA

The Cloud Services collect data (such as configuration, performance, and usage data) directly from Omnissa’s software or systems hosting the Cloud Service, and from Customer’s systems, applications, and devices involved in the use of the Cloud Service, to improve Omnissa products and services, and Customer’s and its Users’ experiences, as more specifically described in Omnissa’s Trust Center at <https://omnissa.com/trust-center>. With respect to user-entered values within configuration object names (such as the machine names, host names or dashboard names) Customer should not name those systems using confidential or personal data.

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 Omnissa Products and Services Notice available at: <https://www.omnissa.com/omnissa-products-services-privacy-notice/>

1.3 AI FEATURES TERMS

The following terms (“**AI Features Terms**”) are hereby added to and become part of the Agreement as additional terms. Capitalized terms not defined in these AI Features Terms have the meanings given in the Agreement. The Agreement applies to the AI Features as part of the Cloud Service with the following modifications:

Use of AI Features

Omnissa AI Features are provided as added functionality available within the Cloud Services. Use of the AI Features is not required for Customer to access or utilize other components of the Cloud Services that do not incorporate AI functionality. Notwithstanding anything to the contrary in the

Agreement, Customer may opt out of any AI Features within the Cloud Services console or by submitting a support request.

Omnissa will publish a description of a new AI Feature at least two weeks in advance of its general availability. The description of the AI Features is available at: <https://docs.omnissa.com/bundle/OmnissaAIPolicy/page/aipolicy.html> and Customer may choose to subscribe to receive change notification. AI Features are labeled as such in the Cloud Services console.

Customer may submit Customer Content (including in the form of prompts or queries) to the AI Features ("**Inputs**") and receive outputs from the AI Features ("**Outputs**"). "**AI Features**" means large language models (LLMs) or other machine learning or artificial intelligence features of the Cloud Service made available for the Customer to use via the Cloud Service UI, API, partner's consoles, or other interfaces.

Training

Omnissa may use Customer Content, Input and Output solely to develop or improve its own machine learning models and artificial intelligence capabilities for the purpose of enhancing the Offerings, provided such Customer Content has been both de-identified and aggregated such that it no longer contains any information that could reasonably be used to identify the Customer, its devices or end user(s). For purposes of this provision, "de-identified" means that all direct identifiers have been removed or obscured, and "aggregated" means that the data has been combined with data from other Omnissa customers in a manner that prevents identification of the source. For these purposes (and without limiting Customer's other obligations with respect to Customer Content generally), such data is provided by Customer to Omnissa strictly "AS IS".

Intellectual Property

Except for Omnissa's express rights in the Agreement, as between the parties, Customer retains all intellectual property and other rights in Customer's Inputs and Outputs (excluding those Outputs that do not contain any Customer Content, such as Outputs referencing Omnissa Documentation).

Customer acknowledges that Outputs provided to Customer may be similar or identical to Outputs independently provided by Omnissa to others.

Infringement by Outputs

Due to the nature of the AI Features, Omnissa does not represent or warrant that (a) any Output does not incorporate or reflect third-party content or materials or (b) any Output will not infringe third-party intellectual property rights. Claims of intellectual property infringement or misappropriation by Outputs are not included in Omnissa indemnification obligations.

Output Limitations

Outputs are generated through machine learning processes and are not complete, or current by Omnissa. Customer should independently review and verify all Outputs as to appropriateness for any or all Customer use cases or applications. The warranty disclaimers and limitations of liability in the Agreement for the Services apply to the AI Features. AI Features may not support all languages supported by the in-scope Services(s).

Special Restrictions on Use of AI Features

Without limiting any restrictions on use of a Service set forth in the Agreement, Customer will not and will not permit anyone else to:

- use the AI Features or any Output to infringe any third-party rights,
- use the AI Features or any Output to develop, train or improve any AI or ML models (separate from authorized use of the Cloud Service under the Agreement),
- represent any Output as being approved or vetted by Omnissa,
- represent any Output as being an original work or a wholly human-generated work,
- use the AI Features for automated decision-making that has legal or similarly significant effects on individuals, unless it does so with adequate human review and in compliance with applicable laws, or
- use the AI Features for purposes or with effects that are discriminatory, harassing, harmful or unethical.

Third Party Model Providers

Omnissa may engage third party model providers as set forth in the applicable Sub-processor list, as may be updated from time to time. Customer agrees that third party model providers may use Inputs and Outputs as necessary to provide AI Features, comply with applicable laws, and enforce respective policies. You further agree to use AI Features in accordance with the policies of the applicable third-party model provider, as follows:

- Microsoft Azure OpenAI: <https://learn.microsoft.com/en-us/legal/cognitive-services/openai/code-of-conduct>. As a Sub-processor for this capability, Microsoft will temporarily store Input and Output, solely for debugging and to monitor for and prevent abusive or harmful uses or outputs of the service. Authorized Microsoft employees may review Input and Output that triggers Microsoft's automated systems to investigate and verify potential abuse.

Omnissa shall not use or permit any third-party to use Customer Content to train, fine-tune, or otherwise improve any third-party or publicly available LLMs.

1.4 COOKIES

In connection with the collection of usage data and service operations data, Omnissa and its service providers use cookies and other tracking technologies. Detailed descriptions of the types of cookies and other tracking technologies Omnissa uses can be found in the Omnissa Cookie Notice available at <https://www.omnissa.com/trust-center/#privacy-notice>. More information on how to choose whether to accept certain cookies used by Omnissa websites and solutions can also be found from that link.

1.5 CLOUD SERVICE OPERATIONS

The following outlines Omnissa's general roles and responsibilities in providing a Cloud Service. While specific roles and responsibilities have been identified as being owned by Customer, any roles or responsibilities not contained in this Cloud Services Guide are either not the duty of Omnissa or are assumed to be Customer's responsibility.

Service Provisioning

Omnissa will provide the following provisioning services. Specific Cloud Services may have different provisioning requirements or capabilities, as set forth in this Cloud Services Guide.

- Omnissa will create an instance of the Cloud Service for Customer.
- Omnissa will create a corresponding service account and send an email or other notification to the contact that Customer identified in the Order, inviting that contact to the newly created instance. A URL to access the Cloud Service will be provided within that notification.
- Omnissa will ensure that the identified contact can create additional user accounts for other users, as needed.

Customer's responsibilities include:

- Deploying and configuring data agents and the proxy to collect and route data into the Cloud Service as needed.
- Configuring the Cloud Service to gather metrics from cloud-based services (e.g., Amazon Web Services) as needed.

Incident and Problem Management

Omnissa will provide incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to infrastructure over which Omnissa has direct, administrative access and control, including servers and services used to provide the Cloud Service.

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

- Customer's account settings in the Cloud Service administrative management console.
- User-deployed and user-configured assets such as proxy agents.
- Anything else not under Omnissa's direct control and administration.

Change Management

Omnissa will provide the following change management elements:

- Processes and procedures to release new code version and bug fixes.

Customer is responsible for:

- Management of changes to Customer's tagging process, alert settings, dashboards, and other content.
- Administration of self-service features provided through the Cloud Service's system console and user portal, up to the highest permission levels granted to Customer.
- Changes in the data collection agents used.
- Cooperating with Omnissa when planned or emergency maintenance is required.

Security

Responsibility for the end-to-end security of the Cloud Service is shared between Omnissa and Customer. The primary areas of responsibility between Omnissa and Customer are outlined below.

Omnissa will use commercially reasonable efforts to implement reasonable and appropriate measures designed to help Customer secure Customer Content against accidental or unlawful loss, access, or disclosure, including the following:

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

Customer is responsible for addressing the following:

- Information Security: Customer is responsible for ensuring adequate protection of the content that Customer deploys and/or accesses with the Cloud Service. This includes, but is not limited to, any level of virtual machine patching, security fixes, data encryption, access controls, roles and permissions granted to Customer's internal, external, or third-party users, etc.
- Network Security: Customer is responsible for the security of the networks over which Customer has administrative level control. This includes, but is not limited to, maintaining effective firewall rules in all software-defined data centers ("**SDDCs**") that Customer deploys in a Cloud Service.
- Security Monitoring: Customer is responsible for the detection, classification, and remediation of all security events that are isolated with Customer's deployed SDDCs, 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 Customer is required to participate, and which are not serviced under another Omnissa security program.

1.6 DATA DELETION

Termination of Customer's entitlement due to expiration, termination, cancellation, or any other cause may result in loss of access to the Omnissa Cloud Service(s), software updates and downloads, account services, support, and tenant and in-scope service data deletion. Data is cycled from all systems within ninety (90) days of tenant deletion initiation. Tenant deletion initiation and associated in-scope service data deletion may be expedited upon request by submitting a non-technical support request.

1.7 OVERAGES

If Customer's use of a Cloud Service exceeds the usage limits set forth in the applicable Order, or if Customer continues to use the Cloud Service following expiration of the applicable Subscription Term, Omnissa may notify Customer of that excess usage. If Customer does not reduce its usage to within the applicable limits or purchase the required capacity within the period set forth in the notice,

Omnissa may (a) suspend Customer's access to the Cloud Service, in whole or in part, until the overage is remedied or additional entitlements are purchased, or (b) terminate the applicable Order (or entitlement) and/or the Agreement. Customer will in any event be obligated to pay Omnissa charges for the excess use. Omnissa shall have no liability for any suspension or termination made in accordance with this section, and such action shall not limit any other rights or remedies available to Omnissa under the Agreement or applicable law.

1.8 AUTHORIZATIONS, COMPLIANCE

The Omnissa Cloud Trust Center, at <https://omnissa.com/trust-center/>, provides information about security, privacy, compliance, and resiliency of Omnissa Cloud Services. The section on compliance programs lists Omnissa offerings that have achieved or are pursuing certification or authorization for specific programs (e.g., FedRAMP). If an offering is not listed, then the offering is not certified or authorized for the particular program, nor is certification or authorization being pursued.

1.9 SUBSCRIPTION UPGRADE PROGRAM

Customers that migrate from legacy Perpetual Licenses to a Cloud Service entitlement must cease use of the Perpetual Licenses within 90 days after the effective date of the applicable Order for the Cloud Service. After the 90-day period, customers that have migrated from Perpetual Licenses to a Cloud Service entitlement may not download/install upgrades or updates for the Perpetual Licenses and may no longer use support services associated with the Perpetual Licenses (including by submitting support tickets).

1.10 SUPPORTED VERSIONS

Omnissa requires Customer to be on supported versions of a Cloud Service to maintain the functional integrity, compliance, and security posture of the Cloud Service. Supported versions of the Cloud Service are eligible for continued support and availability of the Cloud Service and to receive critical security and application updates on an ongoing basis.

In instances where Customer's Cloud Service environment is not already subject to automatic updates in general, such as with respect to Preferred hosting environments, or otherwise will not automatically undergo a particular required update or migration, Omnissa will provide at least six months' notice prior to that Cloud Service offering becoming unavailable (end of General Availability) or going out of support (end of General Support) and will provide a means for Customers to schedule an upgrade or migration to a supported version.

Customers that are not compliant with the [Omnissa Lifecycle Matrix](#) will be required to come into compliance (e.g., upgrade or migrate Cloud Service environments that are not subject to automatic updates) for continued availability, functional integrity, and support from Omnissa. Omnissa reserves the right to schedule an update or migration for a customer that is on an unsupported version, and the right to proceed with the update or migration of a customer's environment to a supported version, if the customer does not comply with the requirement to schedule the update or migration.

From time to time, Omnissa may also require action from Customers in connection with an update, upgrade, or migration. Customers will be notified of this requirement at least 90 days in advance and must complete the required actions within the communicated timeframe (lasting no less than 90 days) for continued availability, functional integrity, and support from Omnissa.

Customers are also subject to Omnisia's processes regarding critical updates for security or legal compliance, which may be implemented with minimal or no advance notice.

2. CLOUD SERVICES

2.1. OMNISSA HORIZON®

Overview

Omnissa's Horizon® offering includes Omnisia Horizon® Cloud Service™ on Microsoft Azure, Amazon Workspaces Core, and the Omnisia-hosted Horizon® Control Plane with associated SaaS services which supports Horizon 8 and Horizon Cloud Service.

Note: If Customer's Horizon Service entitlement includes VMware vSphere Foundation for VDI licenses, Customer's use of those licenses is: (A) subject to the Foundation Agreement found at:

<https://www.broadcom.com/company/legal/licensing>, and (B) restricted to use for Virtual Desktop Infrastructure (VDI), solely for purposes of: (1) hosting: (i) a desktop virtual machine; (ii) a Microsoft Windows terminal services session running a valid Microsoft Windows license; (iii) remote desktop services hosts for the purpose of hosting sessions based desktops or remote applications; or (iv) associated desktop management and monitoring tools; and (2) running VMware products which are included in VMware vSphere Foundation for VDI. If there is any conflict or inconsistency between the terms of the foregoing subsection (B) and any terms in the above-referenced Foundation Agreement (including the SPD), the terms of the foregoing subsection (B) control and prevail.

If Customer's Horizon Service entitlement includes VMware vSphere Foundation for VDI licenses, Customer may only use those licenses with the Horizon Service offering.

If Customer needs support with respect to the VMware by Broadcom offerings in the nature of troubleshooting, diagnostics, and general assistance, Customer must raise a support ticket with Omnisia. If Customer needs support with respect to the VMware by Broadcom offerings for critical and highly complex issues, product bugs, advanced technical challenges, or complex technical troubleshooting, then Customer may, at its election, either: (i) raise a support ticket with Omnisia and Omnisia support will collaborate with Broadcom to provide the resolution, or (ii) raise a support ticket directly with Broadcom.

Specific Service Notes

Omnissa Horizon® Accelerator™ (optional add-on): The Omnisia Horizon® Accelerator™ service provides customers that have purchased a subscription to Horizon with on-going IT lifecycle services for Customer's Horizon virtual desktop environment, whether on-premises, in a public cloud environment, or in a hybrid cloud environment. Customer must have an active subscription to Horizon to purchase an entitlement to Horizon Accelerator, with a Subscription Term at least as long as the entitlement to Horizon Accelerator, Horizon Accelerator uses a hosted dashboard to provide Day 0 to Day 2 support, as well as on-going telemetry, intelligence, and support to deliver a managed desktop-as-a-service experience. Customer may not take possession of any software elements of the Horizon Accelerator service that are installed in Customer's own Horizon environment. Customer is not permitted to manage or operate the Horizon Accelerator service, nor

may Customer have any party other than Omnissa manage and operate the Horizon Accelerator service. The Horizon Accelerator service may store or access Customer information to provide the service. All support activities will be performed through restricted remote access granted by Customer or through guided online sessions. As of the date of this Cloud Services Guide, the Horizon Accelerator service is provided by a third party retained by Omnissa. Customers using Horizon Accelerator must raise all support requests directly to Omnissa; support requests can be initiated from the Horizon Accelerator dashboard or by filing a support case in Omnissa Customer Connect. The Horizon Accelerator Pro Desk will proactively engage customers as necessary. The Horizon Accelerator service will also include an optional onboarding service for Horizon Accelerator customers, at no additional cost.

Omnissa Access: Horizon includes Omnissa Access, hosted by Omnissa. Use of Omnissa Access within Horizon requires an Access connector, which can be installed and managed on a customer's virtual machine or on a utility server.

Omnissa Advanced Monitoring powered by ControlUp - Optional Add-On: Omnissa Advanced Monitoring powered by ControlUp is a third-party solution that delivers a real-time monitoring and visualization engine for Horizon that allows customers to have a unified console for monitoring, triggers and alerts, troubleshooting, and automation for their Horizon deployment. Omnissa Advanced Monitoring allows customers to monitor their entire Horizon environment, detect anomalies, and proactively solve issues across their deployment. Omnissa Advanced Monitoring has an analytics engine that provides insights and reporting on the data that is collected from a customer's environment. Omnissa Advanced Monitoring is hosted by ControlUp, Inc., from its data centers. Customer must purchase an equivalent number of seats for Omnissa Advanced Monitoring as Customer purchased for Horizon.

Omnissa will provide support for the Advanced Monitoring offering. The General Terms and the Cloud Exhibit govern Customer's use of the Advanced Monitoring offering and supersede any terms presented to Customer during the deployment and sign-in process for Omnissa Advanced Monitoring. If Customer uses the Advanced Monitoring service in an on-premises environment, then the General Terms and the Software Exhibit will govern that use. Notwithstanding anything in the General Terms, the Cloud Exhibit, and/or the Software Exhibit, and other than as expressly set forth in this Section 2.1, Omnissa provides the Omnissa Advanced Monitoring service without any indemnification or warranty whatsoever.

2.2. OMNISSA WORKSPACE ONE®

Overview

Omnissa Workspace ONE® is a platform made up of a set of cloud services designed to deliver and manage any application on any device. Depending on the edition of Workspace ONE that Customer licenses, Customer's entitlement may consist of Omnissa Workspace ONE® UEM™ for device management, an access policy and identity management service powered by Omnissa Access, and several sub-service components. Depending on the edition, the service may include access to certain Unified Access Gateway™ components which may need to be installed in Customer's on-premises environment. Customer will also have access to the Enterprise Systems Connector™. Customer may use the service for up to the number of Named Users or Devices for which Customer has paid the applicable fees.

Each edition of Workspace ONE includes entitlements to use different functionality and inclusions. For the selected edition of the service, Customer may only use the functionality entitled for that edition.

When a Device communicates with the Workspace ONE console, it results in transmission of data to and from the Device. That transmission may result in additional charges from Customer's carrier or service provider. OMNISSA DISCLAIMS ANY LIABILITY FOR, AND IS NOT RESPONSIBLE FOR, ANY CARRIER OR INTERNET SERVICE PROVIDER DATA COSTS OR CHARGES CUSTOMER MAY INCUR IN CONNECTION WITH ITS USE OF THE SERVICE.

Notwithstanding anything to the contrary in the General Terms, the Cloud Exhibit, and any Order, the following terms apply:

- For Workspace ONE Standard and Advanced editions, the Subscription Term and the applicable billing period will begin within twenty-four (24) hours after the date on which Customer's instance of the service has been provisioned.
- For Workspace ONE Enterprise, Omnisca will provision Customer's instance of the service within fourteen (14) days after the date Omnisca books the Order. Omnisca can elect to delay the start of the billing period at its discretion.

Definitions

For purposes of this Section 2.2, the following terms have the following meanings:

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

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

"Named User" means Customer's employee, contractor, or Third-Party Agent who has been identified and authorized by Customer to use Workspace ONE.

"Seat" means an entitlement for (i) one (1) Named User if the order is on a per-Named User basis, or (ii) one (1) Device if the Order is on a per-Device basis.

Service Notes

Entitlements

Customer may purchase an entitlement to Workspace ONE on a per-Named User basis or on a per-Device basis. A single order may include both models. Customer is entitled to use Workspace ONE for up to the number of Named Users or Devices for which Customer has paid the applicable fees. Customer can transfer Workspace ONE entitlements from one Named User to another Named User, or from one Device to another Device, within Customer's organization, as long as Customer does not exceed the number of Named Users or Devices for which Customer has paid the applicable fees. If Customer enrolls more Devices in the Workspace ONE UEM console than the number of Devices for which Customer has paid the applicable fees, or if Customer has more Named Users than are covered by the fees that Customer has paid, Omnisca reserves the right to bill Customer for any additional fees incurred, in addition to any other right Omnisca has under the Agreement.

Per Named User Entitlements

If Customer licenses Workspace ONE on a per-Named User basis, Customer may use the service for up to the number of Named Users for which Customer has paid the applicable license fees. Each

Named User may have a maximum of five (5) enrolled Devices (the "**Per Named User Device Restriction**") that are managed by the service.

Customer may not enroll more Devices than the number of Devices permitted to all Named Users in the aggregate. If Customer exceeds that number, Customer must pay for the extra Enrolled Devices. Each Named User may also access Workspace ONE using web-only access, which will not constitute use of a Device by that user.

Customer may also enroll Devices for staging purposes only ("**Staging Devices**"), meaning those devices have not yet been deployed to production. This is different than an inactive device that has been deployed to production. The Per Named Device Restriction noted above will not apply to Staging Devices, so long as those devices are not used as production devices. However, the total number of Staging Devices may not exceed (i) the total number of licensed Named User devices (Named User licenses x 5) **minus** (ii) the Named User devices active in the production environment. Example: Customer purchases 1,000 Named User licenses and therefore is entitled to enroll a maximum of 5,000 devices. If Customer has 700 Named Users enrolled and therefore is licensed for up to 3,500 Named User devices in production, Customer may only enroll 1,500 Staging Devices.

The Per User Device Restriction will continue to apply to devices in production. This means that each Named User may only have 5 devices enrolled at any given time in production. This restriction is not an aggregate restriction; rather, it is a restriction at the user level. Specifically, if one Named User enrolls only 4 devices, that does not entitle another Named User to enroll 6 devices.

Per Device Entitlements

If Customer has purchased entitlements to Workspace ONE on a per-Device basis:

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

Entitlement Utilization

Entitlement utilization (to confirm Customer's compliance with its purchased entitlements) is measured as set forth below. ("N" means the number of Enrolled Devices permitted per Named User)

Workspace ONE 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
Omnissa Intelligence	Enrolled Devices	Named Users are entitled to "N" Enrolled Devices

AirWatch®

If Customer has migrated or converted from an AirWatch® product to Workspace ONE (whether previously as part of a VMware migration offering, purchase of support and subscription services for Workspace ONE, or receipt of a Workspace ONE entitlement from VMware or from Omnisia), use of Workspace ONE (including the applicable Workspace ONE UEM functionality that Customer is using pursuant to the AirWatch terms) is subject to the Agreement, and any legacy terms governing the Workspace ONE UEM functionality will no longer apply.

Security Updates and Maintenance

Some updates to Workspace ONE may be required for security or stability reasons, including for issues that may affect all Users. In most cases, Omnisia will attempt to provide as much advance notice as possible. However, Omnisia reserves the right to push and implement security fixes, bug fixes and other critical patches with no advance notice.

Omnissa Access

A customer's subscription to Workspace ONE includes an entitlement to use the Omnisia Access offering. Customer may use this entitlement to Omnisia Access only with Workspace ONE. See Section 2.3 of this Cloud Services Guide for information on Omnisia Access.

Hub Services

Hub Services is a set of services that adds functionality to Workspace ONE. Hub Services provides Users with a single destination to access 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, can use Hub Services. Customers that have purchased an entitlement to the Workspace ONE cloud service can utilize Hub Services through their existing Omnisia Access tenant. Hub Services is included in all editions of the Workspace ONE cloud service.

Omnissa Workspace ONE® Verify™

Customer acknowledges that Workspace ONE includes Omnisia Workspace ONE® Verify™, Omnisia's multi-factor authentication solution included in Workspace ONE Access. If Customer elects to use Workspace ONE Verify, then Omnisia, its affiliates and its third-party service providers will have access to personal information, including the name, phone number and email address of individual Users. Omnisia, its affiliates, and its service providers will use the personal information collected through Workspace ONE Verify to provide the multi-factor authentication service.

Omnissa Intelligence

Omnissa Intelligence is available in all Workspace ONE UEM editions for basic reporting and data analytics purposes. Premium features may be accessed by purchasing other editions. Omnisia Intelligence monitors a customer's Devices and aggregates and analyzes data from the Devices. Omnisia Intelligence collects data directly from the mobile apps and/or Devices using Omnisia offerings (including but not limited to Workspace ONE UEM, Omnisia Intelligence SDK, Workspace ONE Experience Management, Horizon, Workspace ONE Intelligent Hub, Omnisia Access, Omnisia Unified Access Gateway, and Workspace ONE Mobile Threat Defense) such as configuration, performance, usage, and consumption data. 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 Omnissa Products and Services Notice available at: <https://www.omnissa.com/trust-center/#privacy-notice>.

Omnissa collects data regarding use of the service (“**Customer Data**”) and of the customer applications (“**App User Data**”). Omnissa 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 Customer or to any app user to publish reports (either for the general public or Omnissa customers) on various metrics of interest for particular industry sectors, or otherwise. Omnissa also has the right to use Customer Data and App User Data for data analysis, benchmarking, and machine learning to run models so Omnissa 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 Customer’s use of Omnissa Intelligence, Customer may elect to integrate and use an offering from a partner in the Omnissa Workspace ONE® Trust Network (each a “**TN Partner**”). If Customer elects to use a solution provided by a TN Partner (“**TN Solution**”) in combination with Intelligence, data collected by the TN Solution (“**TN Solution Data**”) will be sent to Omnissa Intelligence to provide the Omnissa Intelligence offering. Omnissa may use any TN Solution Data to improve its products and services, and for other purposes as set forth in the Agreement. The TN Solution is considered a Third-Party Offering under the Agreement, and any data transferred between the TN Partner and Omnissa will be governed by each party’s respective agreement with Customer.

Omnissa Horizon Cloud Service for Application Virtualization

Workspace ONE Enterprise includes an entitlement for the Horizon Cloud Service for application virtualization.

Workspace ONE Preferred Hosting and Deployment Ring Options

With the release of the new architecture with Workspace ONE UEM version 2406, the Workspace ONE dedicated hosting service can be purchased by eligible customers. The Workspace ONE Preferred Hosting service is designed to provide the functionality of the Workspace ONE cloud service and allows Customer to select a Deployment Ring (defined below) during which the customer will receive software version updates. Customers are not given any option to schedule timing of software and microservices updates or to delay their updates beyond their selected Deployment Ring.

With the release of the new architecture along with Workspace ONE UEM version 2406 all Preferred Hosting customers must opt into the following available deployment rings options (“**Deployment Ring**”):

- Ring 1 Preferred Latest: Any software updates of Workspace ONE UEM will be deployed first to Ring 1 as updates are available and progress through the existing CI/CD deployment structure (UAT>Prod), and
- Ring 2 Preferred Deferred: UAT environments will be updated approximately every 8 (eight) weeks with the latest available Workspace ONE UEM major version builds. Once a major version has baked-in UAT for 8 (eight) weeks, that build will be promoted to Production environments in this deployment ring.

Customers that purchased the managed hosting service prior to the release of the modern architecture with Workspace ONE UEM version 2406 were required to select one of the available

Deployment Rings no later than August 23, 2024. If Customer failed to select and communicate its selection to Omnisca by August 23, 2024, then by default the customer was placed in Ring 2 within the same data center region.

For the Preferred Hosting service, Customer can specify the data center region where its Workspace ONE instance will be hosted, based on the then-current list of available data center locations. If Customer moves its Workspace ONE instance from one data center to another, Customer may be required to re-enroll its Devices.

Preferred Hosting Updates and Support

Preferred Hosting customers will receive notifications sixty (60) days and thirty (30) days prior to a version of Workspace ONE going out of support and will be requested to schedule an upgrade to a supported version. Customers that have not scheduled updates to remain compliant with the Omnisca product lifecycle matrix will be required to upgrade for continued availability and support from Omnisca. Omnisca reserves the right to schedule an upgrade for a dedicated 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.

Perpetual + Hosting

Customers (i) that purchased perpetual licenses of the on-premises Workspace ONE Standard and Workspace ONE Advanced software offerings (the “**Software**”) prior to January 2018 and (ii) 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 dedicated 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 that 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 dedicated 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 Omnisca to determine available migration options. Omnisca 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 Omnisca hosting services for the same component of Workspace ONE; for example, all instances of the Workspace ONE UEM console must be either all on-premises or all in the Omnisca hosted environment. The customer must not use the Software, through the Workspace ONE service, in a way that exceeds the customer's license entitlements (e.g., user/device limitations, applicable third-party terms, etc.) as set forth in the applicable Order, and as set forth in the Agreement. If there is a conflict between the (i) Cloud Services Exhibit and this Cloud Services Guide on the one hand and (ii) the Software Exhibit and the Product Guide on the other hand, then the Cloud Services Exhibit and this Cloud Services Guide will control with respect to the service.

Standard Omnisca 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 the hosting service subscription term. The provisions of the General Terms, the Software Exhibit, and the Product Guide continue to apply to the perpetual licenses (e.g., user/device limitations, etc.).

Omnissa Workspace ONE® Accelerator™ – Optional Add-On

The Omnissa Workspace ONE® Accelerator™ service provides customers that have purchased a subscription to Workspace ONE with on-going IT lifecycle services for the customer's Workspace ONE environment, whether on-premises, in a public cloud environment, or in a hybrid cloud environment. Customer must have an active subscription to Workspace ONE to purchase an entitlement to Workspace ONE Accelerator, with a Subscription Term at least as long as the entitlement to Workspace ONE Accelerator. Workspace ONE Accelerator uses a hosted dashboard to provide Day 0 to Day 2 support, as well as on-going telemetry, intelligence, and support to deliver a unified endpoint, application, and access control management experience. Customer may not take possession of any software elements of the Workspace ONE Accelerator service that are installed in Customer's own Workspace ONE environment. Customer is not permitted to manage or operate the Workspace ONE Accelerator service, nor may Customer have any party other than Omnissa manage and operate the Workspace ONE Accelerator service. The Workspace ONE Accelerator service may store or access Customer information to provide the service. All support activities will be performed through restricted remote access granted by Customer or through guided online sessions. As of the date of this Cloud Services Guide, the Workspace ONE Accelerator service is provided by a third party retained by Omnissa. Customers using Workspace ONE Accelerator must raise all support requests directly to Omnissa; support requests can be initiated from the Workspace ONE Accelerator dashboard or by filing a support case in Omnissa Customer Connect. The Workspace ONE Accelerator Pro Desk will proactively engage customers as necessary. The Workspace ONE Accelerator service will also include an optional onboarding service for Workspace ONE Accelerator customers, at no additional cost.

Omnissa Workspace ONE® Tenancy Hierarchy™ – Optional Add-On

Omnissa Workspace ONE® Tenancy Hierarchy™ enables Customer to keep the multi-tenancy architecture of Workspace ONE when sub-organizations have different domains within Customer's Workspace ONE environment, by enabling Customer to procure Workspace ONE entitlements centrally, for sub-organizations under Customer's top level organizational group. Workspace ONE Tenant Hierarchy is only available in conjunction with the purchase of new Workspace ONE subscriptions, as there is no migration path for existing Workspace ONE deployments. Customer must pay a one-time set-up fee for the Workspace ONE environment where Workspace ONE Tenant Hierarchy will be deployed, as well as an annual maintenance fee for each covered subscription (*i.e.*, the subscriptions for all covered sub-organizations). The maintenance term must be coterminous with the covered subscription term. Workspace ONE Tenant Hierarchy supports any edition of Workspace ONE UEM and compatible add-on services.

Omnissa Workspace ONE® Assist™ – Optional Add-On

Omnissa Workspace ONE® Assist™ enables a customer's IT and help desk staff to remotely access and troubleshoot an enrolled Device, in real time, to support productivity. A separate agent is required to be installed on a covered Device, through Workspace ONE UEM on Linux, Android, Windows 10 and 11, Windows Server, MacOS, and Windows CE operating systems. The capabilities are embedded in the Workspace ONE Intelligent Hub application on iOS.

Omnissa Advanced Monitoring powered by ControlUp – Optional Add-On

Omnissa Advanced Monitoring powered by ControlUp is a third-party solution that delivers a real-time monitoring and visualization engine for Horizon that allows Customer to have a unified console for monitoring, triggers and alerts, troubleshooting, and automation for its Horizon deployment.

Omnissa Advanced Monitoring allows a customer to monitor its entire Horizon environment, detect anomalies, and proactively solve issues across its deployment. Omnissa Advanced Monitoring has an analytics engine that provides insights and reporting on the data that is collected from the customer's environment. Omnissa Advanced Monitoring is hosted by ControlUp, Inc., from its data centers. Omnissa Advanced Monitoring can be purchased as an add-on for Workspace ONE Enterprise and Workspace ONE Enterprise for VDI.

If Customer purchases an entitlement to Omnissa Advanced Monitoring as an add-on for Workspace ONE, Customer must purchase an equivalent number of entitlements for Omnissa Advanced Monitoring as it has purchased for the applicable Workspace ONE service.

Omnissa will provide support for Omnissa Advanced Monitoring. The Agreement will govern Customer's use of Omnissa Advanced Monitoring and will supersede any terms presented to Customer during the deployment and sign-in process for Omnissa Advanced Monitoring. Notwithstanding anything in the Agreement, and other than as expressly set forth in this section, Omnissa provides the Omnissa Advanced Monitoring service without any indemnification or warranty whatsoever.

Omnissa Workspace ONE® Mobile Threat Defense™ - Optional Add-On

Omnissa 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 administrator 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. Customer consents to such processing by Lookout, Inc. for these purposes. Refer to the [Lookout Privacy Notice](#), the [Workspace ONE Privacy Disclosure](#), and end user disclosures within the mobile app.

Omnissa will provide support for the Workspace ONE Mobile Threat Defense offering. The Agreement governs Customer's use of Workspace ONE Mobile Threat Defense and supersedes any terms presented to Customer during the deployment and sign-in process for Workspace ONE Mobile Threat Defense.

Maps View

Customer's use of the Maps View (optional) feature and content (available within Workspace One UEM and Intelligence services) is considered a Third-Party Offering under the Agreement, and is subject to the Microsoft Bing Maps and Embedded Maps Service Terms of Use at <https://www.bingmapsportal.com/terms/EndUserTerms> and to the data practices set forth in the then-current Microsoft Privacy Statement available at <https://www.microsoft.com/en-US/privacy/privacystatement>. This feature provides the ability to review Device GPS location data on Bing Maps-rendered maps.

2.3 OMNISSA ACCESS

Overview

OmniSSa Access™ provides an integrated platform for users to access their applications and data on any of their devices. With OmniSSa Access, a customer's IT department can manage entitlements and policy controls from a single management console. If OmniSSa Access is used with Workspace ONE UEM in an on-premises environment, the customer's use is governed by the OmniSSa General Terms, the Software Exhibit, and the Product Guide.

OmniSSa Workspace ONE® Tenancy Hierarchy™ -- Optional Add-On

OmniSSa Workspace ONE Tenancy Hierarchy is an available optional add-on for the OmniSSa Access offering. See Section 2.2 for a description of the Workspace ONE Tenancy Hierarchy service.

2.4 OMNISSA IDENTITY SERVICES

Overview

OmniSSa Identity Services provides centralized user management across Workspace ONE and Horizon Cloud Service Next-Gen offerings through OmniSSa Connect. OmniSSa Identity Services integrates with third-party cloud-based identity providers to set up user provisioning and identity federation. Customer's Workspace ONE UEM tenant must be version 2212 or later to be able to use OmniSSa Identity Services with Workspace ONE UEM.