NOTICE: This Service Description is no longer being updated. Content has been moved to the Cloud Services Guide at:

https://www./content/dam/digitalmarketing/vmware/en/pdf/agreements/vmware-cloud-services-guide.pdf

Service Description

VMware Workspace One® Access™

Last Updated: 29 August 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. All terms used but not defined in this Service Description are defined in the Terms of Service or other documents comprising the Agreement between you and us regarding your use of the Service Offering.

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

1. Introduction

VMware Workspace One® Access™ ("Workspace ONE Access", or the "Service Offering") (formerly known as VMware Identity Manager™), provides an integrated platform for users to access their applications and data on any of their devices. With Workspace One Access, a customer's IT department can easily manage entitlements and policy controls from a single management console.

Workspace One Access provides a number of key capabilities for VMware Workspace ONE® implementations, including:

- **A user portal** which provides browser-based access to different types of applications, including SaaS-based web applications (such as Salesforce, Dropbox, and Concur), VMware Horizon®–based applications and desktops, Remote Desktop Server Host (RDSH)-based applications and desktops, VMware ThinApp®-packaged apps, and Citrix-based applications and desktops. The portal simplifies application access for end users.
- **Enterprise identity management** to sync and extend on-premises directory credentials (such as Active Directory) to SaaS and native mobile applications.
- **Enterprise Single Sign-on (SSO)** to ensure that users have a single identity to log in with for internal, external, and virtual-based applications.
- **A self-service app store** to allow end users to identify and be entitled to applications easily while providing enterprise security and compliance controls to ensure that the right users have access to the right applications.

Workspace One Access complements the functionality of VMware Workspace One® UEM to deliver:

- Device-specific authentication workflows
- Certificate-based authentication
- Adds additional conditional access policies including managed or unmanaged device restrictions
- PIN code strength and timeout enforcement, and
- Selective Remote Wipe of installed enterprise applications.

1.1 Service Portals

The Service Offering includes access to two service consoles:

- **User Portal** provides access to applications and data. Users can use SSO to access SaaS and web applications, request access to applications, and customize their portal.
- **Administrator 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.

1.2 Additional Information

Technical Documentation and Training

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

Legal Terms

Use of the Service Offering is subject to the standard VMware Cloud Service Offerings Terms of Service, which can be found through a link at the main VMware end user terms page, at https://www.vmware.com/download/eula.html.

Where the Service Offering is used with Workspace One Unified Endpoint Management in a on-premise environment, please refer to the VMware End User License Agreement (available at: http://www.vmware.com/download/eula).

2. Service Operations

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

2.1 Service Support

VMware will provide support for problems that you report and selected additional services to assist with adoption and related to the Service Offering. To the extent you provide Your Content (as defined in the Terms of Service) in connection with support, VMware will handle Your Content in accordance with the applicable Terms of Service.

2.2 Service Provisioning

VMware will provide the following:

- Creating a "tenant" for your organization in the Service Offering with default authentication and authorization policies for you to log on to the Service Offering.
- Creating the initial administrative user account in the Administrator Console using default administrator privileges and system preferences.
- Make available the VMware Workspace One Identity Manager Connector installer and installation documents.

You will be responsible for the following:

- Installing the VMware Workspace One Identity Manager Connector ("Connector") in your on-premises environment and configuring it with the Service Offering.
- Creating user and group sync in the Administrator Console and changing default system preferences as needed.
- Creating and configuring SaaS and web applications for single sign-on.
- Changing default entitlement and access policies for applications and service portals.
- Configuring authentication adaptors. **Note**: the Service Offering does not provide authentication products, e.g., RSA secureID, RSA Adaptive Auth, Microsoft Active Directory, Smart Card, etc.; rather, the Service Offering provides the authentication adapters to integrate with the authentication products that you provision separately.

2.3 Monitoring

VMware will provide the following:

- Monitor availability of the Service Offering.

You are responsible for the following:

- Monitoring availability of the Connector and its connectivity with the Service Offering.
- Monitoring integration of the Connector with your user directory and authentication products.

2.4 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.

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

- Connector and any other products you have installed and integrated with Connector on your premises.

2.5 Change Management

VMware will provide the following change management elements:

- 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 Connector.

You are responsible for:

- Installing and upgrading to new releases of the Connector for new features and bug fixes.
- Administration of self-service features provided through the Administrator Console in the Service Offering up to the highest permission levels granted to you. Including by not limited to single sign-on configuration for applications, application entitlement and success policies, user directory synchronization, general account management, etc.

2.6 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 it has sole physical, logical, and administrative level control. You are responsible for the aspects of the service over which you have administrative level access or control. The primary areas of responsibility between VMware and you are outlined below.

- **Information Security:** VMware will protect the information systems used to deliver the Service Offering for 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 for which it has sole administrative level control over. This responsibility stops at any point where you have some control, permission, or access to modify an aspect of the Service Offering.
- **Patching & Vulnerability Management:** VMware will maintain the systems it uses to deliver the Service Offering, including the application of patches it 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:

- **Information Security:** 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:** 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:** 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.

2.7 Hub Services

Hub Services is a set of services that are collocated with 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-premise software offering or as a cloud service offering, can use Hub Services. Customers who 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.

2.8 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.

2.9 Usage Data

The Service Offering collects data (such as configuration, performance, and usage data) directly from VMware's software or systems hosting the Service Offering, and from the customer's systems, applications, and devices involved in the use of the Service Offering, to improve VMware products and services, and your and your users' experiences, as more specifically described in VMware's Trust & 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 VMware's Privacy Notice, including the VMware Products and Services Notice available 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 VMware Privacy Notices available 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 also be found from that link.

3. Business Operations

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

3.1 Ordering and Invoicing

Subscription Ordering

- You may order the Service Offering on a per-user basis or on a per-Device basis. A single order may include both models.
- You may purchase subscriptions for 1, 2, 3, 4 or 5-year terms.
- Initial orders must be a 25-license minimum, unless you are purchasing Workspace ONE Express, in which your initial order must be a 10-license minimum (here, a "license" means an entitlement for one Named User or one Device).
- You can only use the Service Offering for up to the number of users or devices for which you have paid the applicable fees.
- You can transfer Service Offering entitlements from user to user, or from device to device, so long as you do not exceed the number of users or devices in the relevant order.
- Your initial purchase establishes the default billing relationship that applies to all transactions for that SID for the duration of the Subscription Term. For example, if the initial order is placed through a VMware authorized reseller, then, by default, any subsequent payments related to

that SID will be made through that reseller. This billing relationship may be modified at renewal.

- For Workspace ONE Express, Standard, and Advanced, 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 and Enterprise for VDI, the SLA to provision the service is within 14 days. VMware can elect to delay the start of the billing period at its discretion.
- Additional orders for the same SID may be purchased any time during the initial Subscription Term, and those subscription terms will be prorated to and coterminous with the Subscription Term as applicable.
- Changes to the reseller, subscription term, and/or number of users or devices associated with a SID may be made at the time of renewal by contacting VMware.

Invoicing

If you purchase an entitlement to the Service Offering directly from VMware, VMware will invoice you within thirty (30) business days after the beginning of each Billing Period. If you purchase an entitlement to the Service Offering through a VMware authorized reseller, the reseller will invoice you as mutually agreed between you and such reseller. “Billing Period” is the period for which you are being billed for use of the Service Offering. Billing Periods are monthly and are related to the provisioning of your SID, unless otherwise indicated.

You will be invoiced for the quantity of entitlements purchased, regardless of whether the Service Offering is used or not.

3.2 Renewal

VMware reserves the right to not renew any SID at the end of its Subscription Term, in which case we will notify you 30 days prior to the end of the then-current Subscription Term.

Modify Subscription Service at End of Term (the default setting)

You will be contacted prior to the end of the SID subscription term to discuss your renewal options. The “Modify” renewal method setting allows you to modify your Service Offering configuration and to make changes to your reseller relationship, if applicable, by both changing your setting for the SID within the VMware customer portal available at https://my.vmware.com and issuing a new purchase order.

If you choose the modified renewal option, you are expected to review your renewal quote, discuss your route to market and billing options with your VMware sales representative, and submit a purchase order to VMware directly or to your VMware authorized reseller. If you purchase the Service Offering through a VMware authorized reseller, a manual renewal is the only time you may elect a change in your reseller relationship for that specific SID. The deadline to change the renewal option is 30 days prior to the last day of the then-current SID subscription term.

Terminate at End of Subscription Term

You may terminate your existing SID subscription, to be effective at the end of the then-current subscription term, by changing your setting for the SID within the VMware customer portal (available at https://my.vmware.com) to “Cancel”. When this option is set, your access to the Service Offering will expire at the end of the SID subscription term. The deadline to select the

termination option is 30 days prior to the last day of the then-current SID subscription term.

3.3 Suspension and Re-Enablement

While a SID is suspended by VMware as specified in the Terms of Service, VMware will restrict access to the 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 issues that led to suspension; access to the Service Offering and traffic across IP addresses will be restored.

3.4 Termination

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