



NOTICE: This Service Description is no longer being updated. Content has been moved to the Cloud Services Guide, found at <https://www.vmware.com/agreements>

VMware SD-WAN™ VMware Secure Access™ VMware Cloud Web Security™

Service Description

Last Updated: 29 August 2022

© 2022 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. This product is covered by one or more patents listed at <http://www.vmware.com/patents.html>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned in this Service Description may be trademarks of their respective companies.

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, or 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.

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

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

1. Introduction

1.1 Overview

VMware SASE™ is a cloud-native secure access service edge platform that combines VMware SD-WAN™, VMware Secure Access™, VMware Cloud Web Security™, and VMware Enterprise Network Intelligence™ into one holistic solution. The platform's points of presence (PoPs) are strategically distributed around the world and serve as an on-ramp to SaaS and other cloud services.

VMware SD-WAN. VMware SD-WAN™ (“VMware SD-WAN”) is a cloud-delivered software-defined wide area network (SD-WAN) service that provides networking services to enterprise branch locations, and to customers’ remote location workers through the “work from home” offer described in Section 4, below. VMware SD-WAN also provides instant visibility into the state and performance of the customer’s WAN, connecting the global enterprise locations, and its impact on application performance. Applications can be deployed as part of a distributed services on public, private, and hybrid cloud infrastructures as well as in existing enterprise data centers.

VMware SD-WAN includes the following components:

- VMware SD-WAN edge software (the “Software”) which is installed on customer-premises equipment (the “Equipment”) at the customer location (that is, in the customer’s own on-premises environment). The Equipment can be supplied by VMware, or by the customer (provided that the equipment supplied by the customer is x86 compatible). The Software and the Equipment are referred to collectively as the Edge for VMware SD-WAN (the “Edge”). The Edge enables deep application recognition, application and sub-second steering, performance metrics, and maintains end-to-end quality of service in addition to hosting virtual network function (VNF) services.
- The VMware SD-WAN orchestrator (the “Orchestrator”), a solution that provides centralized enterprise-wide installation, configuration, and real-time monitoring in addition to orchestrating the data flow through the cloud network. The Orchestrator enables remote provisioning of virtual services in the customer’s location, in the public cloud, or in the customer’s enterprise data center. This centralized management portal provides insight into global network operation, as well as serving as a central policy engine that supplies the Edge with both network intelligence as well as administrative policies on how applications behave in the enterprise SD-WAN network. The Orchestrator is hosted and managed by VMware.
- Access to a global, distributed set of VMware cloud gateways (the “Gateway(s)”). The Gateways serve as a distributed forwarding plane, and are responsible for delivering network traffic to its final destination. In the process of transport, reliability and performance enhancements are applied to the carried traffic that improve the end-user application experience at the enterprise locations. The Gateways are hosted and managed by VMware.

In addition to connecting branch offices, VMware SD-WAN may also be deployed at an employee’s home, enabling improved user experience and productivity. The Service Offering’s speed, scale, reliability, and flexibility help enterprise network administrators support employees working from home and improves the application experience across one or more WAN links. VMware SD-WAN also provides instant visibility into the performance and reliability of the WAN link(s) to the employee’s home, connecting the employee with the customer’s enterprise locations.

The applications that the employee working from home is accessing can be deployed as part of a distributed services environment on public, private, and hybrid cloud infrastructures as well as in existing enterprise data centers. See Section 4, below, for details of this offer.

VMware Secure Access. VMware Secure Access™ (“VMware Secure Access”) is a remote access solution that is based on Zero Trust Network Access (ZTNA) framework. The cloud-hosted solution helps enable consistent, optimal and secure cloud application access. The solution leverages VMware’s global PoPs that contain Gateways and optimizes traffic handling capabilities for lower latency and better application performance, enabling customers to have a branch-like experience for remote workers. VMware Secure Access consists of three main components:

- The Workspace ONE UEM Console, offered as a hosted service, manages enrollment of devices and ZTNA policies.
- The Orchestrator is used for configuring the networking settings on VMware Secure Access.
- VMware Workspace ONE® Tunnel™ client and VMware Workspace ONE® Intelligent Hub are the client applications installed on the end user devices. The Workspace ONE Tunnel client builds secure tunnels from the end user device to the nearest VMware PoP. Workspace ONE Intelligent Hub manages user onboarding and policy enforcement on the end user device.

Subscriptions to VMware Secure Access are sold on a per-Named User basis (entitling you to manage up to five Devices for each Named User), where “Named User” means your employee, contractor, or Third-Party Agent who has been identified and authorized by you to use VMware Secure Access, and “Device” means any client hardware that enables installing and running of VMware Secure Access client applications on that client hardware. VMware Secure Access is also available as a complement to VMware Workspace ONE®, enabling integrated access control, application management, and multiplatform endpoint management. System logs are deleted on a rolling basis 14 days after creation.

VMware Cloud Web Security. VMware Cloud Web Security™ (“VMware Cloud Web Security”) is available as an add-on to VMware Secure Access or to VMware SD-WAN. That is, you must have an active subscription to the VMware SD-WAN service or to VMware Secure Access to purchase an entitlement to VMware Cloud Web Security.

VMware Cloud Web Security is a secure web gateway service. Administrators may subject internet/SaaS traffic to a variety of security checks at the time the workloads pass through VMware PoPs that contain the Gateways. The security checks include URL filtering, content filtering, anti-virus/anti-malware, cloud sandbox, Data Loss Prevention and Cloud Access Security Broker. Administrators may define which workloads pass through which of these filters based on criteria including business policies, with network-based filters such as subnet and IP address, and non-network-based filters such as users, groups, file type, application, and domain.

Subscriptions to VMware Cloud Web Security are sold on a per-Named User basis or on a bandwidth basis. For these purposes, “Named User” means your employee, contractor, or Third-Party Agent who has been identified and authorized by you to use the offering. “Bandwidth” refers to the bandwidth tier associated with your VMware SD-WAN purchase.

In accordance with settings selected by your IT administrator, select workload data is processed by VMware Cloud Web Security on the applicable PoP, other than the workload data processed for cloud sandbox which is performed by a third-party processor. Other than to the extent sample

extracts of that workload data are retained in logs, screenshots, or copies of confirmed malicious files or URLs, the workload data will not be retained by VMware Cloud Web Security after it is processed through the designated security checks. Logs may contain information including URL destination, IP address, and the user's User ID, Username, name, email address. Logs and screenshots are deleted from the Service Offering within approximately 30 days of creation. Copies of confirmed malicious files and URLs may be retained and used by VMware and its service providers for threat intelligence purposes.

1.2 Technical Documentation and Training

Documentation outlining key concepts and instructions on the configuration of the various features is embedded in the Orchestrator. The URL for the Orchestrator instance will be provided as part of the service provisioning.

1.3 Legal Terms

Your use of the Service Offering is subject to the Terms of Service found through the links at <https://www.vmware.com/download/eula.html>. Use of the Equipment is subject to the Equipment Terms found through a link at <https://www.vmware.com/download/eula.html>.

2. Service Operations

The following outlines VMware's roles and responsibilities in providing the service offerings. 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 the duty of VMware or are assumed to be your responsibility.

2.1 Service Provisioning

VMware SD-WAN. With respect to VMware SD-WAN, VMware will provide the following provisioning services:

- VMware will create a service account and send an email or other notification to the contact that you identified in your Order inviting that contact to the newly created enterprise account. A URL to access VMware SD-WAN will be provided within this notification.
- VMware will ensure that the identified contact can create additional user accounts for other users, as needed.
- VMware will provide access to the Orchestrator
- VMware will ensure that distributed Gateways are made available for use.
- VMware will provide SD-WAN software and/or hardware in accordance with the order

Your responsibilities include:

- Ordering last mile transport links and connecting these to the Edges.
- Provisioning and deploying the Edges in accordance with the ordered quantities.
- Configuring VMware SD-WAN with business appropriate policies that control how the associated traffic behaves in the enterprise SD-WAN.
- Maintaining the security posture through configurable firewall rules on the Orchestrator or via a third-party security solution.
- Monitoring your usage and traffic patterns to ensure these are in line with the network

capacity connected to the Edges. VMware does not guarantee performance characteristics of the solution as this is conditional on the available bandwidth and quality of the bandwidth.

- Procuring and installing appropriate Equipment to run the Software if you do not obtain the Equipment from VMware.

VMware Secure Access. With respect to VMware Secure Access, VMware will provide the following provisioning services:

- VMware will create a service account and send an email or other notification to the contact that you identified in your Order inviting that contact to the newly created enterprise account. A URL to access VMware Secure Access will be provided within this notification.
- VMware will ensure that the identified contact can create additional user accounts for other users, as needed.
- VMware will provide access to the Orchestrator.
- VMware will ensure that distributed Gateways are made available for use.
- VMware will create and provide access to a Workspace ONE UEM tenant for managing remote access users and tunnel policies.

Your responsibilities include:

- Configuring the VMware Secure Access offering and provisioning users in Workspace ONE UEM to enable remote access to the Gateway.
- Maintaining the security posture through configurable tunnel profiles and device traffic rules to be applied to endpoint devices and remote access users connecting to the Gateway.
- Monitor your usage and provisioned VMware Secure Access service to ensure that remote access connectivity and performance are in line with the network capacity.

VMware Cloud Web Security. With respect to VMware Cloud Web Security, VMware will provide the following provisioning services:

- VMware will create a service account and send an email or other notification to the contact that you identified in your Order inviting that contact to the newly created enterprise account. A URL to access VMware Cloud Web Security will be provided within this notification.
- VMware will ensure that the identified contact can create additional user accounts for other users, as needed.
- VMware will provide access to the Orchestrator.
- VMware will ensure that distributed Gateways are made available for use.

Your responsibilities include:

- Configuring the VMware Cloud Web Security offering and setting up security policies (SSL Inspection, URL Filtering, Content Filtering/Inspection, CASB, DLP, etc.) to be applied on traffic to or from Secure Access users or Edges.
- Monitor the VMware Cloud Web Security web logs to ensure the configured policies are being applied appropriately.

2.2 Monitoring

VMware SD-WAN. VMware will provide the following services with respect to monitoring:

- VMware SD-WAN will provide you with the ability, through the offering, to view and monitor the link quality metrics such as bandwidth, packet loss, latency, and jitter as well as link and application utilization statistics between VMware SD-WAN endpoints (branch to branch, branch to data center, branch to Gateway).
- We will provide you with detailed event logs, recording events in relation to changes in link and IPsec tunnel state.
- We will provide you with a global overview of the status of each of the enterprise branch locations and their attached links.

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

- You are responsible for monitoring the availability of the transport links attached to the Edges (e.g., broadband internet service), which are not supplied by VMware.
- You are responsible for monitoring overage use of connected wireless broadband links as well as other links that may be charged on a volume basis. You are responsible for analyzing firewall logs that VMware SD-WAN may collect and taking appropriate action if a security incident is detected.

VMware Secure Access. VMware will provide the following services with respect to monitoring:

- VMware Secure Access will provide you with the ability to view and monitor VMware Secure Access status per PoP, such as the DNS status and Tunnel status, which you are using to connect remote access users to the PoP.
- We will provide you with detailed event logs, recording events in relation to changes in VMware Secure Access.

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

- You are responsible for monitoring the remote access users' connectivity (e.g., broadband internet service), which is not supplied by VMware.
- You have the ability to collect tunnel server logs if required. This is done by configuring the forwarding of tunnel server logs to a local syslog server in an on-premises setup.

VMware Cloud Web Security. VMware will provide the following services with respect to monitoring:

- VMware Cloud Web Security provides the ability to view and monitor Cloud Web Security traffic and associated access logs for the traffic that is directed and passing through the Cloud Web Security platform.
- We will provide you with detailed event logs, recording events in relation to changes in the Cloud Web Security service.

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

- You are responsible for monitoring the connectivity to the Cloud Web Security service. This includes the remote access users' connectivity (e.g., broadband internet service) or transport links attached the Edges, which are not supplied by VMware.
- You are responsible for monitoring the Cloud Web Security web logs for your users as per the Cloud Web Security policies applied.

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:

- Infrastructure over which VMware has direct, administrative access and control, including servers and services used to provide the service offerings.

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

- Your account settings in the Orchestrator console and/or Workspace ONE UEM Console.
- User-deployed and user-configured assets such as laptops, servers, etc.
- Anything else not under VMware's direct control and administration.
- With respect to VMware SD-WAN, availability of connected WAN links to the Edges.
- With respect to VMware Secure Access, configuration of user devices and installed software.
- With respect to VMware Cloud Web Security, configuration of the access policies as per the Enterprise security guidelines.

2.4 Change Management

VMware will provide the following change management elements:

- Processes and procedures to release new code versions, bug fixes related to the offerings.

You are responsible for:

- Management of changes to your alert notifications and other content.
- Administration of self-service features provided through the Orchestrator, up to the highest permission levels granted to you.
- Cooperating with VMware when planned or emergency maintenance is required.

2.5 Service Operations Data

In connection with providing the service offerings, VMware collects and processes information from VMware's software or the systems hosting the offerings, and from your systems, applications and devices that are used to access and use the offerings. That information is processed to facilitate delivery of the offerings, including but not limited to (i) tracking entitlements, (ii) providing support, (iii) monitoring and ensuring the performance, integrity, and stability of the offerings' infrastructure, and (iv) preventing or addressing service or technical issues. 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>

2.6 Usage Data

The service offerings collect data directly from the machines and/or devices involved in the use of the offerings, 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>. For VMware SD-WAN, this includes configuration, performance, and usage data, including limited flow statistics (Edge ID, throughput, application), and limited link statistics (ISP name, bandwidth, speed). For VMware Secure Access, this may include configuration data, feature usage data, performance data, authentication data, system logs, diagnostic data, and support data including Gateway IP address and hostname. For VMware Cloud Web Security, this includes feature usage 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 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 may 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.

2.7 Content

VMware SD-WAN. As VMware SD-WAN is used, the Edges and Gateways send data to the Orchestrator including flow statistics (Edge ID, hostname, source and destination IP address, source MAC address, throughput, destination domain name, protocol, application, and application category) and link statistics (ISP name, Public IP address, bandwidth, speed, latency, packet loss and jitter). During the Subscription Term, data transmitted to VMware SD-WAN will be retained in the Orchestrator and available for querying and alerts for at least two weeks (by default) from the date and time the data was originally ingested into VMware SD-WAN. The amount of data stored depends on the storage space available on the Orchestrator and the amount of data generated by each site's Edge.

VMware Secure Access. VMware Secure Access processes identity and authentication information, device information, communication data, geo-location data, and application access/usage details. This data is not retained after it is processed.

VMware Cloud Web Security. Depending on the customer's configuration of VMware Cloud Web Security, workload data selected by the customer is sent to VMware Cloud Web Security for security checks as designated by the customer. Customers may define which workloads pass through which security checks based on criteria including network-based filters such as subnet and IP address, and non-network-based filters such as users, groups, file type, application, and domain.

3. Business Operations

3.1 Ordering

The SASE offerings are available from authorized VMware channel partners. Subscriptions can be purchased for committed terms of one, three, or five years.

In connection with your order for any of the SASE offerings, you may need to provide information such as site count, site location(s), feature(s), throughput(s), and your network administrator's email. The information you provide is required to provision the service offering for you. Your Subscription Term will begin on the date your instance of the service offering has been

provisioned. If you do not provide the needed information, VMware cannot provision the service offering for you.

For SD-WAN subscription purchases including Equipment, your Subscription Term may begin prior to installation of the Equipment in your location. VMware may permit you to continue to use the service offering for an additional period, not to exceed 30 days, after expiration of your committed Subscription Term, at no additional cost, if your Subscription Term began prior to installation of the Equipment. All terms, other than payment of fees, will continue to apply during any extended use term.

Additional services/products, or upgrades, may be purchased at the time of your initial Order or through the VMware customer portal at any time during the Subscription Term. Additional terms and fees will apply to such additional services. If services/products are added during the term of an existing contract, the contract termination date for the add-on services/products defaults to the same date as that of the existing contract. For the add-on orders, you may be required to configure the Orchestrator to activate the additional services and products.

Service offering capacity reductions must be coordinated with VMware at the time of subscription renewal and will require a manual renewal order for the reduced offering capacity. Orders for reduced capacity must be submitted to VMware at least five (5) calendar days prior to the date of subscription renewal.

3.2 Suspension and Re-Enablement

While a SID is suspended by VMware for delinquent payment or any other reason as set forth in the Terms of Service, VMware will disable your account. VMware will retain SIDs with configurations and data intact until the issue is resolved or the subscription expires or is terminated. SID re-enablement will be initiated within three (3) business days upon resolution of the issues that led to suspension; access to the service offering will be restored. Suspension (when access to the service offering is disabled) does not suspend your financial obligations, nor does it extend the end date of the Subscription Term.

3.3 Termination

Termination of a SID due to termination of the Agreement will result in permanent loss of access to the service offering, and a deletion of any Equipment configuration and data. Data from a terminated SID will be deleted within 90 days of the termination date of the SID. Data may continue to survive in backups for up to one year following termination of your account. Such backups are not accessed unless needed to restore a customer environment and will be deleted as part of periodic deletion activities. During this period, data will not be generally accessible, as the data is intended to be used for disaster recovery purposes (if needed). VMware may retain any anonymized or hashed data. Any deleted data is non-recoverable.

4. VMware SD-WAN Work from Home Offer

Enterprise customers that have employees working from home can purchase subscriptions to VMware SD-WAN to support their remote workforce, through the VMware SD-WAN™ WFH Subscription (“WFH Subscription”) and the VMware SD-WAN™ WFH Pro Subscription (“WFH Pro Subscription”) offer.

Subscriptions purchased through this offer can only be used at employees' home locations. For the WFH Subscription, there is a limit of one business user with two concurrent devices and up to 350 Mbps or the max throughput of the Edge (whichever is lower). For the WFH Pro Subscription there is a limit of one business user with three concurrent devices and up to 1 Gbps or the max throughput of the Edge (whichever is lower). Both the WFH Subscription and the WFH Pro Subscription offers allow for an unlimited number of home users and devices. The key difference between a business user and home user is that the business user can send traffic to the Gateways, to other Edges, or directly to the Internet, but the home user can only send traffic directly to the Internet. Business users and home users must use separate network segments. Both WFH Subscription and WFH Pro Subscription subscriptions will provide access to the same feature set as VMware SD-WAN.

For purposes of this Service Description and this work from home offer, a "business user" means an individual who is the customer's designated User, as defined in the Terms of Service, (e.g., an employee of the customer, an independent contractor performing services for the customer, or a person who is otherwise one of the customer's designated Users). A "home user" means an individual who is not a "business user" or who is not acting as a "business user" but is connected to the Edge in the business user's home, by WiFi or physical port. A "home user" may also be a "business user" of the customer (i.e., a "business user" acts as a "home user" when (s)he is using a personal device (e.g., personal laptop, personal mobile device, gaming system, smart TV, etc.).

VMware reserves the right to confirm compliance by checking the Edge logs to verify adherence to the requirements of this work from home offer.

VMware reserves the right to terminate this work from home offer at any time. However, termination of the offer will not operate to terminate SD-WAN WFH Subscriptions or WFH Pro Subscriptions purchased pursuant to the offer; those subscriptions will expire according to their terms, but cannot be renewed.