NOTICE: This Service Description is no longer being updated.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

Service Description

VMware RemoteHelp™

Updated as of: 30 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 RemoteHelp™ (the "Service Offering") provides a stand-alone platform for carrier customer care technicians and IT admins within MSPs/OEMs to remotely diagnose, support, and troubleshoot problems on end users' mobile devices in a simple and secured way.

The Service Offering provides a number of key capabilities including:

- Browser-based access to a remote device (mobile) screen so the technician can view the device screen and support the end user. Based on the version of the Service Offering purchased, the technician can either only view the device or will be able to control the device.
- A client that is downloaded to the device from the applicable app stores (playstore for Android and the Apple App Store for iOS). The device client connects to the backend server and initiates streaming that gets displayed on the Technician Console.

1.1 Service Portals

The Service Offering includes access to two service consoles:

- **Technician Console** provides access for the technician to view/control the remote device with shortcuts and device diagnostic data. This is the place from where the technician would be able to guide/educate/troubleshoot the end user's device related issues.
- **Administrator Console** provides carrier admins or MSP IT admins a way to configure the system for various roles/rules/policies. The console also provides reports and configurations to modify the system's look and feel.

1.2 Additional Information

Legal Terms

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

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 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.
- Engagement with your IT organization regarding setting up SSO/CRM connectivity for seamless access.
- Engagement with your teams for any branding requirements (if applicable to the edition of the Service Offering purchased).

- Work with your device teams to provide the clients to OEM for signature (if applicable to the edition of the Service Offering purchased).

You will be responsible for the following:

- Providing data for SSO/CRM integration.
- Setting up training for technicians.
- Setting up of Roles/Rules/Policies on the Administration Portal (as required)

2.2 Monitoring

VMware will provide the following:

- Monitor availability of the Service Offering.

You are responsible for the following:

- Monitoring availability of the SSO/CRM systems (if applicable)

2.3 Incident and Problem Management

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

- Availability of the Service Offering.

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

- SSO/CRM integrations (if applicable)

2.4 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.

You are responsible for:

- Any changes to CRM/SSO integration end points.

2.5 Security

The end-to-end security of the Service Offering is shared between VMware and you. VMware will provide security for the aspects of the Service Offering over which it has sole physical, logical, and administrative level control. You are responsible for the aspects of the Service Offering over which you have administrative level access or control. The primary areas of responsibility between VMware and you are outlined below.

VMware will use commercially-reasonable efforts to provide:

- **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. 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 VMware deems critical for the target systems. VMware will perform routine vulnerability scans to surface critical risk areas for the systems it uses to deliver the Service Offering. Critical vulnerabilities will be addressed in a timely manner.

You are responsible for:

- **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.

2.6 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.

2.7 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.

2.8 Data Retention and Deletion

During your Subscription Term, all data older than 90 days is purged based on a scheduled job. Following expiration or termination of your entitlement to the Service Offering, all of Your Content in VMware's possession (both online and in our backup systems) will be deleted within 30 days after the termination date.

3. Purchasing

The Service Offering is available in Basic (Remote View) and Advanced (Remote Control) editions. Consult your VMware sales representative for details on ordering a subscription to the Service Offering, including minimum purchase requirements.