

PRODUCT DATA SHEET

# SUPPLEMENTS THE HPE DATA PRIVACY AND SECURITY AGREEMENT SCHEDULE

	<b>Aruba Central (including the Proximity Tracking Feature)</b>
<b>Aruba* performs the following services:</b>	Provides modern, cloud-native network operations and assurance for wired, Wi-Fi, and SD-WAN networks. Aruba Central enhances traditional management with integrated AI-based network and user insights, and IoT device profiling for secure, unified management and control. In addition, Aruba Central has the capacity to collect certain data related to location of users (including identification of the Wi-Fi access point the client device is associated to and the duration) for purposes of contact tracing and alerting for potential exposure.
<b>Customer Personal Data:</b>	Data collected as part of network management and related applications include: <ul style="list-style-type: none"> <li>• Device MAC</li> <li>• Device IP</li> <li>• Device Operating System</li> <li>• Device Hostname</li> <li>• Username</li> <li>• Email (in case of guest self-registration)</li> <li>• Phone (in case of guest self-registration)</li> <li>• Social media identity (in case of guest social login)</li> <li>• Location of user (based on proximity to specific access points)</li> <li>• Display Name / Group Membership / Title (in case of Cloud Auth use)</li> </ul>
<b>Data subjects to whom Customer Personal Data pertains are:</b>	Customer's client / end-user / employee / contractor and temporary worker
<b>With respect to Customer Personal Data, Customer is acting as:</b>	Controller
<b>Aruba shall process Customer Personal Data</b>	<b>Provisioning Services:</b> The information gathered and stored by the product is the minimum required to ensure secure access to the portal, and essential to performing its function. All session logs about a user will be automatically purged after 90 days.

<b>only as follows:</b>	<b>Support Services:</b> Access to customer environment and data for troubleshooting is provided to Aruba support services based on customer agreements and permissions.
-------------------------	---

\*Aruba, a Hewlett Packard Enterprise company, is referred throughout this document as Aruba

Aruba Central	
<b>Security and Encryption:</b>	<p><b>Product Security Features:</b></p> <ul style="list-style-type: none"> <li> <p>• <b>Physical Security:</b></p> <p>Aruba Central is hosted in the most widely adopted IaaS platform—Amazon Web Services (AWS) that offers the most comprehensive security and compliance features. AWS has put in place security measures around all critical areas including perimeter, infrastructure, data and environment layers.</p> </li> <li> <p>• <b>Network Security:</b></p> <p>Our network security ensures that the physical and virtual network on which the application and data resides is secure. We use services and tools that the IaaS provider offers and some 3<sup>rd</sup> party solutions to make sure our production environment is as secure as it can be from external threats and internal vulnerabilities.</p> <p>Aruba operates separate instances of internal and production environments. The internal environment is focused on development and testing, while the production environment is solely reserved for our customers. Having this physical and logical separation of our production environment from other running instances helps us offer the best quality software deployment to our customers and ensures their data is always confined to one environment.</p> </li> <li> <p>• <b>Application Architecture and Security:</b></p> <p>All traffic that is exchanged between the Central application and the outside world is done using HTTPS over SSL. All traffic flow is encrypted using AES encryption technology.</p> <p>Different application tiers such as web, app and database are designed to operate in an allowlist framework. Only necessary and required communication paths are allowed between tiers. Each instance within a tier is protected by firewall rules to prevent any unauthorized or malicious access.</p> </li> <li> <p>• <b>Data Security:</b></p> <p>All data exchange between the application and devices and users happens using HTTPS. Data at rest is encrypted and stored. Data backup occurs on a regular basis and backup data is stored in a redundant manner. From an organization perspective we have a DevOps team that manages all security and operational aspects of the app.</p> </li> <li> <p>• <b>Geographic Availability:</b></p> <p>Aruba Central is available in multiple locations worldwide, allowing customers to choose in which region to establish an account. Many factors can influence this decision. For example, an organization may require all data to reside in a given region or impose regulatory restrictions on how data can be processed and stored.</p> </li> </ul>

Aruba Central is deployed on clusters in selected Amazon Web Services (AWS) Data Centers, with AWS providing the compute and storage infrastructure. The following table provides a detailed listing of Aruba Central Clusters and the supporting AWS Regions:

<b>ARUBA CENTRAL CLUSTER</b>	<b>AWS REGION (City where Cluster is based)</b>	<b>SIGN UP URL</b>
US-1	US West (Oregon), us-west-2	<a href="https://portal.central.arubanetworks.com/signup">https://portal.central.arubanetworks.com/signup</a>
US-2	US West (Oregon), us-west-2	<a href="https://portal-prod2.central.arubanetworks.com/signup">https://portal-prod2.central.arubanetworks.com/signup</a> OR <a href="https://signup.central.arubanetworks.com/">https://signup.central.arubanetworks.com/</a>
US-WEST-4	US West (Oregon), us-west-2	<a href="https://portal-uswest4.central.arubanetworks.com/signup">https://portal-uswest4.central.arubanetworks.com/signup</a>
CHINA-1	China (Beijing), cn-north-1	<a href="https://portal.central.arubanetworks.com.cn/signup">https://portal.central.arubanetworks.com.cn/signup</a>
EU-1	EU (Frankfurt), eu-central-1	<a href="https://portal-eu.central.arubanetworks.com/signup">https://portal-eu.central.arubanetworks.com/signup</a>
EU-CENTRAL3	EU (Frankfurt), eu-central-1	<a href="https://portal-eucentral3.central.arubanetworks.com/signup">https://portal-eucentral3.central.arubanetworks.com/signup</a>
CANADA-1	Canada (Central), ca-central-1	<a href="https://portal-ca.central.arubanetworks.com/signup">https://portal-ca.central.arubanetworks.com/signup</a>

	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%; text-align: center;">APAC-1</td> <td style="width: 25%;">Asia Pacific (Mumbai), ap-south-1</td> <td style="width: 60%;"><a href="https://portal-apac.central.arubanetworks.com/signup">https://portal-apac.central.arubanetworks.com/signup</a></td> </tr> <tr> <td style="text-align: center;">APAC-EAST1</td> <td>Asia Pacific (Tokyo), ap-northeast-1</td> <td><a href="https://portal-apaceast.central.arubanetworks.com/signup">https://portal-apaceast.central.arubanetworks.com/signup</a></td> </tr> <tr> <td style="text-align: center;">APAC-SOUTH1</td> <td>Asia Pacific (Sydney), ap-southeast-2</td> <td><a href="https://portal-apacsouth.central.arubanetworks.com/signup">https://portal-apacsouth.central.arubanetworks.com/signup</a></td> </tr> </table> <p>All activity on devices assigned to a customer terminate in the chosen cluster, including network statistics and telemetry data pushed over HTTPS connections. Configuration data for all customer accounts are also retained in the chosen cluster</p> <p>All data (including personal data) corresponding to the network devices (i.e. Access Points, Switches, Gateways), client devices and any other user data is stored on databases within the same cluster, with the exception of Airwave customers who opt for the Proximity Tracking Feature. Data for such Airwave customers, as it relates to the Proximity Tracking Feature, will be sent to an AWS cluster located in the US. Any additional processing that might be required is also performed on compute instances within the same cluster or otherwise in accordance with the Data Privacy and Security Agreement for Aruba product services.</p>	APAC-1	Asia Pacific (Mumbai), ap-south-1	<a href="https://portal-apac.central.arubanetworks.com/signup">https://portal-apac.central.arubanetworks.com/signup</a>	APAC-EAST1	Asia Pacific (Tokyo), ap-northeast-1	<a href="https://portal-apaceast.central.arubanetworks.com/signup">https://portal-apaceast.central.arubanetworks.com/signup</a>	APAC-SOUTH1	Asia Pacific (Sydney), ap-southeast-2	<a href="https://portal-apacsouth.central.arubanetworks.com/signup">https://portal-apacsouth.central.arubanetworks.com/signup</a>
APAC-1	Asia Pacific (Mumbai), ap-south-1	<a href="https://portal-apac.central.arubanetworks.com/signup">https://portal-apac.central.arubanetworks.com/signup</a>								
APAC-EAST1	Asia Pacific (Tokyo), ap-northeast-1	<a href="https://portal-apaceast.central.arubanetworks.com/signup">https://portal-apaceast.central.arubanetworks.com/signup</a>								
APAC-SOUTH1	Asia Pacific (Sydney), ap-southeast-2	<a href="https://portal-apacsouth.central.arubanetworks.com/signup">https://portal-apacsouth.central.arubanetworks.com/signup</a>								
<p><b>Privacy Considerations Specific to Proximity Tracking</b></p>	<p>Privacy Considerations if using Proximity Tracking Feature:</p> <ul style="list-style-type: none"> <li>• Before implementing a contact tracing solution based on the location tracking of individuals, it is recommended that your organization conduct a privacy impact assessment to ensure the solution is implemented in compliance with applicable privacy laws. In particular, your organization may need to: <ul style="list-style-type: none"> <li>o (i) establish a legal basis for the processing of personal data for the purpose of contact tracing;</li> <li>o (ii) provide a new or updated privacy notice to individuals to meet transparency requirements and inform them of their rights;</li> <li>o (iii) collect and manage consents from individuals; or</li> <li>o (iv) consult with employee representatives or Works Councils.</li> </ul> </li> <li>• Further, if your organization collects and uses sensitive personal data (e.g. health related information) as part of a contact tracing solution, additional privacy requirements may apply.</li> </ul> <p>For additional information about how Aruba solutions processes information, please see <a href="https://www.arubanetworks.com/gdpr/">https://www.arubanetworks.com/gdpr/</a></p>									
<p><b>Privacy-Specific Certifications:</b></p>	<p>None</p>									