

# Aruba ClearPass

## Annex II: Description of the processing

---

1. Description of processing	<p>Services provides network access control (NAC) to secure wired, and virtual private network connections. It is an “on-premises” solution that runs in the end users’ networks. Processor and its affiliates will: (i) have access to Controller personal data hosted in Processor’s VPC as part of the proof of concept services; and (ii) during the provision of support services through the receipt of data dumps or remote access to Controller systems. Skyhook Services: Limited ClearPass Extensions may require the use of Skyhook Services to broker communication between Controller and external cloud hosted services. Processing is offered as a service only to Controller who accepts the Processor’s HPE Aruba Networking SaaS agreement to register for the Skyhook service with the Extension.</p>
2. Type of personal data processed	<p>Personal data collected includes:</p> <ul style="list-style-type: none"><li>• MAC address</li><li>• IP address</li><li>• Connection information (start time, end time, data transferred)</li><li>• Usernames</li><li>• Passwords</li><li>• Email address</li><li>• Mobile phone numbers</li><li>• Endpoint operating system (OS) profiling information</li><li>• Web browser information</li><li>• Social network or cloud-based login service user profiles</li><li>• Installed/running endpoint applications</li><li>• Information such as group membership or authorization lists obtained through external device queries</li></ul>

---

## Annex II: Description of the processing (continued)

3.	Categories of personal data processed	Controller's employees, contractors, and temporary workers, as well as guests.
4.	Duration of processing	Processor shall process Controller personal data for the duration of the Agreement and/or any applicable transaction document.
5.	Technical & Organizational Measures	Support services: Processor's HPE Aruba Networking TAC CRM is certified compliant with the highest independent, international, industry-accepted privacy standards. Processor shall maintain the information and physical security program for the protection of Controller personal data as detailed in Annex III below

## Annex III: Technical and organizational measures including technical and organizational measures to ensure the security of the data

- **Product:** The product itself is a security product used to control network access on Controller networks. Access controls are defined by the Controller security policy and requirements.
  - All data is stored within an AES128-Bit encrypted database within the access-controlled management interface of the product.
  - There is an SIRT group that follows security advisories for externally reported vulnerabilities, including third-party open source code, as well as internally identified issues.
  - Security updates are regularly released in a timely manner.
- **Technical Security Features:**
  - The product uses firewall to only open specific network ports that need to be open for product usage.
  - All credentials are stored in encrypted format.
  - Product minimizes programs and processes running as root.
- **Third-party Security Certifications:** Common Criteria validated against CPP\_ND\_V1.0 and PP\_NDCPP\_APP\_AUTHSVR\_EP\_V1.0 (VID#10814) FIPS140-2 Level 1 certificate #2577.

Visit [HPE.com](https://www.hpe.com)

[Chat now](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a50009440ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

