

HPE Aruba Networking Central

Allegato II: Descrizione del trattamento dei dati

1.	Descrizione del trattamento dei dati	HPE Aruba Networking Central offre operazioni di rete moderne e cloud-native e una garanzia per reti cablate, Wi-Fi e SD-WAN. HPE Aruba Networking Central potenzia la gestione tradizionale con informazioni integrate su utenti e reti basate sull'intelligenza artificiale e la profilazione dei dispositivi IoT per una gestione e un controllo sicuri e unificati.
2.	Tipo di dati personali trattati	I dati personali raccolti nell'ambito della gestione della rete e delle relative applicazioni includono: a. MAC del dispositivo b. IP del dispositivo c. Sistema operativo del dispositivo d. Nome host del dispositivo e. Nome utente f. Email (in caso di autoregistrazione dell'ospite) g. Telefono (in caso di autoregistrazione dell'ospite) h. Identità sui social media (in caso di accesso dell'ospite tramite social) i. Nome visualizzato/appartenenza a gruppo/titolo (in caso di utilizzo dell'autenticazione cloud)
3.	Categorie di dati personali trattati	Client del Titolare del trattamento, utente finale, dipendente, collaboratore esterno e lavoratore temporaneo.
4.	Durata del trattamento	Le informazioni raccolte e conservate dal prodotto sono quelle minime richieste per contribuire a garantire un accesso sicuro al portale e sono essenziali per il suo funzionamento. I registri di sessione di ciascun utente verranno eliminati automaticamente dopo 90 giorni.
5.	Misure tecniche e organizzative	Il Responsabile del trattamento mantiene il programma di sicurezza informatica e fisica per la protezione dei dati personali del Titolare, come specificato nell'Allegato III di seguito.

Allegato III: Misure tecniche e organizzative, comprese le misure tecniche e organizzative per garantire la sicurezza dei dati

1. Funzionalità di sicurezza del prodotto:

- a. **Sicurezza fisica:** HPE Aruba Networking Central è ospitato sulle piattaforme IaaS più diffuse: Amazon Web Services (AWS) e Microsoft Azure, che offrono le funzionalità di sicurezza e conformità più complete. AWS e Azure ha messo in atto misure di sicurezza attorno a tutte le aree critiche, inclusi il perimetro, l'infrastruttura, i dati e i livelli dell'ambiente.
- b. **Sicurezza della rete:** La sicurezza della rete del Responsabile del trattamento contribuisce a garantire che la rete fisica e virtuale su cui si trovano l'applicazione e i dati sia sicura. Utilizziamo i servizi e gli strumenti offerti dai fornitori IaaS e alcune soluzioni terze per garantire che il nostro ambiente di produzione sia il più sicuro possibile contro minacce esterne e vulnerabilità interne. Il Responsabile del trattamento gestisce istanze separate di ambienti interni e di produzione. L'ambiente interno è focalizzato sullo sviluppo e sui test, mentre l'ambiente di produzione è riservato esclusivamente ai nostri clienti (Titolare del trattamento). Questa separazione fisica e logica del nostro ambiente di produzione da altre istanze in esecuzione ci aiuta a offrire la distribuzione software della migliore qualità ai nostri clienti (Titolare del trattamento) e contribuisce a garantire che i loro dati siano sempre confinati in un unico ambiente.
- c. **Architettura e sicurezza dell'applicazione:** Tutto il traffico scambiato tra l'applicazione centrale e il mondo esterno avviene tramite HTTPS su SSL. L'intero flusso di traffico è crittografato utilizzando la tecnologia di crittografia AES. I diversi livelli dell'applicazione, come web, app e database, sono progettati per funzionare in un framework di elenchi consentiti. Tra i diversi livelli sono consentiti solo i percorsi di comunicazione necessari e richiesti. Ogni istanza all'interno di un livello è protetta da regole firewall volte a impedire qualsiasi accesso non autorizzato o dannoso.
- d. **Sicurezza dei dati:** L'intero scambio di dati tra l'applicazione, i dispositivi e gli utenti avviene tramite HTTPS. I dati inattivi vengono crittografati e conservati. Viene regolarmente effettuato il backup dei dati e i dati di backup vengono conservati in modo ridondante. Da un punto di vista organizzativo, disponiamo di un team DevOps che gestisce tutti gli aspetti di sicurezza e gli aspetti operativi dell'app.
- e. **Disponibilità geografica:** HPE Aruba Networking Central è disponibile in molti luoghi in tutto il mondo, consentendo al Titolare del trattamento dei dati di scegliere in quale regione creare un account. Sono molti i fattori che possono influire su questa decisione. Per esempio, un'organizzazione potrebbe richiedere che tutti i dati si trovino in una determinata regione o imporre restrizioni normative sulle modalità di trattamento e conservazione dei dati.

HPE Aruba Networking Central viene distribuito su cluster in data center selezionati di Amazon Web Services (AWS) e Microsoft Azure e i provider cloud forniscono l'infrastruttura di elaborazione e storage. Nella seguente tabella viene fornito un elenco dettagliato dei cluster HPE Aruba Networking Central e delle regioni supportate:

HPE Aruba Networking Central Cluster	Regione AWS (Città in cui si trova il cluster)	URL di registrazione
US-1	US Ovest (Oregon), us-west-2	portal.central.arubanetworks.com/signup
US-2	US Ovest (Oregon), us-west-2	portal-prod2.central.arubanetworks.com/signup or console.greenlake.hpe.com
US-West-4	US Ovest (Oregon), us-west-2	portal-uswest4.central.arubanetworks.com/signup
US-West-5	US Ovest (Oregon), us-west-2	common.cloud.hpe.com
China-1	Cina (Pechino), cn-north-1	portal.central.arubanetworks.com.cn/signup
EU-1	UE (Francoforte), eu-central-1	portal-eu.central.arubanetworks.com/signup
EU-Central2	UE (Francoforte), eu-central-1	common.cloud.hpe.com
EU-Central3	UE (Francoforte), eu-central-1	console.greenlake.hpe.com
Canada-1	Canada (Centrale), ca-central-1	portal-ca.central.arubanetworks.com/signup

HPE Aruba Networking Central Cluster	Regione AWS (Città in cui si trova il cluster)	URL di registrazione
APAC-1	Asia Pacifico (Mumbai), ap-south-1	portal-apac.central.arubanetworks.com/signup
APAC-East1	Asia Pacifico (Tokyo), ap-northeast-1	portal-apaceast.central.arubanetworks.com/signup
APAC-South1	Asia Pacifico (Sydney), ap-southeast-2	console.greenlake.hpe.com

HPE Aruba Networking Central Cluster	Regione Azure (Città in cui si trova il cluster)	URL di registrazione
UAE North1	EAU Nord (Dubai)	common.cloud.hpe.com

Tutte le attività sui dispositivi assegnati a un Titolare del trattamento terminano nel cluster scelto, comprese le statistiche di rete e i dati di telemetria inviati tramite connessioni HTTPS. Anche i dati di configurazione di tutti gli account del Titolare del trattamento vengono conservati nel cluster scelto.

Tutti i dati (inclusi i dati personali) corrispondenti ai dispositivi di rete (ovvero punti di accesso, switch, gateway), ai dispositivi del Titolare del trattamento e a tutti gli altri dati utente vengono conservati nei database all'interno dello stesso cluster. Eventuali trattamenti aggiuntivi che si rendessero necessari vengono altresì eseguiti su istanze di elaborazione all'interno dello stesso cluster o altrimenti in conformità al DPSA per i servizi del prodotto HPE Aruba Networking.

— Misure di sicurezza:

- Il Responsabile del trattamento mantiene il seguente programma di sicurezza informatica e fisica per la protezione dei dati personali del Titolare ("Programma di sicurezza del Responsabile del trattamento"):
 - L'infrastruttura del Responsabile dispone di versioni adeguatamente aggiornate del software di sicurezza del sistema, che possono includere firewall dell'host, protezione antivirus e definizioni di patch e virus aggiornate. Il Responsabile conserva i registri degli eventi che coinvolgono l'infrastruttura, compresi i sistemi di rilevamento delle intrusioni, per monitorare, rilevare e segnalare modelli di abuso, attività sospette, utenti non autorizzati e altri rischi per la sicurezza:
 - I dipendenti e i collaboratori esterni sono formati sulle politiche del Responsabile in materia di privacy e sicurezza e resi consapevoli delle loro responsabilità in merito alle pratiche di privacy e sicurezza. I dipendenti e i collaboratori esterni del Responsabile del trattamento sono tenuti per contratto a mantenere la riservatezza dei dati personali del Titolare e a rispettare le politiche, gli standard o i requisiti del Responsabile applicabili in relazione al trattamento dei dati personali del Titolare. La mancata osservanza di tali politiche, standard o requisiti sarà soggetta a indagini che potrebbero comportare azioni disciplinari fino alla cessazione del rapporto di lavoro o dell'incarico da parte del Responsabile.
- Qualora il Titolare venisse a conoscenza di una violazione dei dati personali che riguardi i servizi, il Titolare riferirà tempestivamente l'accaduto al Responsabile e lo informerà sulla portata della violazione dei dati personali. La comunicazione dovrà essere inviata al Security Operation Center del Responsabile via email all'indirizzo security@hpe.com.

[Avvia chat](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso. Le uniche garanzie per i prodotti e i servizi Hewlett Packard Enterprise sono quelle espressamente indicate nelle dichiarazioni di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto contenuto nel presente documento potrà essere interpretato come garanzia supplementare. Hewlett Packard Enterprise declina ogni responsabilità per eventuali omissioni ed errori tecnici o editoriali contenuti nel presente documento.

Azure e Microsoft sono marchi o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri Paesi. Tutti i marchi di terzi appartengono ai rispettivi titolari.

a50009439ITE, Rev. 3

HEWLETT PACKARD ENTERPRISE

hpe.com

Visita [HPE.com](https://hpe.com)

