

HPE Aruba Networking User Experience Insight

Annexe II : Description du traitement

1. Description du traitement	<p>HPE Aruba Networking User Experience Insight (UXI) est une application cloud de gestion de l'expérience utilisateur numérique et de résolution des incidents. La solution est composée de capteurs et d'agents logiciels spécifiquement conçus pour les appareils Android™, Windows, macOS et Zebra. Ces capteurs et ces agents spécifiquement conçus assurent en continu des tests des réseaux filaires et sans fil, des services réseau et des applications internes et externes. L'agent UXI pour Zebra peut également identifier et dépanner les problèmes réseau au niveau de l'itinérance et de l'analyse vocale.</p> <p>Fourniture de service : Constituant le minimum requis pour garantir un accès sécurisé au portail, les informations collectées et stockées par le produit sont essentielles au bon fonctionnement de ce dernier. Services d'assistance : L'accès à l'environnement et aux données du Contrôleur pour la résolution des incidents est fourni aux services de support du Responsable du traitement selon les accords et autorisations du Contrôleur.</p>
2. Type de données personnelles traitées	<p>L'application cloud assure la maintenance du compte du Contrôleur et des capteurs associés. Les données liées au compte du Contrôleur incluent les suivantes :</p> <ul style="list-style-type: none">a. Adresse e-mail de connexion et mot de passeb. Prénom et nomc. Sociétéd. Numéro de téléphone (facultatif)e. Emplacement d'un appareil dédié détenu par le Contrôleur (uniquement pour l'agent UXI) <p>Le capteur et l'agent UXI sont des clients du réseau. Lorsqu'une capture de paquet est explicitement déclenchée par le Contrôleur à des fins de dépannage du réseau, l'adresse MAC de tout client du réseau à proximité du problème peut être collectée. User Experience Insight n'utilise pas ces informations pour identifier qui que ce soit. L'agent UXI s'exécute en arrière-plan et collecte des informations sur le réseau et la localisation afin de faciliter la résolution des incidents en cas de baisse de performances réseau. Les informations réseau comprennent l'adresse IP et MAC des appareils, leur SSID Wi-Fi, le nom de leur point d'accès et leurs serveurs DNS. Les informations concernant les appareils indiquent notamment la marque, le modèle, la version de SE, la version de pilote Wi-Fi et le nom.</p>
3. Catégories de données personnelles traitées	Contrôleurs ayant accès au tableau de bord.

4.	Durée du traitement	Le Responsable du traitement traitera les données personnelles du Contrôleur pendant la durée du Contrat et/ou du document de transaction applicable.
5.	Mesures techniques et organisationnelles	Le Responsable du traitement gèrera les informations et le programme de sécurité physique en vue de la protection des données personnelles du Contrôleur selon les modalités détaillées dans l'Annexe III ci-dessous.

Annexe III : Mesures techniques et organisationnelles comprenant les mesures techniques et organisationnelles pour assurer la sécurité des données

1. Fonctionnalités de sécurité liées aux capteurs :

- Sécurité physique :** Le capteur spécifiquement conçu avec l'agent UXI stocke les informations de connexion de façon sécurisée, chiffrée et dissimulée.
- Sécurité du réseau :** Chaque capteur spécifiquement conçu dispose de trois interfaces : Wi-Fi, Ethernet et cellulaire. Ces interfaces réseau sont totalement isolées les unes des autres grâce à un mécanisme d'espace de nom Linux®, sans possibilité de les relier. Par défaut, aucun service n'écoute sur aucun port de ces interfaces. Il est impossible d'utiliser les protocoles SSH ou Telnet sur le capteur. L'agent UXI s'exécute en arrière-plan et dépend des fonctions réseau des appareils Android, Windows et macOS.
- Sécurité des données :** Toutes les communications sont sortantes et initiées par le capteur.

2. Fonctionnalités de sécurité des applications :

- Sécurité physique :** User Experience Insight est hébergé sur Amazon Web Services (AWS) et Google Cloud™. L'ensemble du stockage et du traitement des données se fait aux États-Unis. AWS et Google Cloud ont mis en place des mesures de sécurité autour des zones cruciales comme le périmètre, l'infrastructure, les données et les couches de l'environnement.
- Sécurité du réseau :** User Experience Insight fait appel aux services et outils offerts par le fournisseur IaaS et à certaines solutions tierces pour faire en sorte que notre environnement de production soit le mieux sécurisé possible face aux menaces externes et aux vulnérabilités internes. L'instance de production est déployée sur son propre cloud privé virtuel (VPC) au sein du cloud du prestataire IaaS.
- Sécurité des données :** Tous les échanges de données entre l'application et les utilisateurs se font via HTTPS (TLS 1.2).

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

[Live Chat](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Les informations figurant dans ce document sont susceptibles d'être modifiées sans préavis. Les seules garanties relatives aux produits et services Hewlett Packard Enterprise sont stipulées dans les déclarations de garantie expresses accompagnant ces produits et services. Aucune partie du présent document ne saurait être interprétée comme offrant une garantie supplémentaire. Hewlett Packard Enterprise décline toute responsabilité en cas d'erreurs ou d'omissions de nature technique ou rédactionnelle dans le présent document.

Android et Google Cloud sont des marques déposées de Google LLC. Linux est la marque déposée de Linus Torvalds aux États-Unis et dans d'autres pays. Windows est une marque commerciale ou une marque déposée de Microsoft Corporation aux États-Unis ou dans d'autres pays. Toutes les marques de tiers appartiennent à leurs propriétaires respectifs.

a50009462FRE, Rev. 2

HEWLETT PACKARD ENTERPRISE

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

