



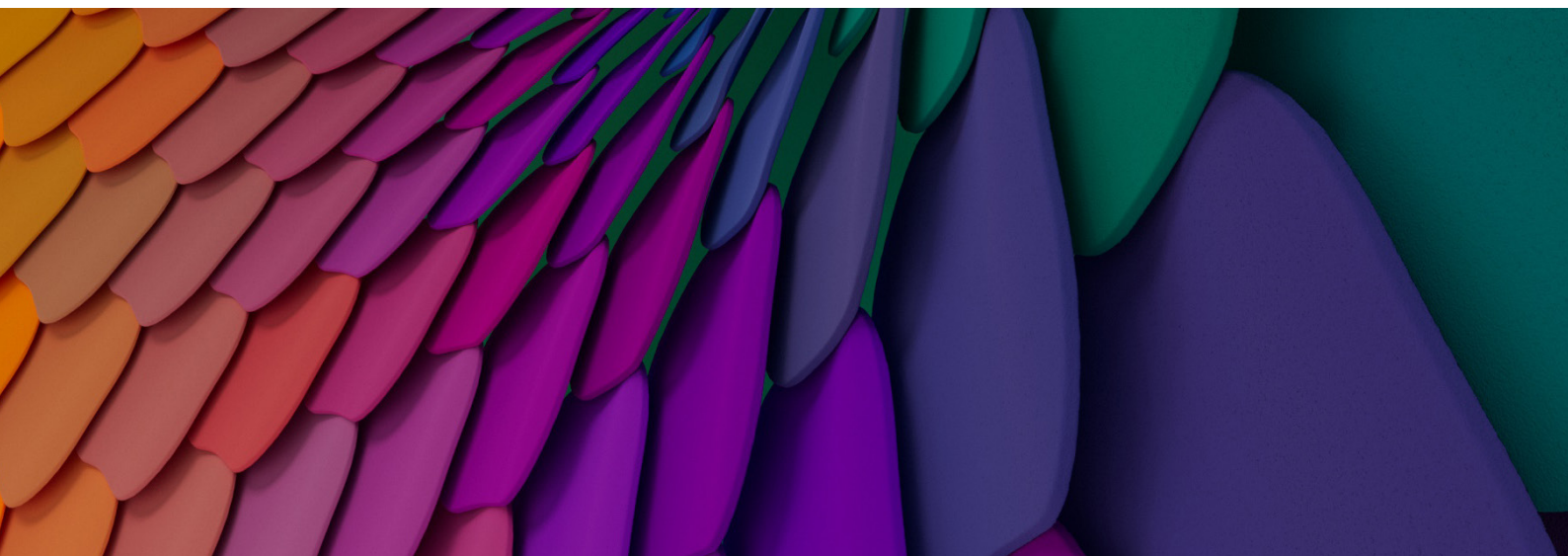
De un vistazo

HPE aruba
networking

Autenticación en la nube para HPE Aruba Networking Central

Incorporación sin fisuras basada en la nube y política segura basada en roles para usuarios y dispositivos

HPE 
GreenLake



Características y ventajas principales

- Flujos de trabajo que ahorran tiempo para configurar y administrar políticas de incorporación, autorización y autenticación para redes cableadas e inalámbricas a través de la nube
- Integración en almacenes de identidades en la nube comunes, como Google Workspace y Azure Active Directory
- Fácil incorporación de dispositivos cableados e inalámbricos con autenticación 802.1X, autenticación MAC para dispositivos que no sean 802.1X o con claves precompartidas múltiples (MPSK), lo que elimina la necesidad de registro previo
- Experiencia de usuario final simplificada mediante una aplicación cliente (móvil, sobremesa, portátil) con soporte para una amplia gama de dispositivos
- Seguridad mejorada con Client Insights basado en IA para proteger las autenticaciones basadas en MAC
- Acceso de visitantes transparente y sin problemas para dispositivos móviles con HPE Aruba Networking AirPass

La dinámica empresarial ha cambiado en los últimos años para dar la bienvenida a un volumen sin precedentes de trabajadores remotos, así como a aquellos que trabajan en entornos híbridos. Sin embargo, el acceso poco seguro a la red y los nuevos problemas de seguridad pueden causar disrupción en el negocio y hacer que las llamadas al servicio de asistencia técnica se disparen.

Aplicar controles de seguridad coherentes y garantizar que los usuarios tengan acceso sin inconvenientes a las aplicaciones y los datos en la oficina, en casa y durante sus desplazamientos es un mandato fundamental. HPE Aruba Networking Central simplifica este proceso para el equipo de TI con el control de acceso a la red (NAC) basado en la nube Cloud Auth, ampliando su capacidad de ofrecer un único punto de visibilidad, así como control sobre toda la infraestructura de red y los servicios de seguridad relacionados.

Gracias a una interfaz y un panel de control fáciles de usar, HPE Aruba Networking Central facilita la incorporación de nuevos clientes, así como la supervisión y la solución de problemas que impiden a los usuarios conectarse a la red. Los usuarios finales se autentican y se les proporcionan autorizaciones para el acceso adecuado a la red mediante de políticas detalladas configuradas por el administrador en HPE Aruba Networking Central.

Ante las crecientes preocupaciones sobre la privacidad, HPE Aruba Networking Central aprovecha 802.1X para la incorporación de dispositivos corporativos y autenticaciones basadas en MAC para dispositivos que no son 802.1X. Estos métodos de autenticación, combinados con Client Insights basado en IA, capturan y elaboran perfiles de todos los dispositivos de la red para lograr una mejor visibilidad y seguridad.

Identidad en la nube

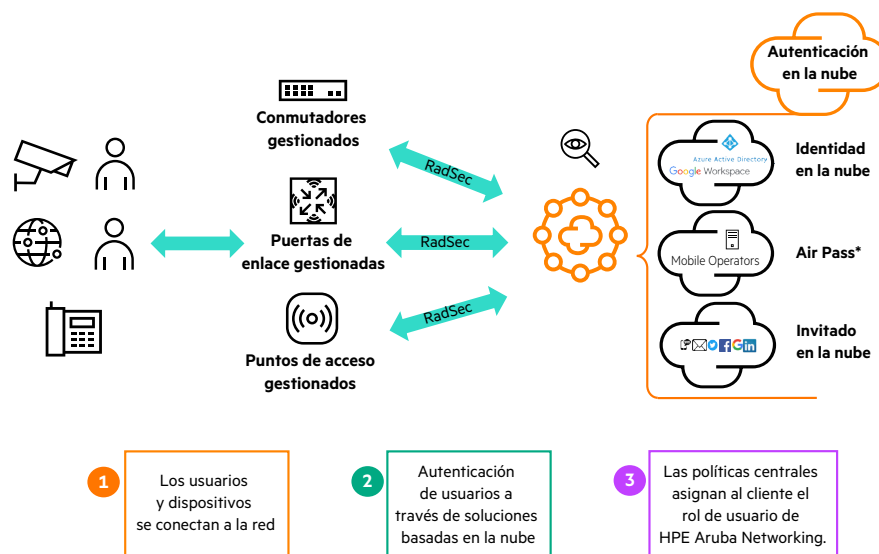
Cloud Auth en HPE Aruba Networking Central permite a los usuarios finales conectarse a redes cableadas e inalámbricas de forma segura y automática. El servicio de seguridad nativo de la nube se integra con el almacén de identidades de la nube previo de una empresa, como Google Workspace o Azure Active Directory, para autenticar la información del usuario y asignarle el nivel correcto de acceso a la red.

Seguridad automatizada a escala del extremo a la nube

Cloud Auth es una parte integral de HPE Aruba Networking Central NetConductor, que optimiza la adopción del acceso basado en identidad y simplifica las operaciones de TI al ofrecer servicios avanzados de configuración, administración y seguridad nativos de la nube, que incluyen automatización y organización de políticas basadas en intenciones, y detección y creación de perfiles basados en IA de todos los clientes conectados.

Para obtener más información, consulta la [página de la solución NetConductor de HPE Aruba Networking Central](#).





* La función Air Pass está disponible para su uso en Estados Unidos.

Figura 1. Interacciones de alto nivel.

Incorporación de dispositivos de usuario final

Los dispositivos de los empleados se pueden configurar fácilmente para una conexión fluida a redes cableadas e inalámbricas. Administrados a través de HPE Aruba Networking Central, los usuarios finales se autentican a través del almacén de identidades en la nube de la empresa con un enlace de inscripción proporcionado en HPE Aruba Networking Central. Utilizando las credenciales de la empresa para iniciar sesión, el usuario será redirigido al almacén de identidades para su autenticación. La incorporación se puede simplificar aún más aprovechando claves precompartidas múltiples (MPSK). Se trata de frases de contraseña únicas para cada usuario o contraseñas fáciles de recordar que no requieren el registro del dispositivo y pueden utilizarse para más de uno de los dispositivos del usuario.

MPSK también permite una conectividad perfecta de dispositivos no vinculados a usuarios individuales, como teléfonos IP, cámaras y termostatos, al desvincular las contraseñas de las cuentas de usuario. En lugar de ello, los administradores generan automáticamente claves únicas para cada uno de los dispositivos y las distribuyen al personal del lugar. Esto proporciona control total a los administradores, ya que ahora pueden restablecer contraseñas y habilitar/deshabilitar claves según sea necesario.

Los dispositivos cliente se pueden configurar mediante HPE Aruba Networking Onboard, una aplicación cliente que instala un perfil Enterprise Passpoint en el dispositivo cliente. Con el perfil Enterprise Passpoint, cada vez que el usuario entre dentro del alcance de la red, el dispositivo cliente se conectará automáticamente con las reglas de acceso a la red adecuadas configuradas por el administrador a través de HPE Aruba Networking Central.

HPE Aruba Networking Onboard ofrece renovaciones automáticas, sin necesidad de pasos de incorporación adicionales ni mantenimiento por parte del usuario final, al tiempo que permite al administrador cambiar y actualizar las políticas en cualquier momento. Compatible con los sistemas operativos macOS, Windows, iOS y Android.

La autorización de portal cautivo es otro método que permite a los usuarios acceder a Wi-Fi introduciendo sus datos en una página de bienvenida. Los administradores de TI tienen la flexibilidad de elegir entre varios métodos de autenticación: 802.1x, basado en MAC, MPSK, portal cautivo y aplicación HPE Aruba Networking Onboard según las necesidades empresariales.



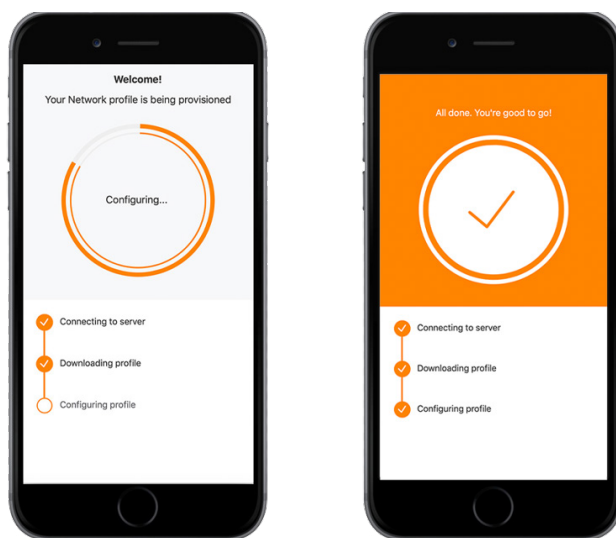


Figura 2. La aplicación cliente HPE Aruba Networking Onboard proporciona una manera fluida para que los usuarios finales se conecten a las redes corporativas.

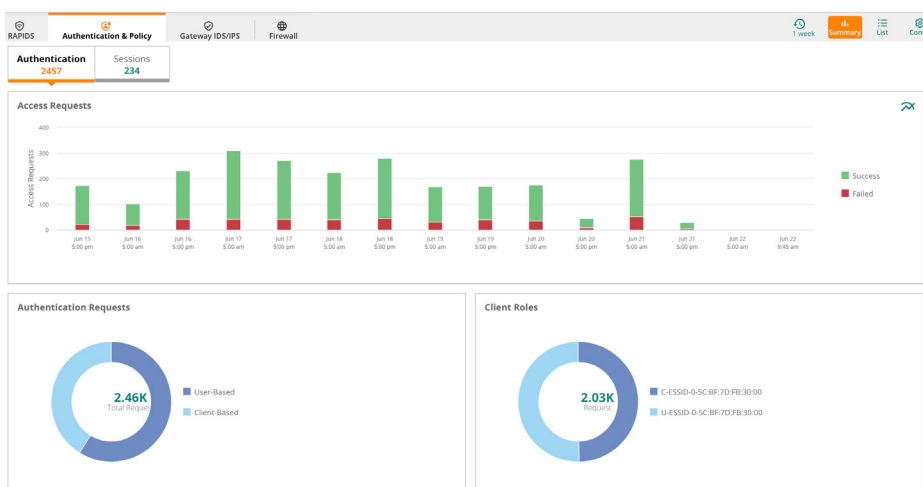


Figura 3. La visibilidad de todas las solicitudes de autenticación y los clientes conectados ayudan al departamento de TI a solucionar fácilmente posibles problemas.

Supervisión dinámica de la política de acceso de los clientes

Se pueden definir políticas de acceso detalladas en HPE Aruba Networking Central según el tipo de dispositivo cliente. Client Insights asigna etiquetas definidas por el sistema o etiquetas personalizadas para identificar o agrupar lógicamente a clientes con características similares. La autenticación en la nube permite una postura de seguridad más sólida al supervisar dinámicamente las etiquetas del cliente e iniciar una desconexión cuando se detecta un cambio de etiqueta, lo que garantiza que el cliente reciba políticas de acceso que correspondan a la nueva etiqueta.





Supervisión y resolución de problemas de conectividad de red

El panel de autenticación en la nube de HPE Networking Aruba Central proporciona visibilidad granular de las solicitudes de autenticación de los usuarios, así como detalles de la sesión para los clientes que están conectados a puntos de acceso administrados por HPE Networking Aruba Central.

Desde la pestaña de autenticación, el administrador de TI puede ver datos sobre la cantidad de solicitudes de acceso exitosas y fallidas en un rango de tiempo seleccionado, e incluye desgloses de solicitudes de usuario frente a cliente, roles de cliente y motivos de fallo (por SSID, política y motivos de rechazo).

La pestaña de sesiones muestra métricas como la cantidad de sesiones activas, direcciones MAC (aleatorias y no aleatorias), la duración de cada sesión y el uso de datos durante cada sesión dentro de una duración seleccionada.

Acceso de visitantes transparente y sin inconvenientes para dispositivos móviles

[HPE Aruba Networking Air Pass*](#) es la primera solución de roaming para móviles sin fisuras del sector, diseñada para unificar las experiencias de redes empresariales y móviles.

Air Pass se administra en HPE Aruba Networking Central, lo que extiende la experiencia 5G a la empresa mediante la tecnología wifi de Aruba. AirPass utiliza acuerdos prenegociados con operadores de redes móviles (MNO).

AirPass ofrece a los invitados y visitantes una experiencia wifi ininterrumpida en espacios interiores con el beneficio adicional de la seguridad de nivel empresarial.

Incorporación optimizada de sensores UXI

Flujo de trabajo optimizado para la incorporación de sensores UXI sin intervención manual mediante Wi-Fi Easy Connect™ seguro y estandarizado, también conocido como protocolo de aprovisionamiento de dispositivos (DPP). Una vez que se registra un sensor UXI, puede conectarse e integrarse automáticamente según la configuración habilitada por el administrador.

*Actualmente, Air Pass solo está disponible en EE. UU.



Resumen

A medida que las organizaciones siguen dando soporte a más trabajadores remotos, cada vez es más importante proteger a los usuarios y los dispositivos para garantizar que se proporcionan los niveles de acceso adecuados para la continuidad de la actividad empresarial, al tiempo que se aumenta la eficacia en las aprobaciones y políticas administrativas.

Cloud Auth en HPE Networking Aruba Central ofrece una solución de NAC e incorporación basada en la nube sin fisuras. Las pequeñas y medianas empresas con personal de TI limitado se beneficiarán de flujos de trabajo simplificados y políticas seguras basadas en roles administradas a través de HPE Aruba Networking Central para garantizar que los usuarios y dispositivos tengan un acceso a la red adecuado. La experiencia de los usuarios finales se amplifica con la aplicación cliente HPE Aruba Networking Onboard, que admite una amplia gama de dispositivos y permite una conectividad sin fisuras a la red mediante perfiles que se renuevan automáticamente en nombre del usuario.

Recursos

Para obtener más información, consulta los siguientes recursos o ponte en contacto con tu representante de ventas de HPE Aruba Networking:

[HPE Aruba Networking Central](#)

[Client Insights basado en IA en HPE Aruba Networking Central](#)

[HPE Aruba Networking Central NetConductor](#)

Toma la decisión de compra correcta.
Contacta con nuestros especialistas
en preventa.



Contáctanos

Visita ArubaNetworks.com



Hewlett Packard
Enterprise

© Copyright 2024 Hewlett Packard Enterprise Development LP. La información aquí contenida está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de Hewlett Packard Enterprise figuran en las declaraciones expresas de garantía incluidas en los mismos. Nada de lo que aquí se indica debe interpretarse como una garantía adicional. Hewlett Packard Enterprise no se responsabilizará de los errores u omisiones técnicos o editoriales que pudiera contener el presente documento.

Todas las marcas de terceros pertenecen a sus respectivos titulares.

AAG_CloudAuthenticationforCentral_LP_031924 a00115477ese