Claro Wifi360°

HomePass®

Manual de la aplicación móvil

Plume®

HomePass

HomePass es una aplicación que le permite supervisar y gestionar de forma más eficiente su red WiFi y la conectividad de sus usuarios.

Tabla de contenidos

Instalación de la App
Google Play App Store

Gestión de los Pods (extensores)

Pruebas de Velocidad

Plume Control
Accesos

Plume Guard
Protección en línea

Soporte
técnico y cuenta

Instalación de la aplicación

Descargar la aplicación

En Android y IOS, encontrará la aplicación HomePass by Plume Design Inc. Que podrá identificar fácilmente por su logotipo.

Proceda con la descarga e instalación en su smartphone.

Instalación de la aplicación

Iniciar sesión en HomePass

Abra la aplicación e ingrese en “Iniciar Sesión”.

Ingrese el mismo correo que se especificó al contratar este servicio.

Se enviará un correo electrónico para validar la instalación.

Luego del mensaje de confirmación, ya se puede usar la aplicación.

Navegación por la aplicación

Pantalla de inicio

La apariencia, navegación y funcionalidades son las mismas en las versiones para Android y IOS.

Las pestañas en la parte inferior permiten un acceso rápido a las 3 pantallas principales de la aplicación.

- **Pantalla de inicio**
- **Personas**
- **Configuración de la aplicación**

iOS

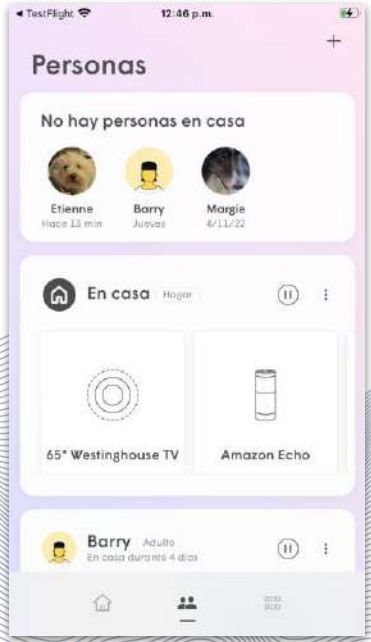
Android

Navegación por la aplicación

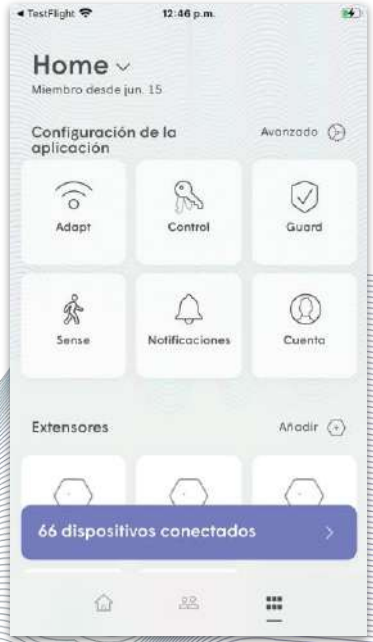
Pantallas principales

- **Pantalla de inicio:** En esta parte se ofrece una visión general del estado actual de la red y se ofrece una vista de alto nivel de los eventos de Guard, Sense, Control y Adapt.
- **Personas:** En esta parte se gestionan los usuarios de la red y sus funciones relacionadas con Control, tales como los Tiempos de espera y el Congelamiento de Internet.
- **Configuración de la aplicación:** En esta área se gestionan todas las funciones y configuraciones de HomePass.

Inicio



Personas



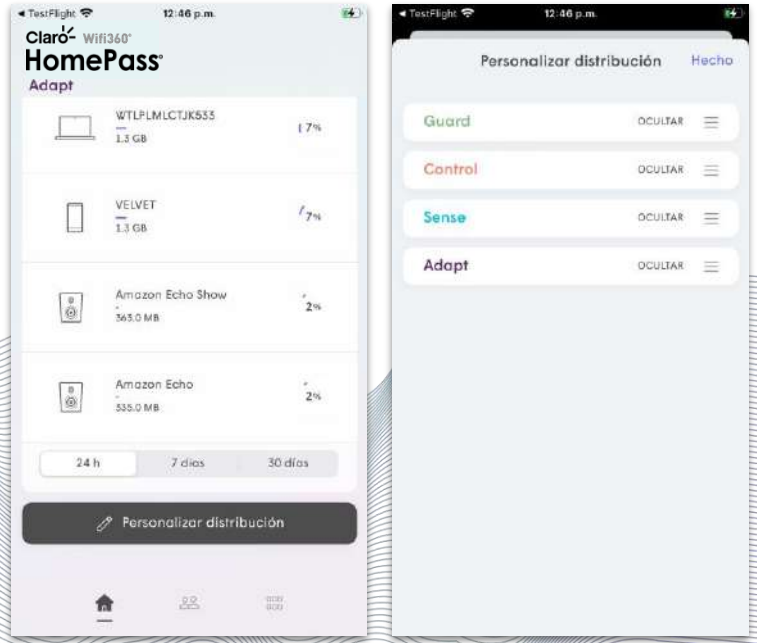
Configuración de la aplicación

Navegación por la aplicación

Pantalla de inicio

Se puede personalizar el diseño de la pantalla de inicio de HomePass 2.0. Los usuarios pueden editar el orden de las tarjetas mostradas u ocultarlas según sus preferencias.

Si quieres personalizar el diseño de la pantalla de inicio, desplázate hasta la parte inferior de la pantalla de inicio y elige Personalizar diseño.



Navegación por la aplicación

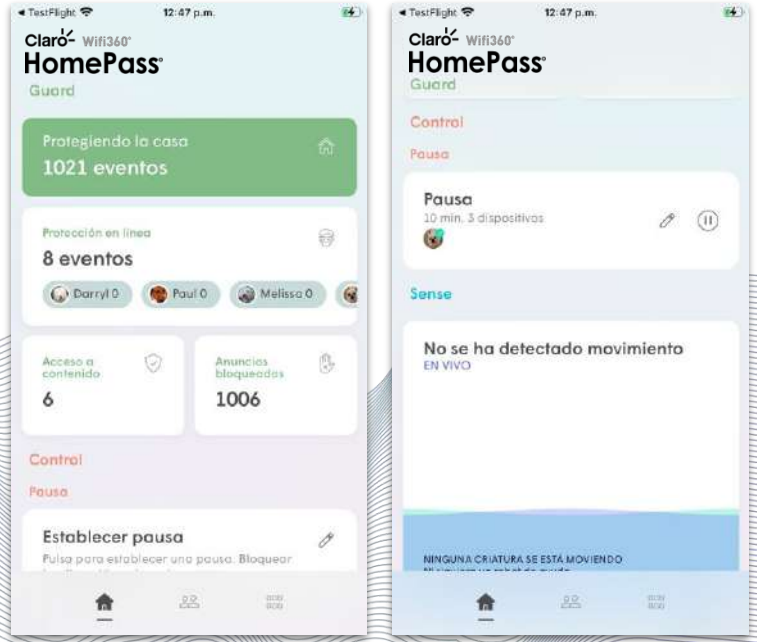
Secciones de la pantalla de inicio

Guard

- Muestra el estado actual de Guard y una vista de alto nivel de la protección en línea, la protección avanzada de IoT, el bloqueo de anuncios y los eventos de Acceso a contenidos

Control

- **Tiempo de espera:** Muestra los usuarios o dispositivos que se encuentran congelados. Te permite establecer un tiempo de espera global.



Navegación por la aplicación

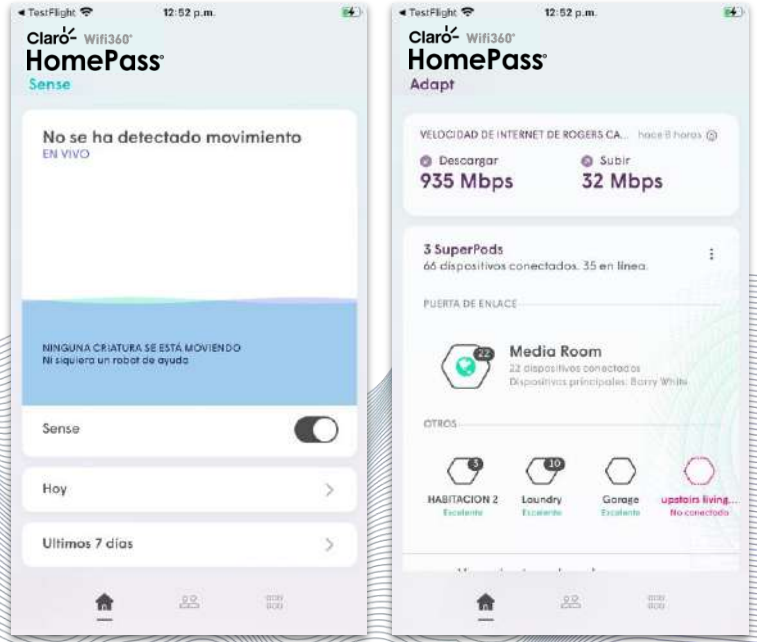
Secciones de la pantalla de inicio

Sense

- **Vista en vivo**: Muestra el movimiento actual que hay en el hogar.
- **Hoy y los últimos 7 días:** También se pueden obtener las vistas del historial de movimiento. Al tocar estos recuadros se abre la configuración de Sense.

Adapt

- **Velocidad de internet del ISP:** Muestra los resultados más recientes de la prueba de velocidad del ISP. Al tocar este recuadro se abre el historial de pruebas de velocidad y se puede realizar una prueba de velocidad ISP de forma manual.
- **Gateway**: Muestra todos los nodos conectados a Ethernet (nodos Gateway) y muestra el estado general de la red, incluyendo la cantidad de dispositivos.
- **Otros**: Muestra el estado actual de cada pod (extensor) conectado a Wi-Fi. Al tocar las opciones, aparecen las opciones Localizar y nombrar Nodos, Añadir un pod y Comprar un nodo.
- **Ver cobertura de la red**: Muestra la vista de la topología

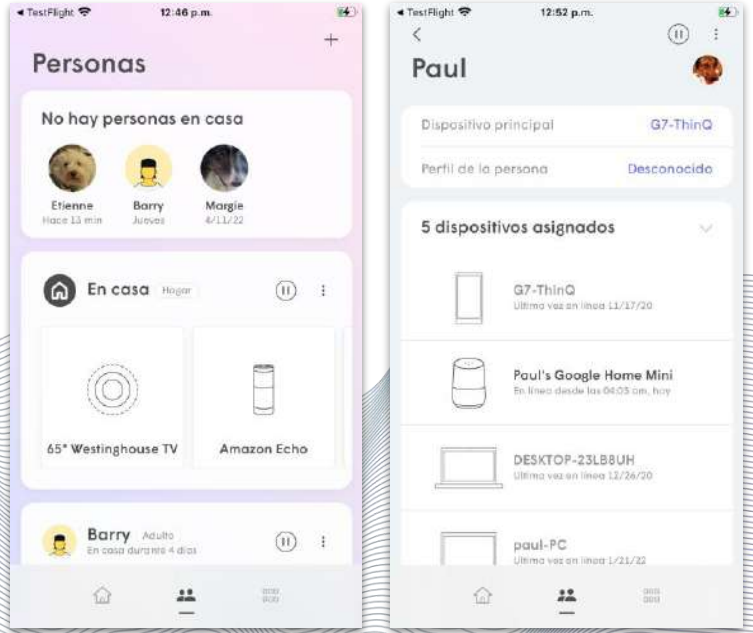


Navegación por la aplicación

Personas

La pantalla Personas es el lugar donde se gestionan los usuarios individuales de la red.

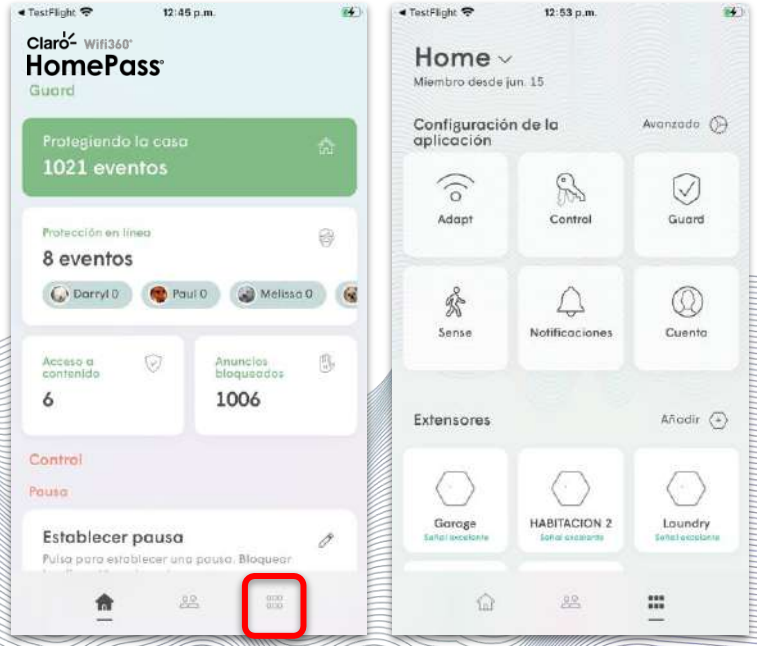
- **Personas es casa:** Muestra una lista de todas las personas que se encuentran actualmente en casa según el estado de conexión de su dispositivo principal a la red.
- **En casa** - Se utiliza para los dispositivos no asignados - Todos los nuevos dispositivos que se conecten a la red se añadirán a esta tarjeta hasta que se asignen a una persona.
- **Tarjetas de personas:** Muestra un resumen de cada persona en la red. Al pulsar sobre una tarjeta se pueden cambiar los dispositivos asignados, establecer el perfil de la persona para que acceda a los contenidos, se quede inactivo, se congele y se le invite a la aplicación HomePass.



Navegación por la aplicación

Configuración de la aplicación

- **Adapt**: Cambia el SSID.
- **Control**: Permite gestionar y crear contraseñas para el acceso al WiFi.
- **Guard**: Protección en línea, Protección avanzada de IoT™, Bloqueo de anuncios y Modo de privacidad.
- **Sense**: Detección de movimiento
- **Comando**: Controla tu red HomePass mediante asistentes de voz.
- **Notificaciones**: Gestiona las notificaciones push que se envían desde la red HomePass
- **Cuenta**: Cierra la sesión de la cuenta o cambia de cuenta. Consulta la información de afiliación, en caso de que sea necesario.
- **Avanzado**: Reservas y reenvío de puertos, modo de red, DNS, configuración UPnP.



Configuración de la aplicación

Extensores

- **Recuadros de Pod** : Se muestra el estado de cada pod (extensor) y al pulsar sobre uno de los recuadros se accede a la pantalla de detalles de ese pod.
- **Añadir**: Se utiliza para añadir un pod (extensor) disponible a la red.
- **Añadir un Pod a mi cuenta:** Abre un enlace a la tienda web correspondiente para comprar pods o extensores adicionales. Esto es opcional para los CSP.

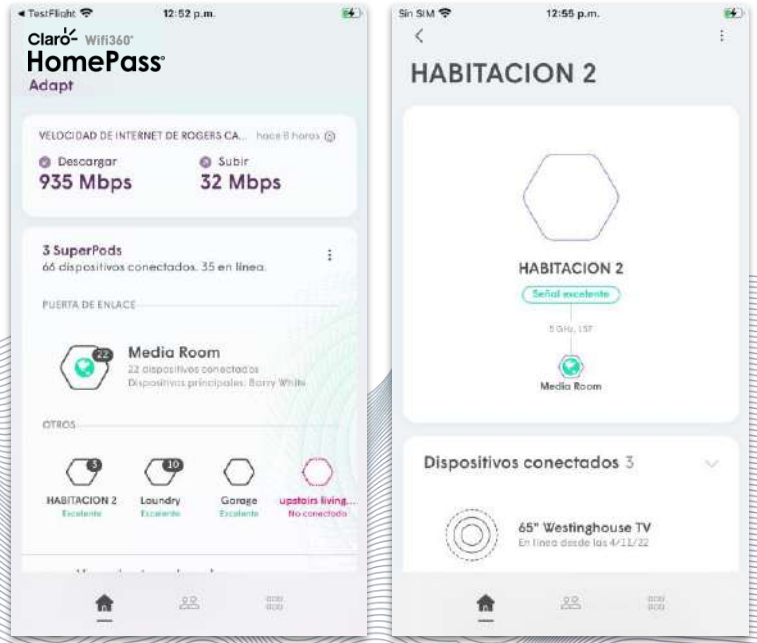
Soporte técnico

- **Preguntas frecuentes:** Abre el centro de ayuda de HomePass (base de conocimientos pública)
- **Correo electrónico**: Permite abrir un ticket de soporte Esto es opcional para los CSP.
- **Llámanos**: Llama al servicio de asistencia. Esto es opcional para los CSP.

Gestión de los Pods (extensores)

Cómo gestionar los pods (extensores)

- Si deseas acceder a la lista de pods (extensores), desplázate hasta la sección **Adapt.**
- Los usuarios pueden hacer clic en los Pods (extensores) para ver los detalles.



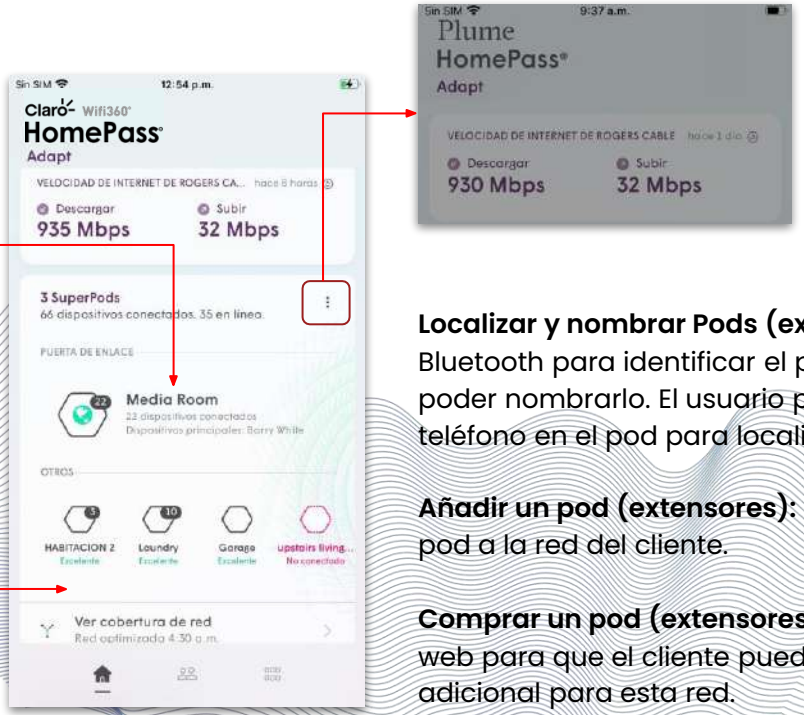
Adapt

Velocidad de Internet: Ofrece información Sobre la última prueba de velocidad.

Nombre del pod: Al pulsar el nombre de un pod se abrirá la pantalla de detalles del pod.

Al pulsar sobre el nombre de cada pod se abrirán opciones adicionales del mismo.

- Cambiar el nombre de este Pod
- Localizar y nombrar el Pod
- Eliminar este Pod
- Ver información del hardware



Localizar y nombrar Pods (extensores): Utiliza el Bluetooth para identificar el pod más cercano y poder nombrarlo. El usuario puede tocar su teléfono en el pod para localizarlo de inmediato.

Añadir un pod (extensores): Añade un nuevo pod a la red del cliente.

Comprar un pod (extensores): Abre la tienda web para que el cliente pueda comprar un pod adicional para esta red.

Pantalla de detalles del pod (extensores)

Imagen del pod – Al pulsar la imagen del pod, el led del pod empieza a parpadear para identificarlo visualmente durante el cambio nombre. El pod seguirá parpadeando durante 20 minutos o hasta que se cambie el nombre del pod.

Nombre del pod: Al pulsar esta opción se puede editar el nombre del pod.

Jerarquía del pod: Muestra la forma en que este pod se conecta al resto de la red, hasta el pod de Gateway. Al tocar cualquiera de los pods que aparecen aquí, se abrirá la pantalla de detalles de ese pod.

Opciones adicionales: Muestra las siguientes opciones para este pod:

- Renombrar este pod
- Localizar y nombrar el pod
- Eliminar este pod
- Ver información del hardware

Calidad de la conexión: Indica la calidad de la conexión de este pod con su unidad madre inmediata. Al tocar esta opción, se obtiene una descripción de los diferentes niveles de calidad.

Lista de dispositivos conectados: Muestra todos los dispositivos que se han conectado a este pod, incluyendo la imagen de la persona asignada si está disponible. Al tocar el dispositivo se abrirá la pantalla de detalles de ese dispositivo.

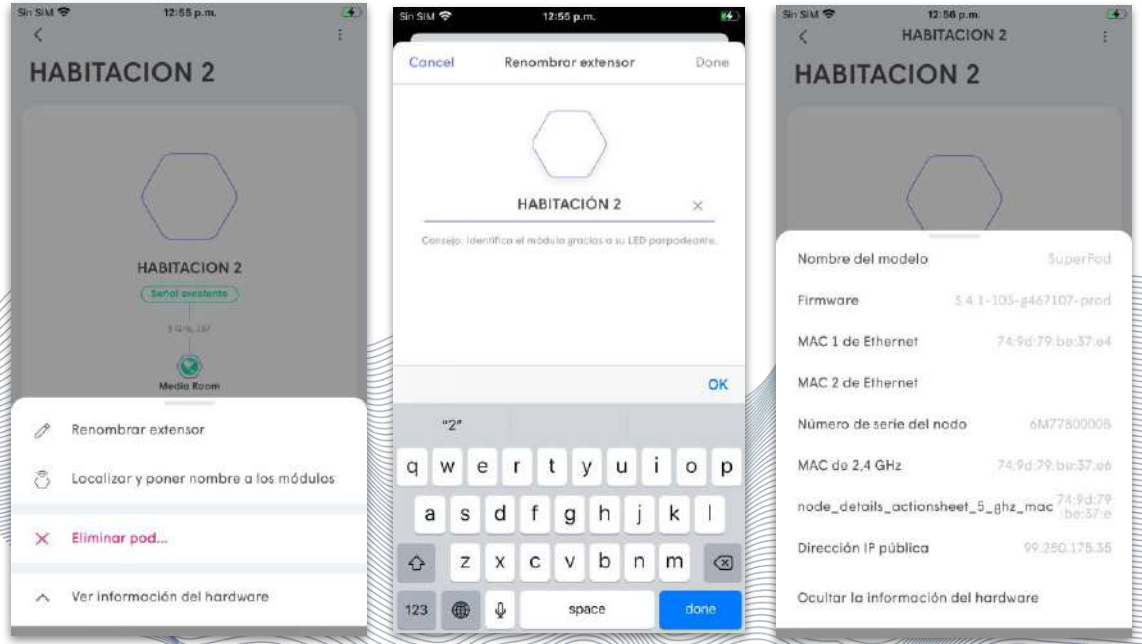
Opciones del pod (extensores)

Cambiar el nombre del pod: Por defecto, a los pods se les asignan los nombres Habitación 1, Habitación 2, etc., según el orden en que se añadieron a la cuenta. Al cambiar el nombre se puede identificar mejor la ubicación de cada pod.

Localizar y nombrar: Utiliza el Bluetooth para identificar el pod más cercano y poder nombrarlo. El usuario puede tocar su teléfono en el pod para localizarlo de inmediato.

Eliminar pod: Elimina el pod de la red

Ver información del hardware: Ofrece información como el firmware, el número de serie y las direcciones MAC.



Salud del pod (extensores)

La clasificación de la salud del pod que se muestra se basa en la conexión con la unidad madre inmediata de ese pod. La clasificación no tiene en cuenta todas las conexiones de los pods que se encuentran situados más arriba, ni la velocidad que se suministra en la puerta de enlace.

Al pulsar sobre la clasificación de salud aparece una descripción de lo que significa cada clasificación y una descripción del impacto esperado.

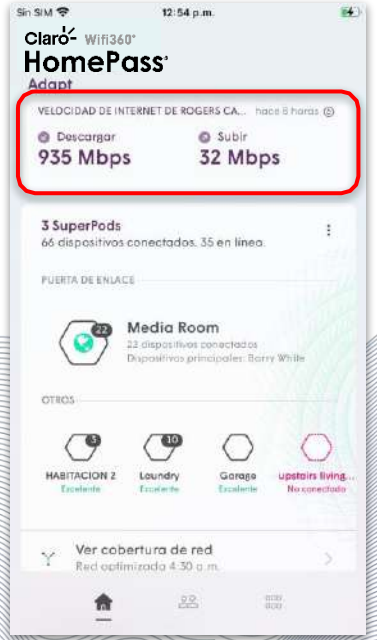
Pruebas de velocidad

Tipos de pruebas de velocidad

Hay dos pruebas de velocidad diferentes integradas en la aplicación HomePass.

- Prueba de velocidad ISP (velocidad WAN)
- Velocidad del dispositivo

Desde la pantalla de inicio, desplázate hasta la **sección Adapt,** la aplicación mostrará el último resultado obtenido para la velocidad del ISP. Al pulsar sobre los resultados, aparecerá el historial de pruebas de velocidad.
Al utilizar los servidores de Ookla, la prueba de velocidad del ISP se ejecuta en el propio pod de Gateway, midiendo la velocidad que ofrece el ISP.



Al realizar una prueba de velocidad, utilizará todo el ancho de banda disponible para ver cuánto hay disponible. Por esta razón, las pruebas de velocidad del ISP solo se ejecutan cuando la red no está ocupada.

Pruebas de velocidad de ISP

Esta prueba se ejecuta automáticamente una vez cada 12 horas, aunque solo cuando no hay tráfico en la red.

Se muestra un historial de pruebas de velocidad , tanto de **carga** como de **descarga,** que puede ordenarse para las **últimas 24 horas**, **7 días** o **30 días**.

También se resaltan las velocidades mínimas y máximas que se han medido durante el periodo de tiempo seleccionado.

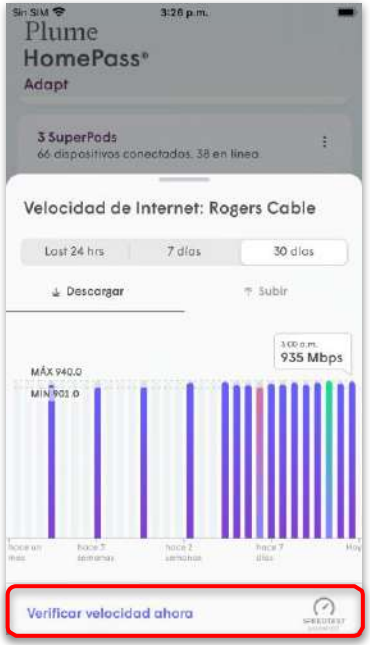
Pruebas de velocidad

Pruebas de velocidad de ISP

Al pulsar sobre **Comprobar velocidad ahora**, se activará manualmente otra prueba de velocidad del ISP.
Las pruebas de velocidad ISP manuales pueden realizarse desde la aplicación incluso desde ubicaciones remotas siempre que haya una conexión a Internet y la red Plume esté en línea.

Temporización automática de la prueba de velocidad de ISP

La temporización de las pruebas de velocidad ISP automáticas viene determinada por factores de la red local. El momento en que se activaron las pruebas de velocidad, el momento en que se ejecutó la última prueba de velocidad y el estado de ocupación de la red son factores que determinan el momento en que se ejecutará la siguiente prueba.
Por ello, no todas las redes realizarán una prueba de velocidad ISP al mismo tiempo.



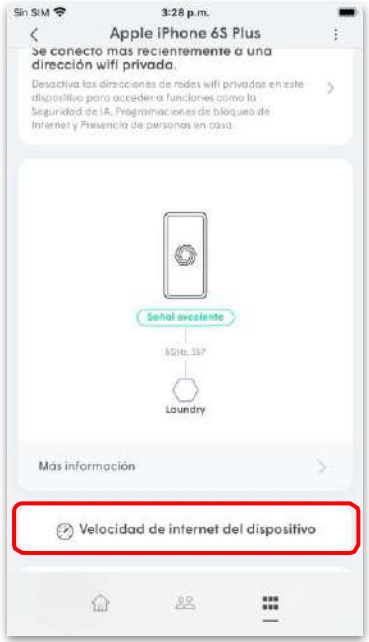
Pruebas de velocidad

Pruebas de velocidad del dispositivo

Al pulsar sobre el dispositivo que ejecuta la aplicación HomePass, aparecerá la pantalla de detalles de ese dispositivo. A partir de ahí, puedes probar la **velocidad de Internet del dispositivo**.

Una prueba de velocidad del dispositivo mide la velocidad de Internet que se entrega a ese dispositivo a través de todas las conexiones que tiene que pasar en
la red. Los resultados se verán limitados por la calidad de la conexión del ISP, las conexiones de un pod a otro, la conexión del dispositivo y sus propias capacidades WiFi.

Para acceder a la prueba de velocidad de Internet del dispositivo, abre la tarjeta del dispositivo que esté utilizando la aplicación HomePass.



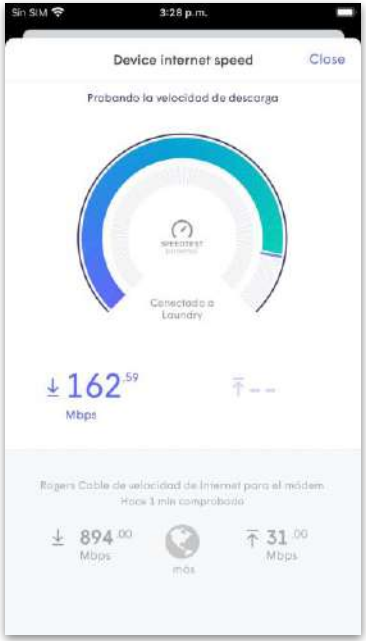
Pruebas de velocidad del dispositivo

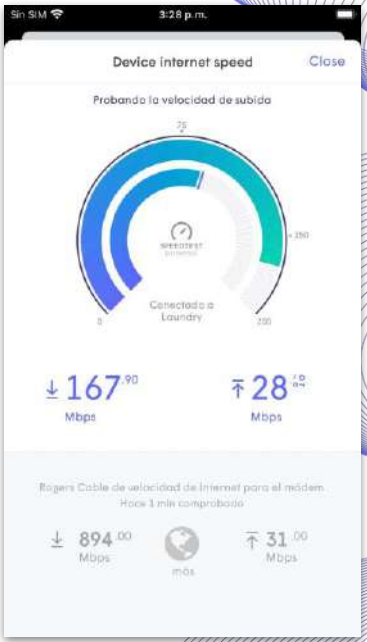
Verifica que el dispositivo esté conectado a la red WiFi de Plume y que no esté conectado a una red celular u otra red WiFi antes de probar la **velocidad de Internet del dispositivo**.

La prueba ejecutará tanto una prueba de descarga como de carga.

Al finalizar, un mensaje en la parte superior de la pantalla ofrecerá algunas expectativas de rendimiento del cliente basadas en los resultados.

Siempre se mostrarán los resultados de la prueba de velocidad de Internet del dispositivo anterior.





Plume Control

Control™ - Gestión de contraseñas WiFi

Las funciones de gestión de contraseñas WiFi de Control™ permiten a los usuarios establecer hasta 30 contraseñas diferentes para una sola red WiFi SSID. De este modo, cada miembro de la casa puede tener sus propias credenciales independientes que se utilizan exclusivamente para sus dispositivos y aún queda bastante para los invitados individuales. Otras características de Control incluyen el control de Acceso a contenidos.

Se pueden establecer tres zonas de acceso independientes:

- **Hogar (todo el acceso)**: Concede un acceso WiFi doméstico completo a las personas en las que confías expresamente. De esta forma, tus dispositivos podrán interactuar con todos los demás dispositivos conectados en tu casa. La primera contraseña que se cree durante la configuración inicial se encuentra en esta zona.
- **Invitado (acceso limitado)** - Crea contraseñas personalizadas para cada invitado y luego elige a qué dispositivos conectados de la zona Hogar (impresoras, televisiones, cámaras de seguridad o termostatos) pueden acceder para que se sientan al momento como en casa.
- **Solo Internet -** Los dispositivos con contraseñas WiFi de solo Internet se conectarán únicamente a Internet y no a ninguno de los dispositivos conectados en tu casa.

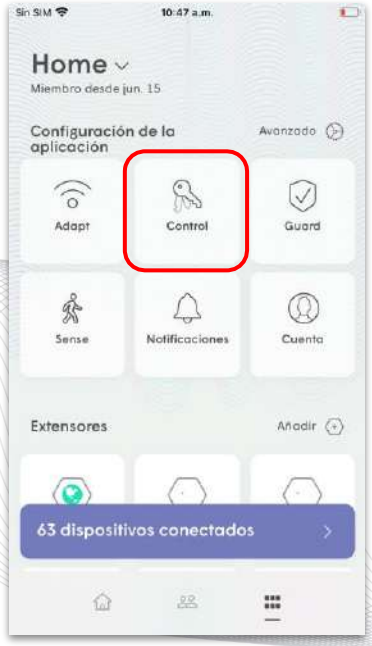
Al usar la aplicación HomePass, se puede desactivar o eliminar cualquier contraseña en cualquier momento por el administrador en caso de que se vea comprometida. Las contraseñas de invitados y de solo Internet también se pueden desactivar de forma programada, para que no se puedan utilizar una vez que los invitados se marchen.

Plume Control

Gestión de contraseñas WiFi

Desde la pantalla de inicio, pulsa en **Configuración de la aplicación** para acceder al menú principal.

Pulsa en **Control** para gestionar las contraseñas.



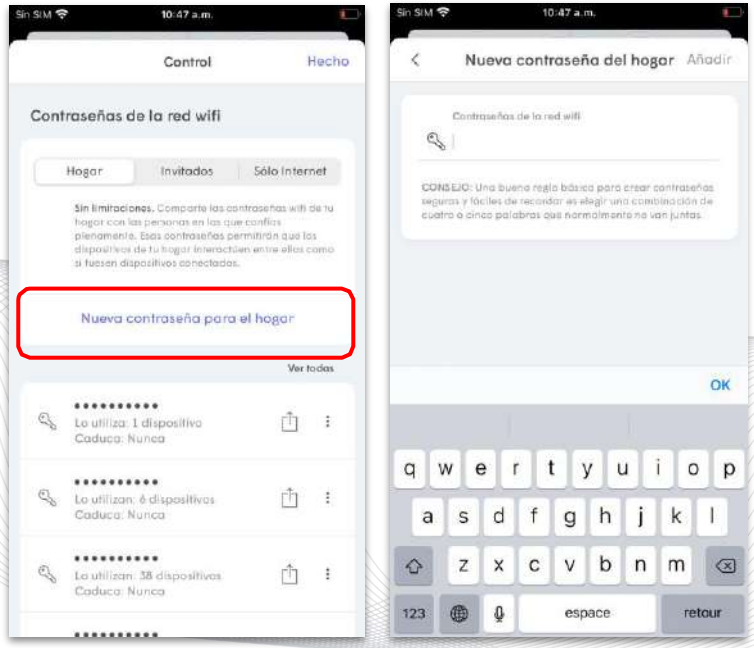
Contraseñas de inicio

Para crear una nueva contraseña de Inicio, elige la pestaña de **Inicio.**

Pulsa en Nueva contraseña de inicio

Las contraseñas deben tener entre 8 y 64 caracteres y pueden incluir letras mayúsculas y minúsculas, números y caracteres especiales.

Toca la marca de verificación verde para guardar la nueva contraseña.



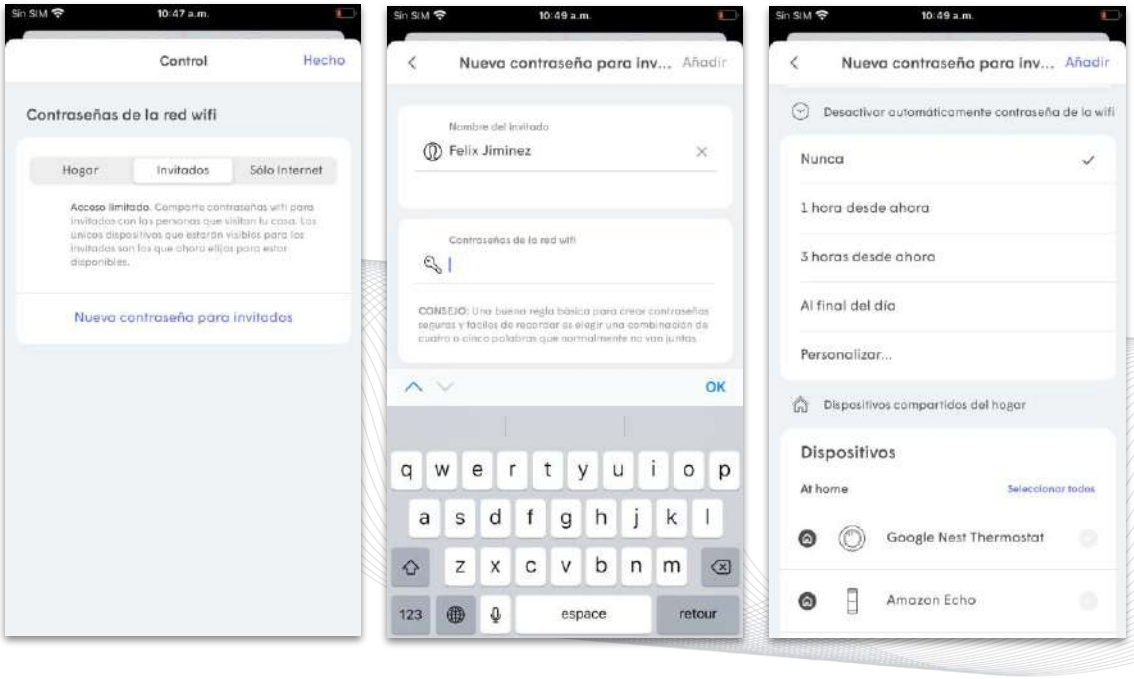
Contraseñas de invitados

Para crear una nueva contraseña de invitado, elige la pestaña **Invitado.**

Pulsa en **Nueva contraseña de invitado** en iOS o el icono azul + si utilizas Android.

Ingresa un nombre de invitado y luego la contraseña de WiFi.

Elige la opción **Desactivar automáticamente la contraseña WiFi** y los **dispositivos** de la zona doméstica que se van a compartir en la red local.



Contraseñas de solo Internet

Para crear una nueva contraseña de solo Internet, elige la pestaña de **Solo Internet** .

Pulsa Nueva contraseña de solo Internet

Elige una opción de **contraseña de WiFi de desactivación automática** y toca la marca de verificación verde para guardar la nueva contraseña.

Compartir contraseñas

Comparta fácilmente cualquier contraseña creada.

Pulsa el icono de compartir junto a la contraseña que deseas enviar.

Elige la aplicación que desees utilizar para enviar el enlace (SMS, iMessage, correo electrónico, airdrop, android beam, etc.). Solo se mostrarán las opciones disponibles en el dispositivo.

El destinatario recibirá un enlace de duración limitada que abre una página web con el SSID y su contraseña

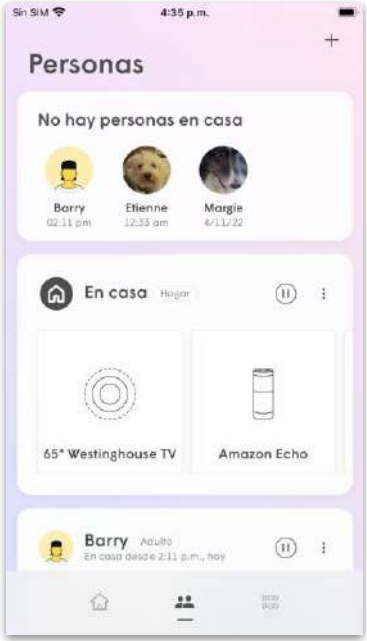
Gestión de personas

Las **tarjetas de personas** pueden ser asignadas a personas y a dispositivos específicos para que las restricciones de **Acceso a contenidos** o los tiempos de espera puedan ser establecidos para todos los dispositivos asignados al mismo tiempo.

En la pantalla de inicio, pulsa el icono de **Personas**.

Habrá dos Tarjetas ya creadas.

- **El titular de la cuenta:** Se crea durante la incorporación, con el dispositivo que ejecuta HomePass ya asignado.
- **En casa** - Se utiliza para los dispositivos no asignados - Todos los nuevos dispositivos que se conecten a la red se añadirán a esta tarjeta hasta que se asignen a una persona.



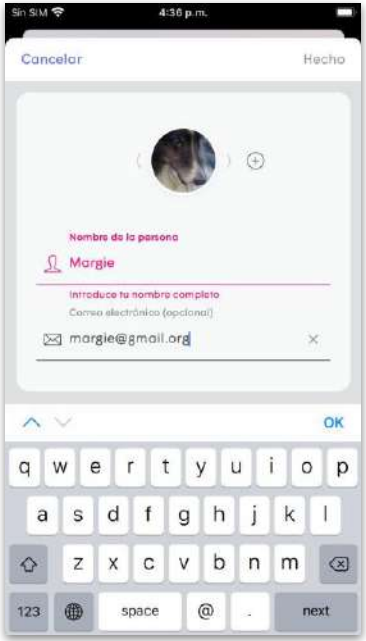
Gestión de personas

Pulsa sobre el **+** para empezar a añadir una nueva persona.

Escribe el nombre completo de la persona.

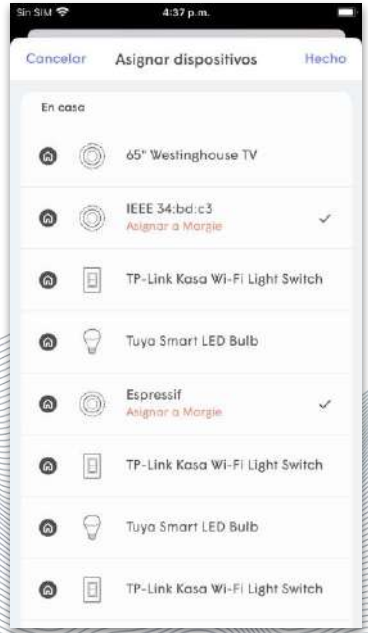
Al pulsar el icono de la cámara, podrás tomar una **Nueva foto de perfil** con la cámara o seleccionar una foto preexistente de la galería de imágenes de tu dispositivo.
También puedes usar el < > junto a la imagen para elegir un avatar. Tras crear el perfil, pulsa en los tres puntos de la parte superior
derecha de la página. De este modo, aparecerán las siguientes opciones:

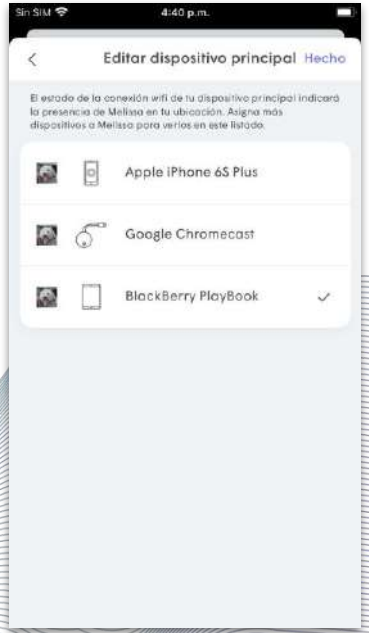
- Editar el perfil de las personas
- Editar los dispositivos asignados
- Eliminar... (eliminar el perfil)



Gestión de personas

- Elige el(los) dispositivo(s) de la lista que quieras asignar a esta persona.
  Pulsa sobre la marca de verificación verde para guardar.
  Cuando el dispositivo principal de una persona se conecta o se desconecta de la red, la función People at Home (Personas en casa) la utiliza para enviar notificaciones.
  Sense también utiliza estos eventos para determinar el estado de Hogar/Ausente.
- Pulsa **Seleccionar dispositivo principal** y elige uno de los dispositivos asignados.





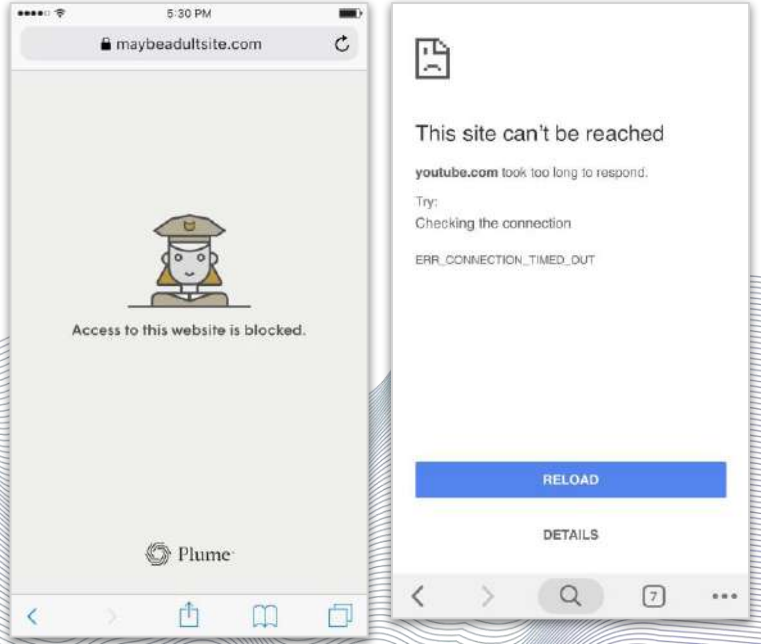
Acceso a contenidos

El **Acceso a contenidos** utiliza una base de datos de dominios conocidos para restringir a qué tipos de sitios web puede acceder la persona o el dispositivo en función de los siguientes niveles:

- **Sin límites -** No hay restricciones de contenido
- **Sin contenido para adultos** - Todo el contenido etiquetado como contenido para adultos no será accesible.
- **Contenido apto para adolescentes** - Se admite la mayoría de los contenidos, excepto los que se consideran demasiado sensibles para los adolescentes. Se filtrarán las categorías etiquetadas como NO apropiadas para adolescentes y no se podrá acceder a ellas.
- **Apropiado para niños** - Solo se podrá acceder a los contenidos apropiados para los niños más pequeños.

Acceso a contenidos

- Al intentar acceder a un sitio HTTP bloqueado por la función de Acceso a contenidos, el navegador mostrará una página con el logotipo de Plume y un mensaje de **"Se ha bloqueado el acceso a este sitio"**.
- Al acceder a un sitio web HTTPS bloqueado, se mostrará el mensaje predeterminado del navegador **"No se puede acceder a este sitio"** o **"Se ha agotado el tiempo de conexión"**.

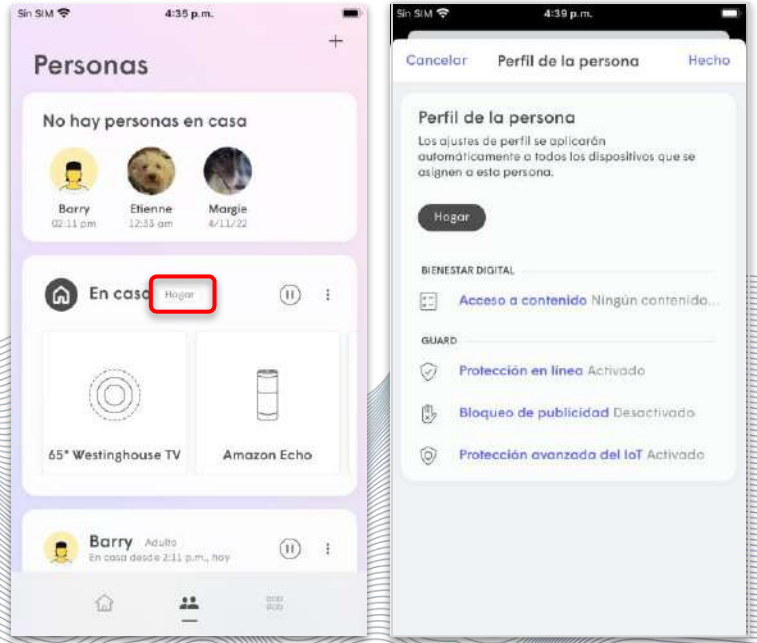


NUEVO - Perfiles de persona

Los **Perfiles de persona** aplican un conjunto de niveles de **Acceso a contenidos** y funciones de Guard a una persona o a la tarjeta de familia. Así, el usuario puede ver rápidamente a qué tipo de contenidos tiene acceso la persona. Al crear una nueva persona, es necesario aplicar un **Perfil de persona**.

Conjuntos de perfiles de persona predeterminados (Acceso a contenidos, Protección en línea, Protección avanzada de IoT, Bloqueo de anuncios)

- **Adultos -** Sin límites, Activo, Desactivado, Activado
- **Adolescente -** Apto para adolescentes, Activado, Desactivado, Activado
- **Niño -** Adecuado para niños, Activo, Desactivado, Activado
- **Familiar -** Sin contenido para adultos, Activo, Desactivado, Activado
- **Desconocido -** El perfil de la persona no se ha establecido para ella. Las reglas de acceso a contenidos preexistentes se establecieron con anterioridad como persona o de dispositivo mediante HomePass 1. Este estado se mostrará en las tarjetas de persona cuando los usuarios pasen por primera vez de la aplicación HomePass 1 a la aplicación HomePass 2.

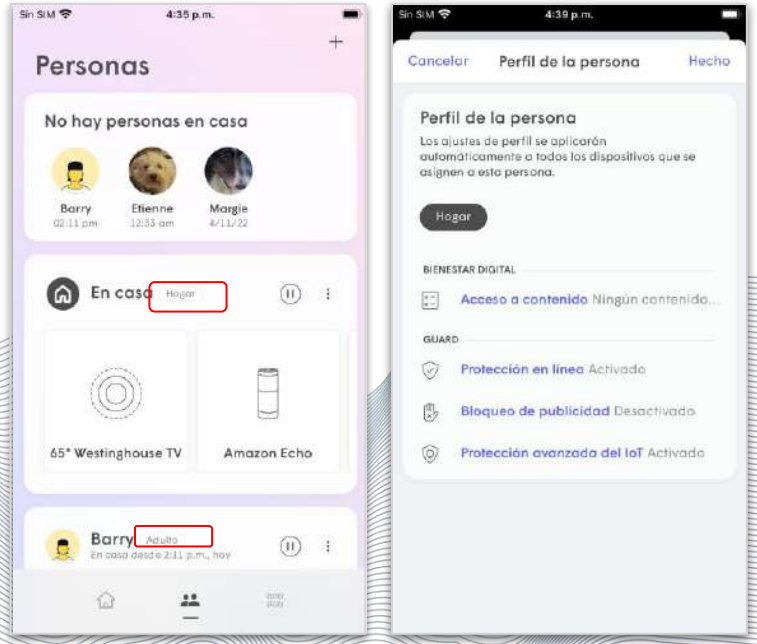


Transición a los perfiles de persona

Los usuarios existentes del HomePass original tenían las reglas de Acceso a contenidos configuradas por persona o dispositivo.

En el caso de los usuarios existentes, las reglas de Acceso a contenidos y de Guard establecidas previamente en la aplicación original de HomePass se seguirán aplicando a todos los dispositivos y continuarán funcionando como antes, aunque las tarjetas de persona mostrarán sus **perfiles de persona** como **desconocidos.**

El usuario puede actualizar el Perfil de persona a la configuración deseada para cada persona. De esta forma, los usuarios podrán ver rápidamente la regla de Acceso a contenidos que se aplica a cada persona en la lista de tarjetas personales.

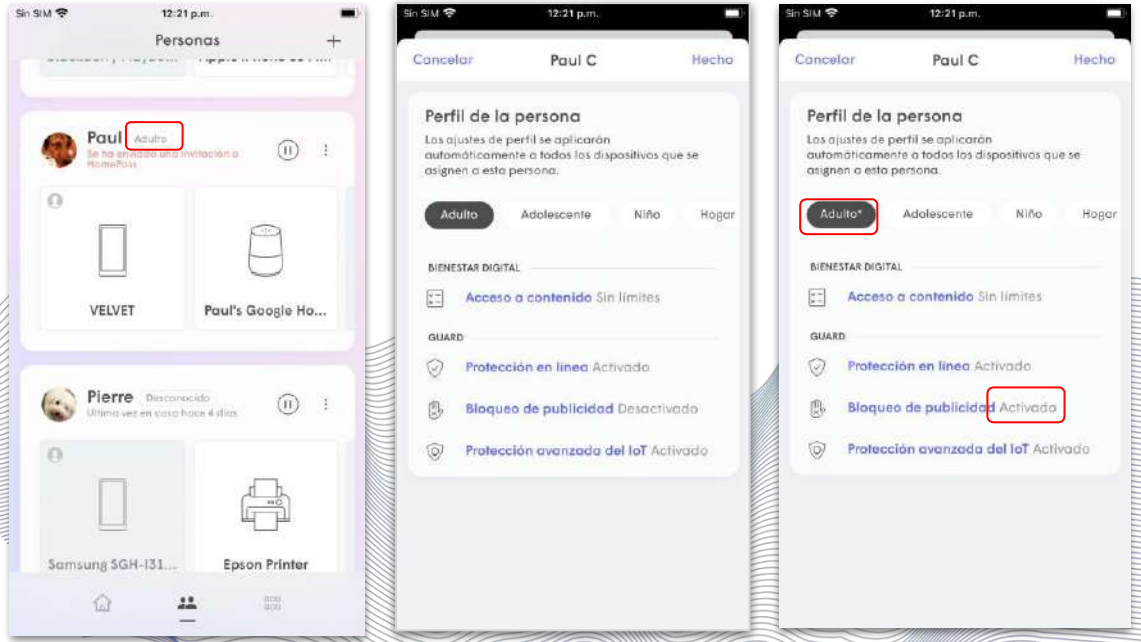


Perfiles de personas

En cuanto se asigne un perfil de persona a alguien, éste se podrá personalizar en función de esa persona.

Al pulsar sobre el Perfil de persona asignado a una persona, podrás realizar cambios en las reglas de Acceso a contenidos y Guard.

Una vez personalizado, el Perfil de persona mostrará un asterisco junto a él indicando que se ha personalizado para esa persona. Este proceso solo puede realizarse para personas individuales y la configuración predeterminada del Perfil de persona no se puede modificar.



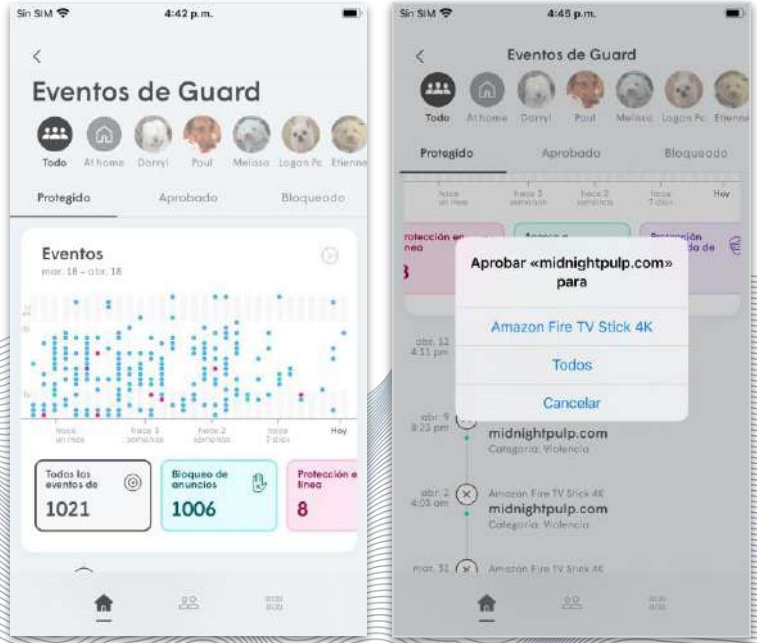
Aprobación manual del contenido

Los administradores pueden aprobar (poner en la lista blanca) dominios o direcciones IP* que hayan sido bloqueados por Acceso al **Contenido** , **Protección en línea** o **Bloqueo de anuncios**. Se pueden aprobar hasta un total de 50 entradas de forma manual para cada ubicación. Estas pueden aplicarse por red, por persona o por dispositivo.

La configuración a nivel de dispositivo reemplaza la configuración a nivel de persona y de red.

Al pulsar sobre **Gestionar eventos de seguridad** en las páginas de persona, dispositivo o Guard, se puede aprobar a mano un sitio bloqueado de la lista de **Protegidos** o ingresar un dominio o dirección IP* específica en la lista de **Aprobados**.

Las direcciones IP solo pueden ser aprobadas si existen IP salientes
Se ha activado la protección IP saliente y la Prevención de intrusiones



Personas

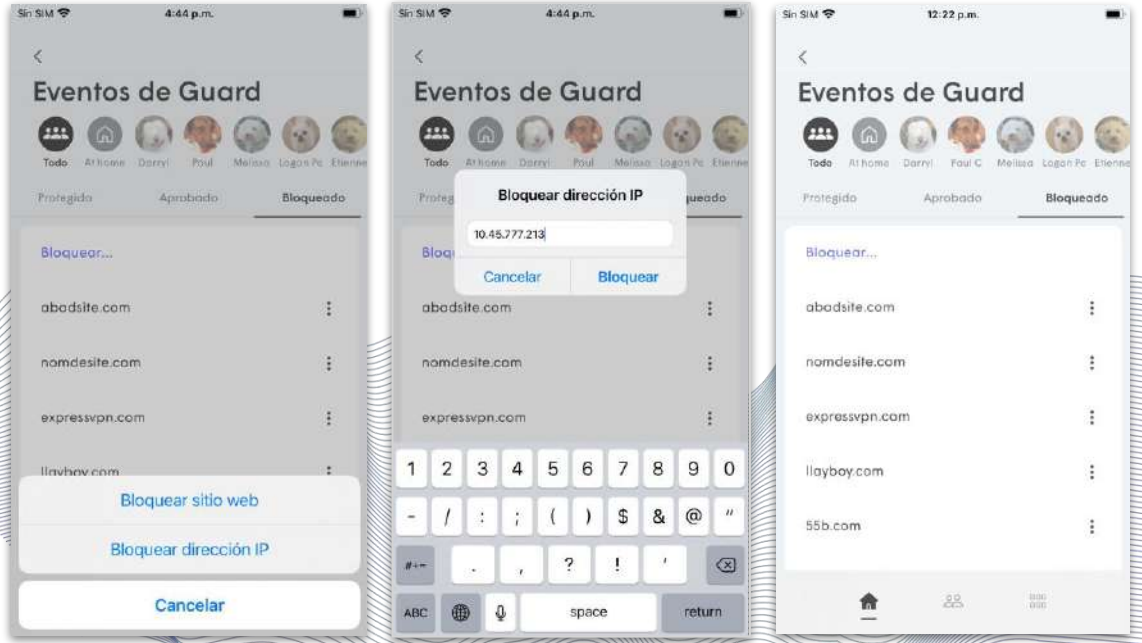
Bloqueo manual de contenidos

Los administradores pueden bloquear manualmente (poner en la lista negra) dominios o direcciones IP* que no hayan sido bloqueados por **Acceso a Contenidos**, **Protección en línea o Bloqueo de anuncios.** Se pueden bloquear hasta un total de 50 entradas manualmente.

La configuración a nivel de dispositivo reemplaza la configuración a nivel de persona, que a su vez reemplaza la configuración a nivel de red.

Al pulsar sobre **Gestionar eventos de seguridad** en las páginas de persona, dispositivo o Guard, se puede bloquear de forma manual un dominio o una dirección IP* específica al introducirla en la lista de **Bloqueos**.

Las direcciones IP solo pueden bloquearse si se ha activado la protección IP saliente y la prevención de intrusiones

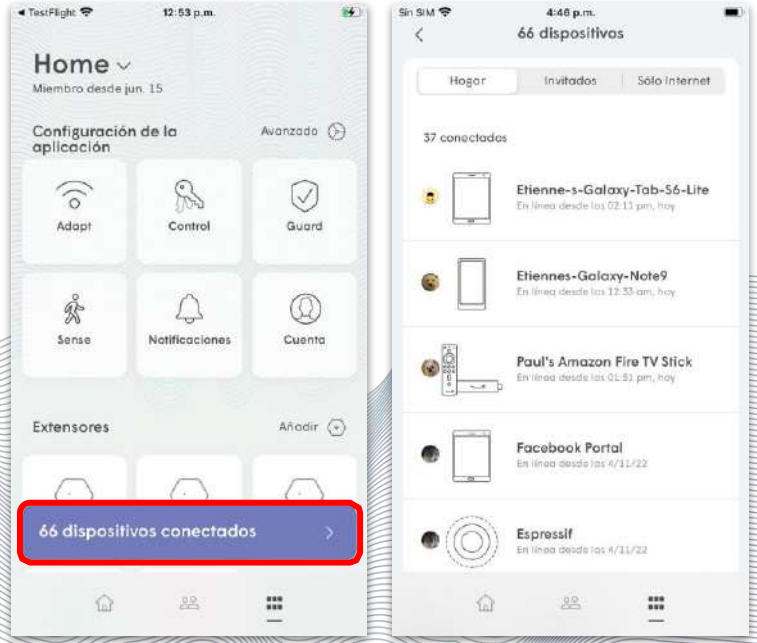


Gestión de dispositivos

Puedes definir las restricciones de Acceso a contenidos, los horarios de congelación de Internet o los tiempos de espera en función del dispositivo.

Si deseas acceder al dispositivo, dirígete al Menú de más opciones. Selecciona el dispositivo del que quieras obtener información.

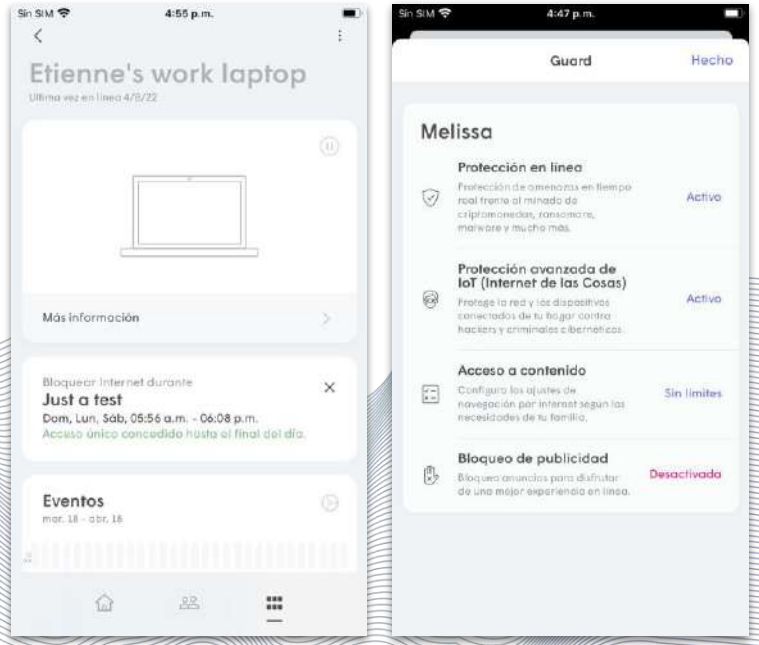
Además, puedes acceder a la pantalla de detalles de un dispositivo específico al tocar el dispositivo en las pantallas de detalles de la persona o del pod.



Gestión de dispositivos

A partir de la pantalla de detalles del dispositivo podrás:

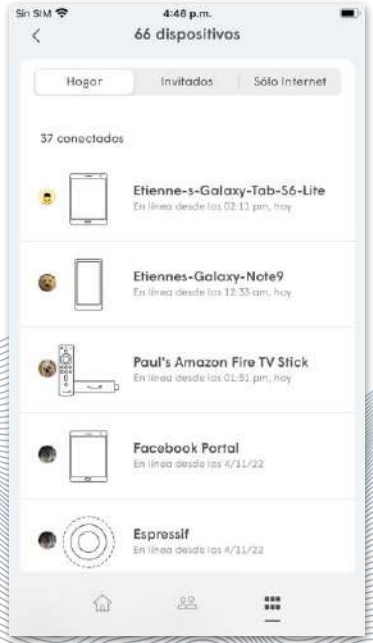
- Ver cómo se conecta a la red.
- Comprobar la calidad de la conexión con el pod.
- Ver la contraseña que se está utilizando, la persona y la habitación a la que se ha asignado.
- Ver el uso del ancho de banda.
- Gestionar la protección en línea, el acceso a contenidos y el bloqueo de anuncios.
- Ver las direcciones MAC e IP asignadas



Gestión de dispositivos

Al pulsar sobre los tres puntos de la esquina superior derecha, tendrás la opción de:

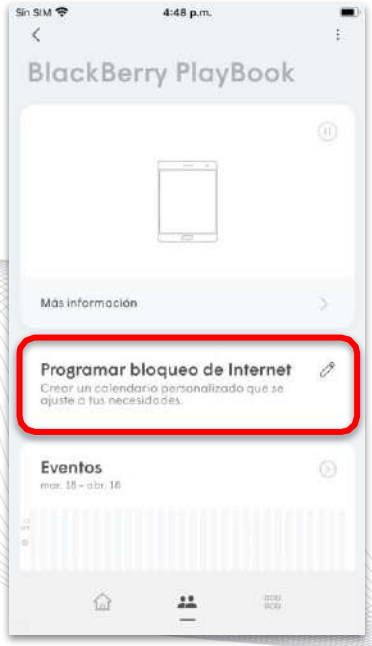
- Cambiar el nombre del dispositivo
- Cambiar la asignación de persona
- Cambiar la asignación de habitación



Congelación de Internet

La congelación de Internet impide que un solo dispositivo o personas accedan a la red durante el tiempo programado.

Esta función es útil para los padres que desean limitar la cantidad de tiempo que sus hijos pasan en Internet.

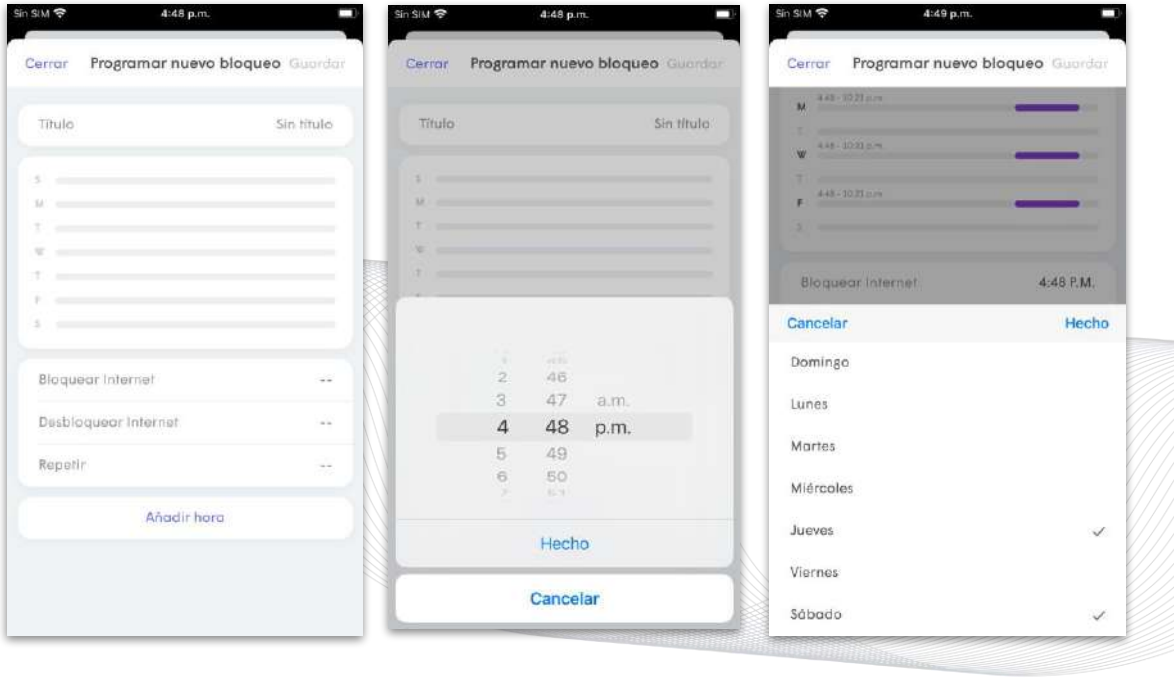


Plume Control

Congelación de Internet

Ingresa las horas de inicio y finalización del horario de Congelación.

Utiliza la opción Repetir para elegir el día en que se aplicará este horario.

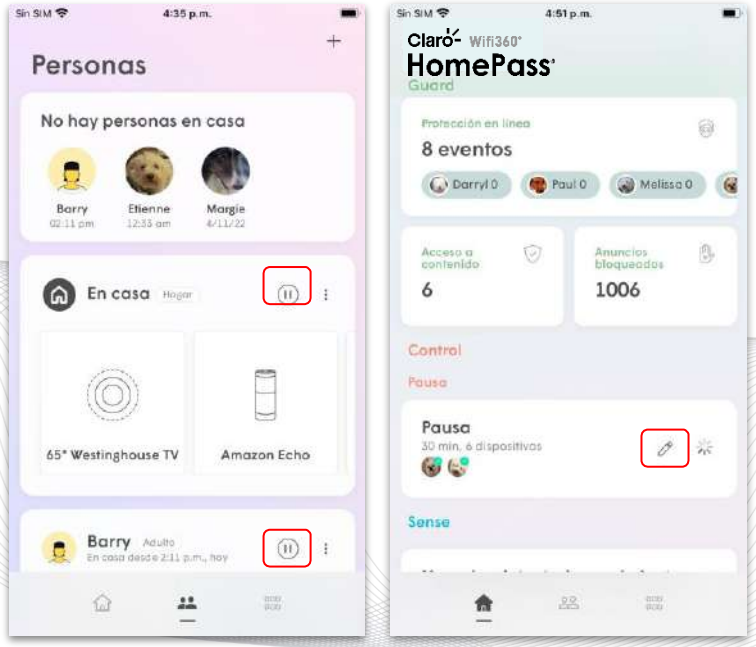


Pausa

Al tocar el botón de Pausa en un dispositivo individual o en una persona, se bloqueará temporalmente el acceso a Internet durante un breve período de tiempo.

Asimismo, puedes aplicar un tiempo de espera más amplio desde la pantalla de inicio si eliges varios dispositivos.

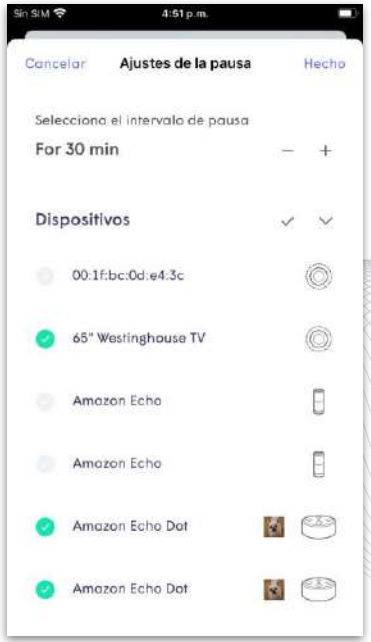
El único dispositivo que no puede tener un tiempo de espera es el que ejecuta la aplicación HomePass.



Pausa

- Elige los Dispositivos (La marca de verificación negra elige todos en la categoría)
- Toca el botón de pausa para activar el tiempo de espera
- Los botones -, + y x se pueden utilizar para acortar y aumentar la duración o cancelar el Tiempo de espera

El único dispositivo que no puede tener un tiempo de espera es el que ejecuta la aplicación HomePass.



Qué es Guard™?

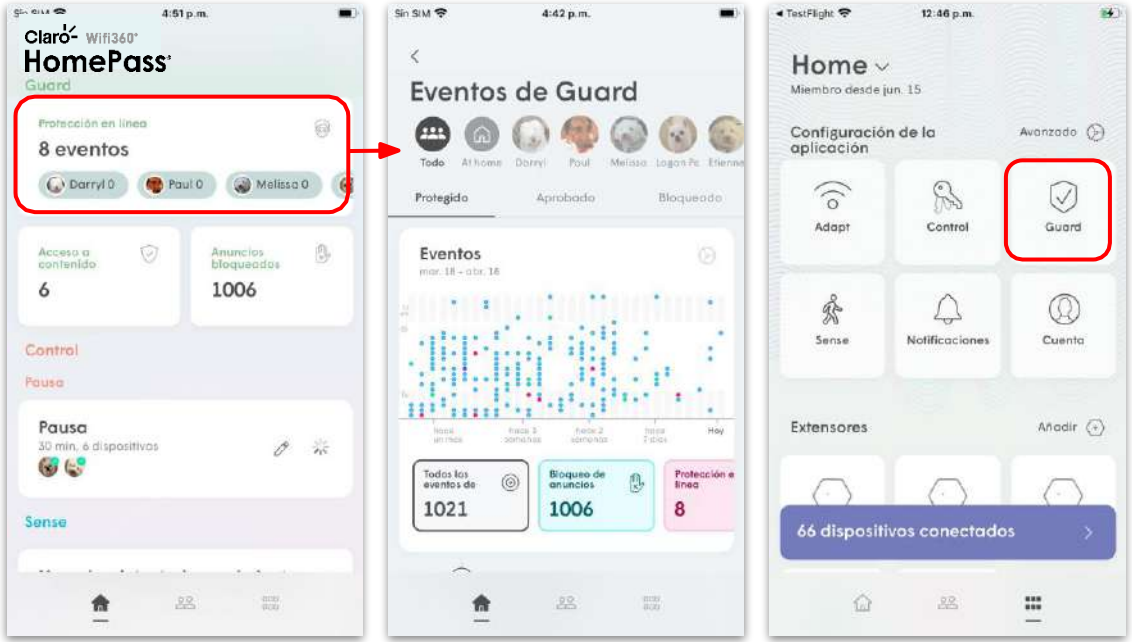
Si se activa, Plume Guard protege tu red al impedir el acceso a sitios web maliciosos que pueden dañar los dispositivos de tu red, sin que ello afecte al rendimiento de tu experiencia de navegación.

Hay tres componentes en Guard:

- **Protección en línea** - Si se activa por red, por persona o por dispositivo, la protección en línea bloquea el acceso de tus dispositivos a sitios web maliciosos conocidos.
- **Protección avanzada de IoT™ (AIP) -** La protección avanzada de IoT™ pone en cuarentena los dispositivos domésticos inteligentes si se detecta un comportamiento inusual. AIP solo se puede activar a nivel de red.
- **Bloqueo de anuncios -** Si se activa por red, por persona o por dispositivo, el bloqueador de anuncios hace que tu experiencia en la web sea más agradable al bloquear los servidores de publicidad conocidos.

Plume Guard

- Se puede acceder a los eventos de Guard desde la pantalla de inicio.
- La pantalla de eventos de Guard te permite ver todos los eventos y puede filtrarse a nivel de red o de persona.
- También se puede acceder a la configuración de Guard a nivel de red desde la pantalla de **Configuración de la aplicación.**

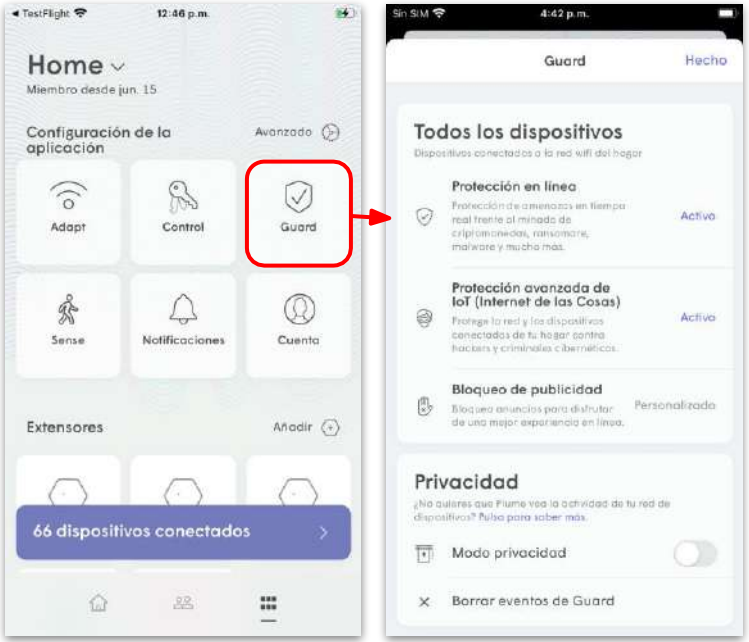


Protección en línea

La protección en línea utiliza una base de datos en constante actualización de los sitios web que se sabe que contienen:

- Malware y botnets
- Phishing y fraude
- Spyware y Adware,
- URL de spam
- Keyloggers y monitoreo
- Evasión de proxies y anonimizadores.

La protección en línea se puede configurar a nivel de red, dispositivo o persona.



Plume Guard

La protección de la IP saliente y la prevención de intrusiones

Además de la protección de la red basada en las búsquedas de DNS, la protección en línea también tiene otra función que protege los dispositivos de la conexión a direcciones IP dañinas.

Esta función bloquea tanto las conexiones entrantes (Protección contra Intrusiones) como las salientes (Protección Saliente) de los dispositivos a direcciones IP dañinas conocidas.

La Protección IP saliente y la Prevención de intrusiones se habilitan al activar la Protección en línea siempre que tengas un SuperPod conectado como pod de Gateway que ejecute el firmware 2.4.3 o versión posterior.

Plume Guard

Gestión de eventos de seguridad

Al pulsar sobre **Inicio de la protección** aparece una lista con un gráfico que muestra todos los eventos bloqueados.

La lista contiene datos de 30 días y al tocar el gráfico se resalta el número de eventos durante ese día.

También puedes filtrar por el tipo de evento.

Plume Guard

Gestión de eventos de seguridad

En cada evento hay una breve descripción que ofrece más información sobre la razón por la que fue bloqueado y el dispositivo que intentó acceder a él.

Al pulsar sobre un evento de la lista se ofrece la opción de desbloquear ese dominio.

En función del nivel en el que se haya bloqueado, se te da la opción de desbloquearlo para la persona, el dispositivo o todo el mundo.

Se pueden añadir un máximo de 50 entradas a la lista blanca de forma manual.

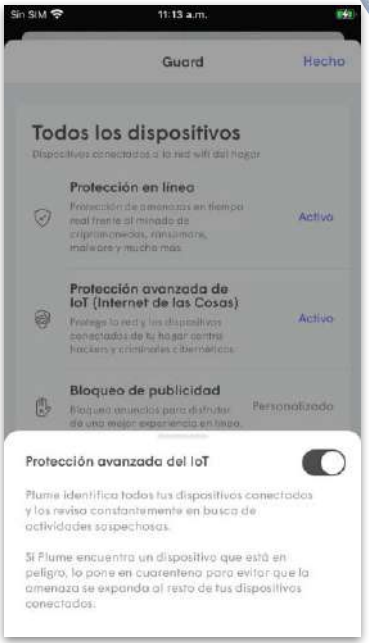
Plume Guard

Protección avanzada de IoT™

La protección avanzada de IoT™ estudia el comportamiento de los dispositivos.

La nube conoce los dominios a los que se supone que acceden regularmente los dispositivos domésticos inteligentes compatibles. Si un dispositivo compatible intenta acceder a un dominio previamente desconocido, se pone en cuarentena de inmediato y se envía una notificación al usuario.

Mientras se encuentra en cuarentena, el dispositivo mantendrá la conectividad a Internet, aunque se ubicará en la zona de solo Internet para que no pueda infectar a otros dispositivos de la red local.



Plume Guard

Protección avanzada de IoT™

Una vez que se bloquee el dispositivo, aparecerá un mensaje debajo de él, que indicará que se ha restringido al acceso solo a Internet.

Al pulsar sobre el dispositivo, aparecerán más detalles sobre el motivo del bloqueo, incluida la URL a la que pretendía acceder. Un enlace en la descripción permite a los usuarios buscar en la web más información del fabricante.

El usuario tiene la opción de retirar el dispositivo de la cuarentena durante una hora para que se pueda analizar.

Si el evento se debe a una actualización reciente del firmware o de las características del dispositivo que ahora requiere el acceso a un dominio previamente desconocido, se puede retirar el dispositivo de la cuarentena de forma permanente.

Plume Guard

Bloqueo de anuncios

Habilitado a nivel de **red**, **persona**, o **dispositivo**.

El bloqueo de anuncios bloquea los servidores de publicidad conocidos, aunque los sitios web seguirán mostrándose sin ciertos anuncios.

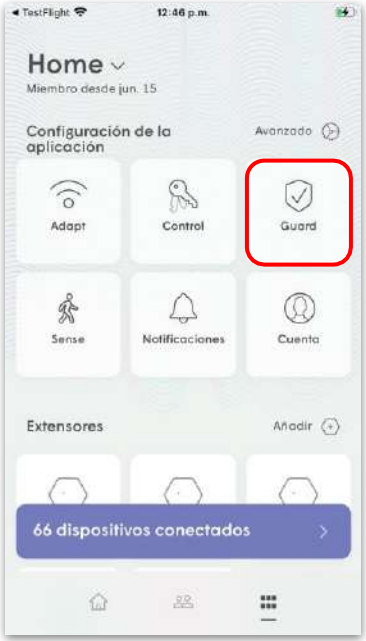
Plume Guard

Modo de privacidad

Al activar el **modo de privacidad** se desactiva todo el muestreo de DNS. Además, existe una opción para eliminar el historial de eventos de seguridad.

Al activar este modo se **desactivan** todas las funciones de **Guard y Acceso a Contenidos**.

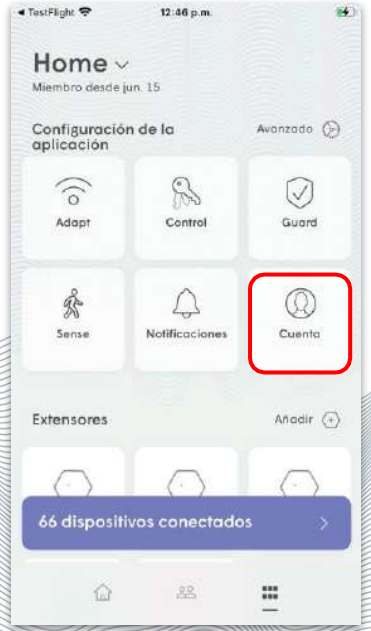
La precisión de **escritura del dispositivo** también se verá afectada al activar esta función.



Cuenta

La página Cuenta se utiliza para:

- Cambiar de ubicación si está disponible
- Configurar una nueva red bajo la misma cuenta
- Salir de la cuenta actual
- Ver el estado de afiliación de cada ubicación



Soporte técnico

Estas opciones se encuentran bajo el menú principal, en la parte inferior.

La página de soporte técnico incluye:

- Número de teléfono y enlaces para contactar con el soporte técnico.
- Enlaces a las preguntas frecuentes de soporte de Plume

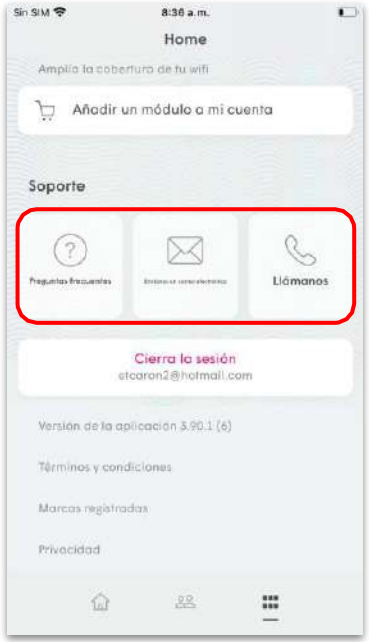


Tabla de contenidos

Instalación y Pantallas de la aplicación (IOS & Android)

Gestión de los pods (extensores)

Pruebas de velocidad

Plume Control™

- Contraseñas y zonas de control
- Gestión del acceso para personas y dispositivos
- Congelación de dispositivos y tiempos de espera

Plume Guard™

- Protección en línea
- Protección avanzada de IoT™
- Bloqueo de anuncios
- Modo de privacidad

Soporte y menús de la cuenta

Claro Wifi360°

HomePass®

Manual de la aplicación móvil

Comunicaciones Claro hogar – Mayo 2023