



Ajax es un sistema de seguridad inalámbrico que protege contra intrusiones, incendios e inundaciones, y permite a los usuarios controlar aparatos eléctricos directamente desde una app móvil. El sistema responde inmediatamente a las amenazas informándole a usted y a la compañía de seguridad sobre todas las incidencias.



Hub 2 representa un panel de control de sistema de seguridad inteligente que admite detectores con verificación fotográfica de intrusiones. Representando un elemento clave del sistema de seguridad, controla el funcionamiento de los dispositivos Ajax y, en caso de amenaza, comunica las señales de alarma inmediatamente informando al propietario y a la central receptora de alarmas de las incidencias.

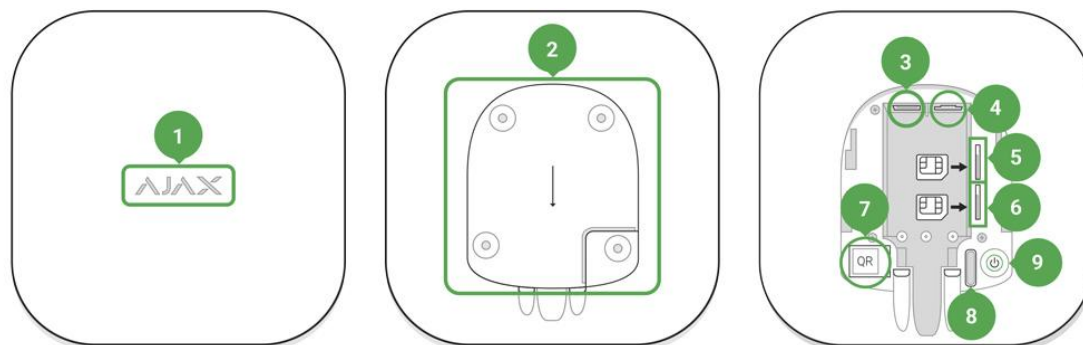
Hub 2 requiere conexión a Internet para acceder al servicio en la nube Ajax Cloud para la configuración y administración del sistema desde cualquier lugar del mundo a través de las apps de Ajax, la comunicación de alarmas y eventos, y la actualización del firmware del sistema operativo OS Malevich. El servicio Ajax Cloud está alojado en Amazon Web Services. Todos los datos se almacenan en un sistema con seguridad multinivel y el intercambio de información con el hub se realiza a través de un canal cifrado.

Para comunicarse con el servicio Ajax Cloud, el hub utiliza una conexión a Internet por cable (Ethernet) y dos tarjetas SIM 2G. Se recomienda el uso de todos los canales de comunicación con el fin de garantizar una conexión más fiable con el servicio de Ajax Cloud y para proteger contra el fallo de uno de los proveedores de servicios.

Los usuarios pueden administrar el sistema de seguridad y responder con prontitud a las alarmas y notificaciones mediante las apps diseñadas para iPhone y smartphones con Android,

MacOS y Windows. El sistema notifica las alarmas y otros eventos mediante notificaciones push, SMS y llamadas telefónicas.

Elementos funcionales



1. Logotipo de Ajax con indicador luminoso
2. Panel de fijación SmartBracket (deslizar hacia abajo con fuerza para abrir; la parte perforada es necesaria para activar el interruptor antisabotaje en caso de que se intente arrancar el hub de la superficie. ¡No la desprenda!)
3. Conector del cable de alimentación
4. Conector del cable de Ethernet
5. Ranura de respaldo para la instalación de una tarjeta micro-SIM
6. Ranura principal para la instalación de una tarjeta micro-SIM
7. Código QR
8. Interruptor antisabotaje
9. Botón de encendido

Principios de funcionamiento del Hub 2

El hub recopila información sobre el funcionamiento de los dispositivos conectados de manera cifrada, analiza los datos y, en caso de alarma, informa al propietario del sistema del peligro en menos de un segundo y comunica la alarma directamente a la central receptora de alarmas de la compañía de seguridad.

Para comunicarse con los dispositivos, supervisar su funcionamiento y responder rápidamente a amenazas, Hub 2 utiliza la tecnología de radio Jeweller. Para la transmisión de datos visuales, Hub 2 utiliza el protocolo de radio Ajax Wings. Es un protocolo de alta velocidad basado en la tecnología Jeweller. Wings también utiliza una antena especializada para mejorar la fiabilidad del canal.

Todos los dispositivos Ajax

Indicación LED del hub



El logotipo con un indicador luminoso se puede iluminar en rojo, blanco o verde dependiendo del estado del dispositivo.

Evento	Indicador luminoso
Están conectados Ethernet y al menos una tarjeta SIM	Se ilumina en blanco
Sólo un canal de comunicación está conectado	Se ilumina en verde
El hub no está conectado a Internet o no hay conexión con el servicio Ajax Cloud	Se ilumina en rojo
No hay alimentación	Se enciende durante 3 minutos, luego parpadea cada 20 segundos. El color del indicador depende del número de canales de comunicación conectados.

Cuenta Ajax

El sistema de seguridad está configurado y administrado a través de apps de Ajax diseñadas para iPhone y smartphones con Android, macOS y Windows.

Para configurar el sistema, instale la [app Ajax](#) y registre una cuenta. Recomendamos usar la app del Sistema de seguridad Ajax para administrar uno o varios hubs. Si planea administrar más de cien hubs, recomendamos usar la aplicación [Ajax PRO: Tool for Engineers](#) (para iPhone y smartphones con Android) o [Ajax PRO Desktop](#) (para computadoras de escritorio y portátiles con Windows y macOS). Como parte del proceso, deberá confirmar su dirección de correo electrónico y su número de teléfono. Tenga en cuenta que puede usar su número de teléfono y su dirección de correo electrónico para crear una sola cuenta de Ajax. No necesita crear una nueva cuenta para cada hub: puede añadir varios hubs a una sola cuenta.

Una cuenta con información sobre los hubs añadidos se carga en el servicio basado en la nube Ajax Cloud de manera cifrada.

Requisitos de seguridad

Al instalar y utilizar Hub 2, siga las normas generales de seguridad eléctrica para el uso de aparatos eléctricos, así como los requisitos de las normativas de seguridad eléctrica.

¡Está terminantemente prohibido desmontar el dispositivo conectado a la alimentación!
Además, no utilice el dispositivo con un cable de alimentación dañado.

Conexión del hub

1. Retire la tapa del hub deslizándola hacia abajo con fuerza. ¡No dañe la parte perforada ya que es necesaria para activar el interruptor antisabotaje en caso de un intento de sabotaje del hub!
2. Conecte el cable de alimentación y el cable de Ethernet a los conectores correspondientes.

1 — Entrada de corriente
2 — Entrada Ethernet
3, 4 — Ranuras de tarjeta SIM

3. Mantenga pulsado el botón de encendido durante 3 segundos hasta que se enciendan las luces del logotipo de Ajax. El hub necesita hasta 2 minutos para actualizarse a la versión de firmware más reciente y acceder a Internet. El color verde o blanco del logotipo indica que el hub está funcionando y está conectado al servicio Ajax Cloud.

Si la conexión Ethernet no se establece automáticamente, desactive el filtrado de proxy y dirección MAC, y active DHCP en la configuración del router; el hub recibirá automáticamente una dirección IP. Después, podrá asignar una dirección IP estática en la aplicación de Ajax.

4. Para conectarse a través de GSM, necesita una tarjeta micro-SIM emitida por un operador móvil con la solicitud de PIN deshabilitada (puede deshabilitarla usando un teléfono móvil) y un saldo suficiente en la cuenta para pagar los servicios del operador móvil. Si usa una tarjeta SIM, instálela en la ranura principal. Si el hub no está conectado a través de GSM, use Ethernet para configurar los ajustes del operador de red (configuración de itinerancia, puntos de acceso APN, nombre de usuario y contraseña). Para conocer la configuración de su operador de telefonía celular, comuníquese con el servicio de soporte de su proveedor de servicio.

Añadir un hub a la app Ajax

1. Entre en la app Ajax. Asegúrese de otorgarle acceso a todas las funciones del sistema solicitadas, especialmente a los permisos para mostrar notificaciones. Si utiliza un smartphone con Android, recomendamos usar [instrucciones de configuración de las notificaciones push](#).
2. Acceda a su cuenta y haga clic en **Añadir un Hub**. Elija un método adecuado, de forma manual o usando una guía paso a paso. Si está configurando el sistema por primera vez, recomendamos usar la guía paso a paso.
3. Especifique el nombre del hub y escanee el código QR situado debajo de la tapa o introdúzcalo manualmente.

4. Espere hasta que el proceso de adición del hub haya terminado. Una vez vinculado, el hub aparecerá en la pestaña **Dispositivos** .

Usuarios del sistema de seguridad

Cuando añade un hub a su cuenta, usted se convierte en el administrador de este dispositivo. Un único hub puede acomodar hasta 50 usuarios/administradores. El administrador invita a los usuarios a utilizar el sistema de seguridad y determina sus derechos.

Cambiar el administrador del sistema de seguridad y retirarlo del hub no causará el restablecimiento de los dispositivos conectados a él.

Derechos del usuario del Sistema de seguridad Ajax

Ajustes del hub

Antes de vincular el dispositivo al hub, cree al menos una estancia.

La descripción del evento del dispositivo especificará la estancia donde se ubica el dispositivo:



Para crear una estancia, vaya a la pestaña **Estancias** y haga clic en **Añadir una estancia**. Asigne un nombre a la estancia y, si lo desea, adjunte (o tome) una foto: así le será más fácil encontrar la estancia en la lista.

Para eliminar una estancia o cambiar su imagen o nombre, vaya a los ajustes de la estancia (haga clic en el icono del engranaje).

Conexión de detectores y dispositivos

Cuando agregue un hub utilizando una guía paso a paso, se le solicitará que agregue dispositivos que protejan las instalaciones. Pero puede negarse y volver a este paso más tarde.

Para agregar un dispositivo al hub:

1. En la aplicación Ajax, abra la estancia y seleccione **Añadir dispositivo**.
2. Asigne un nombre al dispositivo, escanee su código QR (o introdúzcalo manualmente), seleccione un grupo (si el modo de grupo está habilitado).
3. Haga clic en **Añadir** y empezará la cuenta atrás para que añada un dispositivo.
4. Encienda el dispositivo durante la cuenta atrás y su LED se encenderá una vez. Para vincular un dispositivo al hub, el dispositivo debe estar ubicado dentro del rango de comunicación por radio del hub (en las mismas instalaciones protegidas).

Si la conexión falla, apague el dispositivo durante 5 segundos e inténtelo de nuevo.

Videovigilancia

Puede conectar cámaras de terceros al sistema de seguridad: se ha implementado una integración perfecta con las cámaras IP y grabadoras de vídeo Dahua, Hikvision y Safire, y también puede conectar cámaras de terceros que admitan el protocolo RTSP. Puede conectar hasta 25 dispositivos de videovigilancia al sistema.

[Cómo agregar una cámara o grabadora de vídeo Dahua al hub](#)

[Cómo agregar una cámara o grabadora de vídeo Hikvision/Safire al hub](#)

[Cómo agregar una cámara de terceros al hub](#)

Ajustes del hub

Para introducir los ajustes del hub, selecciónelo en la lista de dispositivos y haga clic en el icono del engranaje .

Parámetros personalizables:

- Usuarios
- Ethernet
- Red móvil
- Geocercas
- Grupos
- Test de zona de detección
- Jeweller
- Servicio
- Centro de supervisión

- PRO
- Compañías de seguridad
- Guía del usuario

Usuarios — ajustes del sistema de seguridad para los usuarios. Determina quién tiene acceso a su sistema de seguridad, los derechos que se otorgan a los usuarios y cómo el sistema de seguridad les notifica acerca de los eventos.

Cómo notifica las alarmas el sistema de seguridad Ajax

Cómo añadir nuevos usuarios al hub

Ethernet — ajustes de la conexión de internet por cable.

Celular — habilitar/deshabilitar la conexión celular, configurar la conexión y verificar el saldo de la cuenta.

Geocercas — configurar recordatorios de armado/desarmado del sistema de seguridad si se cruza una zona específica. La ubicación del usuario se determina mediante el módulo GPS del smartphone.

Qué son las geocercas y cómo funcionan

Grupos — configuración del modo de grupo.

Las funcionalidades que ofrece el modo de grupo:

- Gestión de la seguridad de instalaciones individuales o grupos de detectores. La oficina está protegida mientras el encargado de limpieza trabaja en la cocina.
- Diferenciación de acceso a las herramientas de administración de los modos de seguridad. Los empleados del departamento de marketing no tienen acceso a la oficina jurídica.

Hub OS Malevich 2.6: nuevo nivel de seguridad

Test de zona de detección — probar la zona de detección de los detectores conectados al hub. El test le permite determinar la distancia a la cual los detectores registran las alarmas.

Qué es el test de zona de detección

Jeweller — configuración del período de sondeo para el hub y los dispositivos conectados. La configuración determina la frecuencia con la que el hub intercambia datos con los dispositivos y con qué rapidez se detecta la pérdida de comunicación.

- **Intervalo de ping del detector** — la frecuencia de sondeo del hub de los dispositivos conectados, fijada en el rango comprendido entre 12 y 48 segundos (por defecto, 36 seg.).
- **Número de paquetes no entregados para determinar un fallo de conexión** — un contador de paquetes no entregados (por defecto, 30 paquetes).

El tiempo antes del envío de un mensaje referente a la pérdida de comunicación entre el hub y el dispositivo se calcula usando la fórmula:

*Intervalo de sondeo * (número de paquetes no entregados + 1 paquete de corrección)*

Cuanto menor sea el período de sondeo, más rápido recibe la información el hub acerca de los eventos de los dispositivos conectados y más rápido reciben los dispositivos las órdenes del hub; no obstante, esto reduce el tiempo de funcionamiento de los dispositivos con baterías incluidas. Entretanto, la información acerca de una alarma o sabotaje se comunica al instante.

Tenga en cuenta que el intervalo limita el número máximo de dispositivos conectados:

Intervalo	Límite de conexión
12 seg	39 dispositivos
24 seg	79 dispositivos
36 seg o más	100 dispositivos

¡Solo es posible conectar 10 sirenas al hub con cualquier configuración!

Servicio — un grupo de ajustes de servicio del hub.

Ajustes de conexión del Hub y del servicio Ajax Cloud:

- **Intervalo de ping del servidor.** La frecuencia de sondeo del hub del servicio Ajax Cloud, establecida en el rango de 10 a 300 seg. El valor recomendado y predeterminado es de 60 seg.
- **Retardo de alarma por conexión fallida.** Es un retardo requerido para reducir el riesgo de una falsa alarma asociada con la pérdida de la conexión con el servicio Ajax Cloud. Se activa tras 3 sondeos sin éxito del servidor del hub. El retardo puede fijarse en el rango de 30 a 600 seg. El valor recomendado y predeterminado es de 300 seg.

El tiempo para generar un mensaje referente a la pérdida de comunicación entre el hub y el servicio Ajax Cloud se calcula usando la siguiente fórmula:

$$(\text{Intervalo de sondeo} * 4) + \text{Filtro de tiempo}$$

Con los ajustes predeterminados, el servicio Ajax Cloud informa de una pérdida del hub tras 7 minutos:

$$(30 \text{ s} * 4) + 300 \text{ s} = 7 \text{ min}$$

Qué tan rápido se detecta la pérdida de conexión entre el hub y el servicio Ajax Cloud

- **Luminosidad del LED.** Ajuste de la luminosidad de los LED en el logotipo del hub. Fijar el intervalo de 1 a 10 (el valor predeterminado es 10).
- **Comprobación de la integridad del sistema.** Una vez la función está habilitada, el hub comprueba el estado de todos los dispositivos antes del armado: carga de la batería, antisabotaje, conexión. Si se detecta un problema durante el armado, el hub no activa el modo armado y emite un aviso.
- **Permiso de armado** (la opción se vuelve activa solo después de habilitar la **Comprobación de la integridad del sistema**). Cuando la función está activa, el sistema de seguridad puede armarse incluso en caso de fallo de funcionamiento.

Para armar el sistema de seguridad que tiene fallos a través de la aplicación Ajax:

1. Active el modo armado — recibirá una alerta correspondiente con una lista de errores.
2. Confirme el armado del sistema de seguridad pulsando **Armar**.

Para confirmar la activación del modo armado en el sistema de seguridad con errores cuando utiliza un teclado KeyPad o un mando SpaceControl:

1. Active el modo armado — recibirá una negativa.
2. Confirme el armado del sistema reactivando el modo armado en 30 s.

¿Qué es una comprobación de la integridad del sistema?

- **Actualizaciones de software automáticas.** Configurar las actualizaciones automáticas del firmware OS Malevich. Cuando el hub está encendido, actualiza automáticamente el firmware si está disponible una nueva versión.

Cómo se actualiza el OS Malevich

Configuración del detector de incendios FireProtect y FireProtect Plus

- **Alarma interconectada de FireProtect.** Esta función activa las sirenas que incorporan todos los detectores de incendios si al menos uno de ellos detecta una amenaza.

¿Qué es una alarma interconectada de FireProtect?

- **Ignore la primera alarma.** Función de pospuesta de la alarma que verifica la presencia de humo.

La opción funciona de la forma siguiente:

1. Un detector detecta la alarma de humo.
2. Se activa un temporizador de 30 seg. incorporado dentro del detector.
3. Si el detector sigue detectando una amenaza tras 30 seg., se comunica una alarma al hub.

Este ajuste se recomienda si hay fuentes potenciales de falsas alarmas dentro de las instalaciones, por ejemplo, si el detector está instalado en una ubicación en la que las corrientes de aire son habituales.

Los ajustes para recopilar y almacenar informes del sistema de seguridad Ajax

- **Registros del hub.** Puede deshabilitar los registros o seleccionar un canal de transmisión:
 - Ethernet
 - Wi-Fi (solo en Hub Plus)
 - No — el registro está deshabilitado

¡No recomendamos deshabilitar los registros, ya que esta información podría ser útil en caso de errores en el funcionamiento del sistema!

Ajustes de activación de la sirena

- **Si el hub o la carcasa del detector están abiertos.** Cuando la función está activa, el hub activa las sirenas conectadas si las carcasas del hub, del detector o de cualquier otro dispositivo Ajax están abiertas.
- Si un botón de alarma se pulsa en la aplicación. Cuando la función está activa, el hub activa las sirenas conectadas si el botón de pánico se presiona en la app de Ajax.

Deshabilite la respuesta de la sirena presionando el botón de pánico en el mando SpaceControl en los ajustes del mando (**Dispositivos SpaceControl Ajustes**)

Central receptora de alarmas — los ajustes para la conexión directa a la central receptora de alarmas de la compañía de seguridad.

Los eventos y alarmas pueden comunicarse a la central receptora de alarmas de la compañía de seguridad sin estos ajustes

En qué consiste la Central receptora de alarmas

PRO — ajustes para usuarios PRO (instaladores y representantes de las compañías de seguridad) del sistema de seguridad. Determina quién tiene acceso a su sistema de seguridad, los derechos que se otorgan a los usuarios y cómo el sistema de seguridad les notifica acerca de los eventos.

Compañías de seguridad — una lista de compañías de seguridad en su zona. La zona está determinada por los datos de GPS o los ajustes regionales de su smartphone.

Guía del usuario — abre la guía del usuario de Hub 2.

Desvincular hub — retira su cuenta del hub. No obstante, se guardan todos los ajustes y detectores vinculados.

Restablecer los ajustes del hub

Restablecer el hub a los ajustes de fábrica:

1. Encienda el hub si está apagado.
2. Elimine todos los usuarios e instaladores del hub.
3. Mantenga pulsado el botón de encendido durante 30 segundos: el logotipo de Ajax en el hub comenzará a parpadear en rojo.
4. Elimine el hub de su cuenta.

Alertas sobre eventos y alarmas

El sistema de seguridad Ajax informa al usuario acerca de alertas y eventos que utilizan tres tipos de notificaciones: notificaciones push, SMS y llamadas telefónicas. Los ajustes de alertas pueden modificarse solo para usuarios registrados.

Tipos de eventos	Objetivo	Tipos de notificaciones
Fallos de funcionamiento	Pérdida de conexión entre el dispositivo y el hub Inhibición Carga de batería baja en el dispositivo o hub Enmascaramiento Intentos de sabotaje a la carcasa del detector	Notificaciones push SMS
Alarma	Intrusión Incendio Inundación El hub ha perdido la conexión con el servicio Ajax Cloud	Llamadas Notificaciones push SMS
Eventos	Encender/apagar <u>WallSwitch</u> , <u>Relay</u> , <u>Socket</u>	Notificaciones push SMS
Armar/desarmar	Armar/desarmar instalaciones enteras o grupo Activar el modo noche	Notificaciones push SMS

Cómo notifica Ajax a los usuarios sobre las alarmas

Conectarse a una compañía de seguridad

La lista de organizaciones que conectan el sistema a sus centrales receptoras de alarmas se pueden encontrar en el menú **Compañías de seguridad (Dispositivos Hub Ajustes Compañías de seguridad)**:

Póngase en contacto con los representantes de la compañía que preste estos servicios en su ciudad y acuerde con ellos la conexión.

La conexión a la Central Receptora de Alarmas (CRA) se realiza a través del protocolo Contact ID o SIA.

Montaje

¡Antes de instalar el hub, asegúrese de que ha seleccionado la ubicación óptima y de que cumple con los requisitos de estas instrucciones! Es recomendable que el hub esté oculto de miradas indiscretas.

Asegúrese de que el hub tiene una intensidad de señal estable con todos los dispositivos conectados. Si la intensidad de señal es baja (una sola barra), no garantizamos un funcionamiento estable del sistema de seguridad. ¡Implemente las medidas necesarias para mejorar la calidad de la señal! Al menos, reubique el hub, ya que cambiar su posición tan solo 20 cm puede mejorar significativamente la calidad de recepción.

Si se detecta una intensidad de señal baja o inestable tras la reubicación, utilice un repetidor de señal de radio ReX.

Al instalar y utilizar el dispositivo, siga las normas generales de seguridad eléctrica para el uso de aparatos eléctricos, así como los requisitos de las normativas de seguridad eléctrica.

Instalación del hub:

1. Fije el panel de montaje SmartBracket con los tornillos incluidos. Si usa otros dispositivos de fijación, asegúrese de que no dañan o deforman el panel.

No se recomienda usar cinta adhesiva de doble cara para la instalación. Esto puede provocar que un hub caiga y el dispositivo puede averiarse debido al golpe.

2. Fije el hub al panel de montaje. Tras la instalación, compruebe el estado del interruptor antisabotaje en la app de Ajax y después la firmeza de la fijación del panel.
3. Para conseguir una mayor fiabilidad, fije el hub a la placa con los tornillos incluidos.

Recibirá una notificación si se realiza un intento de extraer el hub de la superficie o de quitarlo del panel de fijación.

¡Está terminantemente prohibido desmontar el dispositivo conectado a la alimentación! No use el dispositivo con un cable de alimentación dañado.

No desmonte o modifique el hub o alguna de sus partes individuales: esto puede interferir con el correcto funcionamiento del dispositivo y dar lugar a errores.

No sitúe el hub:

- Fuera de la estancia (al aire libre).
- Cerca de objetos metálicos o espejos que puedan atenuar o causar apantallamiento de la señal.
- En lugares con altos niveles de interferencia de radio.
- Dentro de habitaciones con mucha humedad y temperaturas fuera de los límites permisibles.

Mantenimiento del sistema Ajax

Compruebe periódicamente el correcto funcionamiento del sistema de seguridad Ajax. Limpie la carcasa de polvo, telarañas y otras suciedades que puedan aparecer. Utilice un paño suave y seco que sea adecuado para el cuidado del dispositivo.

Para su limpieza, no use sustancias que contengan alcohol, acetona, gasolina u otros disolventes activos.

Cómo reemplazar la batería del hub

Este empaque incluye

1. Hub 2
2. Cable de alimentación
3. Cable de Ethernet
4. Kit de instalación
5. Kit de inicio de GSM: no disponible en todos los países
6. Guía rápida de inicio

Especificaciones técnicas

Clasificación	Panel de control del sistema de seguridad inteligente compatible con Ethernet y dos tarjetas SIM
Número máximo de dispositivos conectados	Hasta 100
Grupos de seguridad	Hasta 9
Usuarios del sistema de seguridad	Hasta 50
Videovigilancia	Hasta 25 cámaras o DVRs
Estancias	Hasta 50
Protocolos de comunicación de la Central receptora de alarmas	Contact ID, SIA
Fuente de alimentación	110 – 240 V CA, 50/60 Hz
Batería recargable incorporada	Li-Ion 2 Ah (hasta 16 horas de duración de la batería en caso de desconexión de Ethernet)
Resistencia al sabotaje	Disponible, antisabotaje

Banda de frecuencia operativa	868.0–868.6 MHz o 868.7–869.2 MHz, dependiendo de la región de venta
Potencia de radiofrecuencia de salida	8.20 dBm / 6.60 mW (hasta 25 mW)
Modulación de la señal de radio	GFSK
Alcance de la señal de radio	Hasta 2,000 m (sin obstáculos)
Canales de comunicación	2 tarjetas SIM (GSM 850/900/1800/1900 MHz GPRS) Ethernet
Rango de temperatura de funcionamiento	De -10°C a +40°C
Humedad de funcionamiento	Hasta 75%
Dimensiones	163 x 163 x 36 mm
Peso	362 g