

Manual de usuario del Hub

Actualizado September 28, 2021



Hub es un dispositivo central del sistema de seguridad Ajax que coordina el funcionamiento de los dispositivos conectados e interactúa con el usuario y la compañía de seguridad. Utilizado en espacios interiores.

Hub necesita acceso a internet para conectarse al servidor en la nube Ajax Cloud y configurar, controlar desde cualquier punto del mundo, transmitir notificaciones de eventos o actualizar el software. Los datos personales y los registros detallados de las operaciones del sistema se almacenan bajo protección multinivel, y el intercambio de información con Hub se lleva a cabo a través de un canal cifrado las 24 horas del día.

Para comunicarse con Ajax Cloud, el sistema usa conexión Ethernet y la red 2G de las operadoras móviles.



Si es posible, utilice ambos canales de conexión a internet. Esto asegurará una comunicación más fiable entre Hub y el Ajax Cloud y evitará fallos en el funcionamiento de uno de los proveedores de servicios de comunicación.

Hub se puede controlar a través de una [aplicación para smartphones](#) con iOS y Android. Las aplicaciones móviles permiten responder al instante a cualquier notificación del sistema de seguridad.

Siga el enlace para descargar la aplicación para su smartphone:

[Android](#)

[iOS](#)

En el Hub puede configurar de qué eventos y cómo se notificará al usuario. Elija la opción que más le convenga: notificaciones push, mensajes SMS o llamadas telefónicas. Si una compañía de seguridad administra el sistema Ajax, la señal de alarma se le enviará directamente sin pasar por el servidor.

[Compre el panel de control de seguridad inteligente Hub](#)

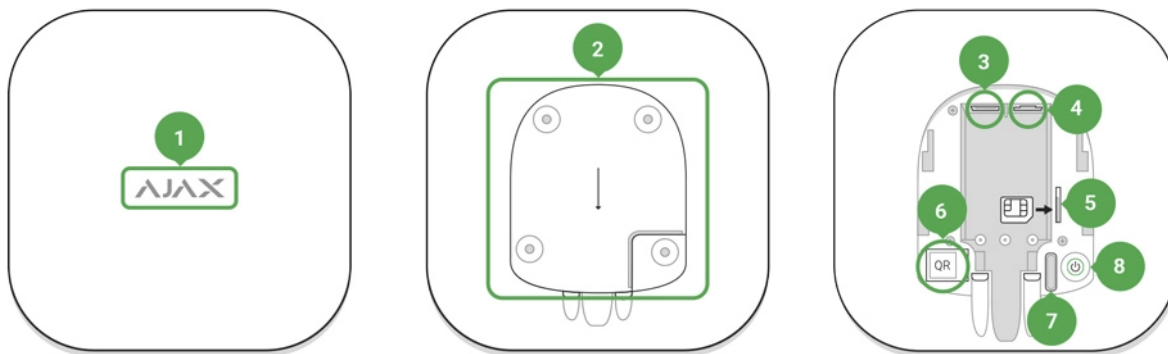
Hasta 100 dispositivos Ajax se pueden conectar al Hub. El protocolo de seguridad [Jeweller](#) se usa en la comunicación entre dispositivos, con un radio de cobertura de hasta 2 km sin obstáculos.

[Lista de dispositivos Ajax](#)

Utilice escenarios para automatizar el sistema de seguridad y disminuir la cantidad de acciones de rutina. Ajuste el programa de seguridad, programe acciones de dispositivos de automatización ([Relay](#), [WallSwitch](#) o [Socket](#)) en respuesta a una alarma, pulsando el [Button](#) o por programación. Se puede crear un escenario de forma remota en la app Ajax.

[Cómo crear y configurar un escenario en el sistema de seguridad Ajax](#)

Entradas del Hub e indicación de funcionamiento



1. Logotipo con LED que informa del estado del Hub
2. Panel de fijación SmartBracket (la pieza perforada es necesaria para activar el interruptor antisabotaje en caso de que se intente arrancar el Hub de la superficie)
3. Entrada para conectar el cable de alimentación
4. Entrada para conectar el cable Ethernet
5. Ranura para instalar la tarjeta de una operadora móvil (Micro SIM)
6. Código QR
7. Interruptor antisabotaje
8. Botón de encendido

Indicación LED del hub

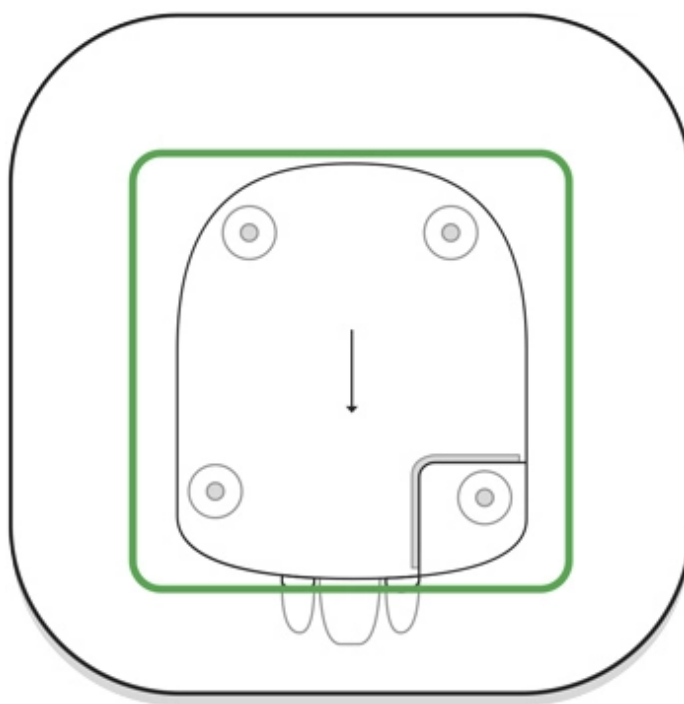


El logotipo con un indicador luminoso se puede iluminar en rojo, blanco o verde dependiendo del estado del dispositivo.

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 10 segundos. El color del indicador depende del número de canales de comunicación conectados.

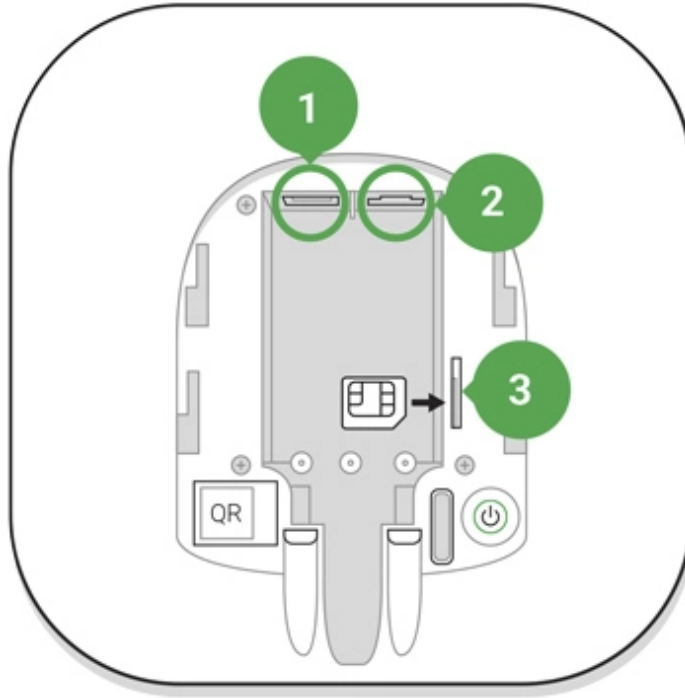
Conectar Hub a la red

1. Abra la tapa del Hub bajándola con fuerza.



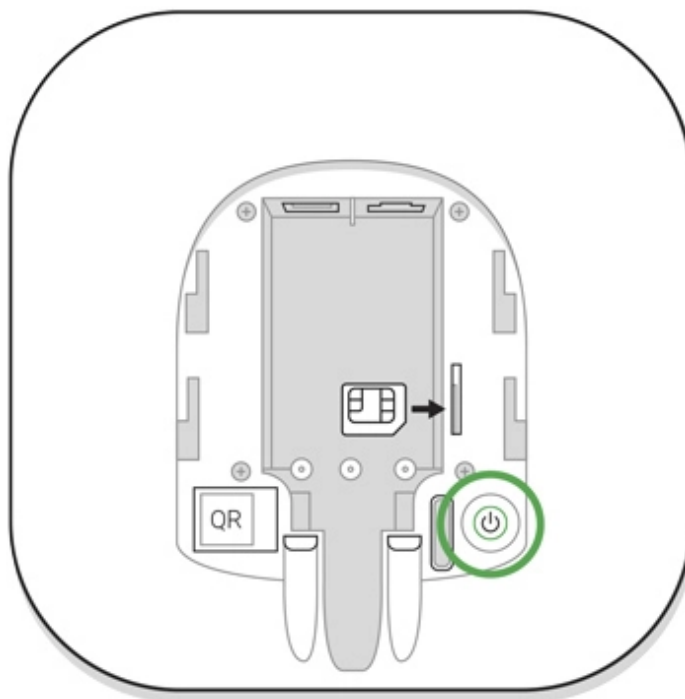
¡Tenga cuidado de no dañar el interruptor antisabotaje que protege al Hub de ataques informáticos!

2. Conecte los cables de alimentación y el cable Ethernet en sus entradas correspondientes.



- 1 – Entrada de corriente
- 2 – Entrada Ethernet
- 3 – Ranura de tarjeta SIM

3. Pulse el botón de encendido durante 2 segundos hasta que el logo se encienda. Hub necesita aproximadamente dos minutos para identificar los canales de comunicación disponibles.



La luz verde clara o blanca del logo informa de que Hub se ha conectado al servidor

Si la conexión Ethernet no funciona automáticamente, desactive el proxy, la filtración por dirección MAC y active el DHCP en los ajustes del router: el Hub recibirá una dirección IP. En la próxima configuración del Hub en la aplicación móvil, podrá preestablecer una dirección IP estática.

Para conectarse a la red 2G, necesitará una tarjeta de una operadora móvil en formato Micro-SIM con la solicitud del código PIN desactivada (la solicitud del código PIN puede desactivarse desde su teléfono móvil) e importe suficiente en la cuenta para pagar los servicios GPRS, SMS y realizar llamadas.



En algunas regiones, Hub se vende con una tarjeta SIM incorporada

Si el hub no se conecta a Ajax Cloud a través de la red 2G, utilice Ethernet para configurar los parámetros de red en la aplicación móvil. Para preestablecer el punto de acceso, nombre de usuario y contraseña correctamente, por favor póngase en contacto con el servicio de soporte de la operadora.

Cuenta Ajax

El sistema de seguridad Ajax se configura a través de la aplicación a la que esté conectada el administrador. La cuenta con la información sobre los Hub añadidos se guarda encriptada en el servidor en la nube Ajax Cloud.

Los parámetros de usuario del sistema de seguridad Ajax y los dispositivos conectados se guardan en el Hub y están siempre conectados a él. Ningún cambio del administrador de Hub provocará fallos en la configuración de los dispositivos conectados a él.



El número de teléfono solo se puede usar una vez para crear una cuenta Ajax

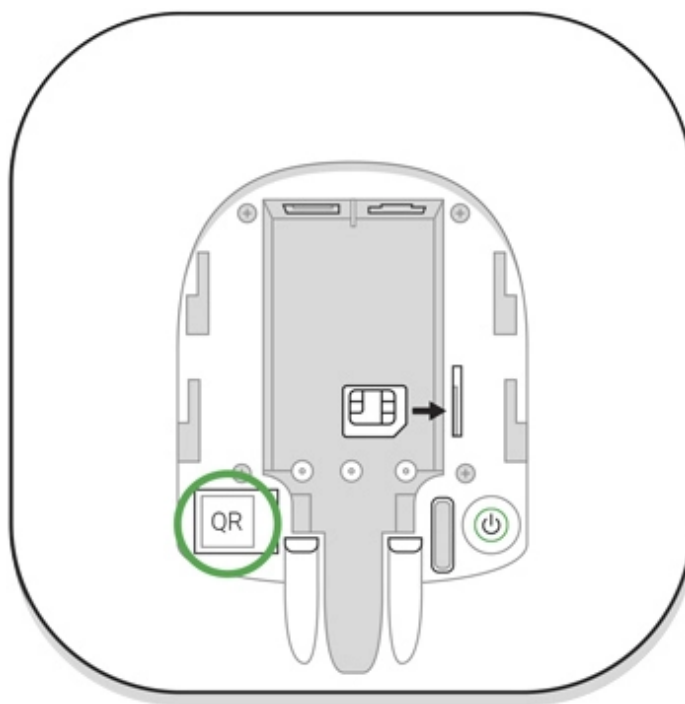
Cree una cuenta del sistema Ajax en la aplicación móvil siguiendo la guía paso a paso. Como parte del proceso, necesitará confirmar su dirección de correo electrónico y número de teléfono móvil.

Su cuenta puede combinar los roles de administrador de un Hub y usuario de otro Hub.

Añadir un Hub a la aplicación Ajax Security System

¡Debe proporcionar acceso a la aplicación a todas las funciones del sistema (en particular para mostrar notificaciones)! Es una condición **sine qua non** para controlar el sistema de seguridad Ajax desde un smartphone.

1. Entre en su cuenta.
2. Abra el menú “**Añadir Hub**” y seleccione el método que desee: manual o con una guía paso a paso.
3. En el registro, escriba el nombre del Hub y escanee el código QR ubicado bajo la tapa (o introduzca la clave de registro manualmente).



4. Espere hasta que el Hub quede registrado y aparezca un nuevo dispositivo en el escritorio de la aplicación.

Instalación del Hub



Antes de instalar el Hub, asegúrese de que ha seleccionado la mejor ubicación: la tarjeta SIM posee una señal de recepción consistente, se ha comprobado la comunicación por radio de todos los dispositivos y el Hub debería estar oculto a la vista directa.



El dispositivo está destinado exclusivamente a la instalación en interiores.

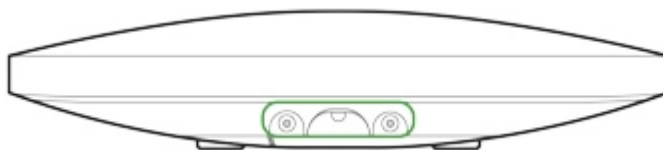
El Hub debe fijarse de forma segura a la superficie (vertical u horizontal). Recomendamos encarecidamente no utilizar cinta adhesiva de **doble cara**, ya que no garantiza una fijación segura y facilita el desmontaje del dispositivo.

El Hub no se debe colocar:

- fuera de las instalaciones (al aire libre);
- cerca o dentro de objetos metálicos o espejos que causen atenuación y apantallamiento de la señal;
- en lugares con poca cobertura GSM;
- cerca de fuentes de interferencia de radio: a menos de 1 metro del enrutador y los cables de alimentación;
- en estancias con temperatura o humedad que excedan los rangos permisibles.

Instalación del Hub:

1. Ponga el Hub en la tapa y fíjelo con los tornillos del paquete.
2. Fije la tapa del Hub a la superficie utilizando los tornillos del paquete. Si usa cualquier otro dispositivo de fijación, asegúrese de que no daña o deforma la tapa del Hub.



No voltee el hub en fijación vertical (por ejemplo, en una pared). Con la fijación adecuada, el logotipo de Ajax se leerá horizontalmente.



Fijar la tapa del Hub con tornillos evita cualquier desliz accidental del mismo y minimiza

el riesgo de robo impulsivo del dispositivo.

Si el Hub está firmemente fijado, se activará el interruptor antisabotaje y recibirá la notificación correspondiente en caso de que se arranque la carcasa de la superficie.

Estancias en la aplicación Ajax Security System

Las estancias combinan los dispositivos conectados. La aplicación puede crear hasta 50 estancias, cada dispositivo se podrá ubicar solo en una estancia.



¡Si no crea una estancia, no podrá añadir dispositivos a la aplicación Ajax Security System!

Crear y configurar una estancia

Las estancias se crean en la aplicación móvil a través del menú «**Añadir estancia**».

Asigne un nombre a la estancia, si lo desea, adjunte (o cree) una foto: así le será más fácil encontrar la estancia en la lista.

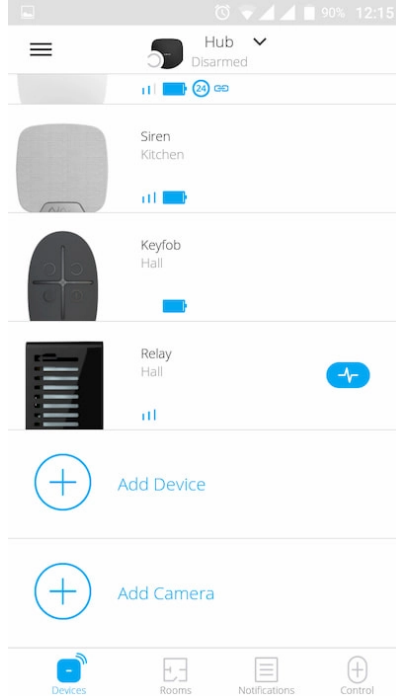
Pulse el engranaje  y vaya al menú de configuración de la estancia.

Para eliminar una estancia, mueva todos los dispositivos guardados en ella a otras estancias a través del menú de configuración de dispositivos. Eliminar la estancia borrará todos sus ajustes.

Conectar dispositivos a Hub



El hub no es compatible con los módulos de integración [uartBridge](#) y [ocBridge Plus](#).



Durante el primer registro de Hub en la aplicación móvil, se le pedirá que añada dispositivos para proteger la estancia. Sin embargo, puede rechazar y volver a este paso más tarde.



¡El dispositivo solo se puede añadir si el sistema está desarmado!

1. Abra una estancia en la aplicación móvil y seleccione la opción «**Añadir dispositivo**».
2. Eliga un nombre para el dispositivo, escanee el **código QR** (o inserte la ID manualmente), seleccione una estancia y vaya al siguiente paso.
3. Cuando la aplicación inicie la búsqueda e inicie la cuenta atrás, encienda el dispositivo, que parpadeará una vez con un LED. Para que el dispositivo sea detectado y se pueda conectar, deberá estar situado dentro del área de cobertura de la red inalámbrica del hub (en un solo recinto protegido).



La solicitud de conexión al hub se transmite durante un corto periodo de tiempo al encender el dispositivo


Si la conexión con el Hub falla al primer intento, apague el dispositivo durante 5 segundos y vuelva a intentarlo.








Se pueden conectar hasta 10 cámaras o grabadores NVR con soporte de protocolo RTSP al Hub Ajax.

Cómo configurar y conectar una cámara IP al sistema de seguridad Ajax

Estados del hub


Iconos


Los iconos muestran algunos de los estados de Hub. Puede verlos en la app Ajax, en el menú **Dispositivos** .

Iconos	Sentido
	2G conectado
	La tarjeta SIM no está instalada
	La tarjeta SIM está defectuosa o tiene código PIN
	Nivel de carga de la batería Hub. Se muestra en incrementos de 5%
	Se detecta un fallo de funcionamiento del Hub. La lista está disponible en la lista de estados del hub
	El hub está conectado directamente a la central receptora de alarmas
	El hub ha perdido la conexión con la central receptora de alarmas a través de una conexión directa

Estados

Los estados se pueden encontrar en la app Ajax:

1. Vaya a la pestaña **Dispositivos** .
2. Seleccione Hub en la lista.



Parámetro	Significado
Fallo de funcionamiento	Haga clic  para abrir la lista de fallos de funcionamiento de Hub.

	El campo solo aparece si se detecta un fallo de funcionamiento
Intensidad señal celular	Muestra la intensidad de la señal de la red móvil para la tarjeta SIM activa. Recomendamos instalar el hub en lugares con intensidad de la señal de 2 a 3 barras. Si la intensidad de la señal es débil, el hub no podrá marcar o enviar un SMS sobre un evento o alarma
Nivel de batería	Nivel de carga de la batería del dispositivo. Se muestra el porcentaje <u>Cómo se muestra la carga de la batería en las apps Ajax</u>
Tapa	Estado del interruptor antisabotaje que responde al intento de desmantelar el hub: <ul style="list-style-type: none"> • Cerrado: la tapa del hub está cerrada • Abierto: el hub se ha quitado del soporte SmartBracket <u>¿Qué es un interruptor antisabotaje?</u>
Alimentación externa	Estado de la conexión de alimentación externa: <ul style="list-style-type: none"> • Conectado: el hub está conectado a la alimentación externa • Desconectado: sin alimentación externa
Conexión	Estado de la conexión entre el hub y Ajax Cloud: <ul style="list-style-type: none"> • En línea: el hub está conectado a Ajax Cloud • Sin conexión: el hub no está conectado a Ajax Cloud
Datos celulares	El estado de la conexión del hub a Internet móvil: <ul style="list-style-type: none"> • Conectado: el hub está conectado a Ajax Cloud a través de Internet móvil • Desconectado: el hub no está conectado a Ajax Cloud a través de Internet móvil

	Si el hub tiene suficientes fondos en la cuenta o tiene SMS/llamadas adicionales, podrá realizar llamadas y enviar mensajes SMS incluso si se muestra en este campo el estado No conectado
Ethernet	<p>Estado de la conexión a Internet del hub a través de Ethernet:</p> <ul style="list-style-type: none"> • Conectado: el hub está conectado a Ajax Cloud a través de Ethernet • Desconectado: el hub no está conectado a Ajax Cloud a través de Ethernet
Ruido Promedio (dBm)	<p>El nivel de potencia acústica en las frecuencias del Jeweller en el lugar donde está instalado el hub.</p> <p>El valor aceptable es 80dbm o menos</p>
Centro de supervisión	<p>El estado de la conexión directa del hub a la central receptora de alarmas:</p> <ul style="list-style-type: none"> • Conectado: el hub está conectado directamente a la central receptora de alarmas • Desconectado: el hub no está conectado directamente a la central receptora de alarmas <p>Si se muestra este campo, la central receptora de alarmas utiliza una conexión directa para recibir eventos y alarmas del sistema de seguridad</p> <p><u>¿Qué es una conexión directa?</u></p>
Modelo del hub	Nombre del modelo del hub
Versión de hardware	Versión de hardware. No se puede actualizar
Firmware	Versión de firmware. Se puede actualizar de forma remota
ID	ID/número de serie. También se encuentra en la caja del dispositivo, en la placa de circuito del dispositivo y en el código QR bajo el panel SmartBracket

Configurar el Hub

La configuración se puede cambiar en la [app Ajax](#):

1. Vaya a la pestaña **Dispositivos** .
2. Seleccione Hub en la lista.
3. Vaya a **Configuración** haciendo clic en el icono .



Tenga en cuenta que después de cambiar la configuración, debe hacer clic en el botón **Volver** para guardarlos.


Avatar es una imagen del título personalizada para el sistema de seguridad Ajax. Se muestra en el menú de selección del hub y ayuda a identificar el objeto requerido.

Para cambiar o establecer un avatar, haga clic en el icono de la cámara y configure la imagen deseada.

Nombre del hub. Se muestra en el SMS y en el texto de la notificación push. El nombre puede contener hasta 12 caracteres cirílicos o hasta 24 caracteres latinos.

Para cambiarlo, haga clic en el icono del lápiz y escriba el nombre del hub que desee.

Usuarios: configuración de usuario para un sistema de seguridad: qué derechos se conceden a los usuarios y cómo el sistema de seguridad les notifica eventos y alarmas.

Para cambiar la configuración de usuario, haga clic en  frente al nombre del usuario.

Cómo el sistema de seguridad Ajax notifica las alertas a los usuarios

Cómo añadir nuevos usuarios al hub

Ethernet: configuración de la conexión de Internet por cable.

- Ethernet: le permite activar y desactivar Ethernet en el hub
- DHCP/Estática: selección del tipo de dirección IP del hub a recibir: dinámica o estática
- Dirección IP: dirección IP del hub
- Máscara de subred: máscara de subred en la que funciona el hub
- Router: puerta de enlace utilizada por el hub
- DNS: DNS del hub

Red móvil: habilita/deshabilita la comunicación celular, configuración de conexiones y comprobación de cuenta.

- Red móvil: habilita y deshabilita tarjetas SIM en el hub
- Roaming: si está activada, las tarjetas SIM instaladas en el hub pueden funcionar en itinerancia
- Ignorar error de registro de red: cuando se activa esta configuración, el hub ignora los errores al intentar conectarse a través de una tarjeta SIM. Active esta opción si la tarjeta SIM no se puede conectar a la red
- Desactivar ping antes de conectar: cuando se activa esta opción, el hub omite los errores de comunicación del operador. Active esta opción si la tarjeta SIM no se puede conectar a la red

- **SIM 1:** muestra el número de la tarjeta SIM instalada. Haga clic en el campo para ir a la configuración de la tarjeta SIM

Configuración de la tarjeta SIM

Configuración de conexión

- **APN, Nombre de usuario y Contraseña:** configuración para conectarse a Internet a través de una tarjeta SIM. Para conocer la configuración de su operador de telefonía celular, comuníquese con el servicio de soporte de su proveedor.

Cómo establecer o cambiar la configuración de APN en el hub

Uso de datos móviles

- **Entrante:** la cantidad de datos recibidos por el hub. Se muestra en kB o MB.
- **Saliente:** la cantidad de datos enviados por el hub. Se muestra en kB o MB.



Tenga en cuenta que los datos se cuentan en el hub y pueden diferir de las estadísticas de su operador.

Restablecer estadísticas: restablece las estadísticas sobre el tráfico entrante y saliente.

Comprobar saldo

- **USSD:** introduzca el código que se utiliza para comprobar el saldo en este campo. Por ejemplo, *111#. Después de eso, haga clic en **Comprobar saldo** para enviar una solicitud. El resultado se mostrará debajo del botón.

Geofence: configura recordatorios para armar/desarmer el sistema de seguridad al cruzar un área especificada. 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. Esto le permite:

- Gestione los modos de seguridad para sitios o grupos de detectores independientes.
Por ejemplo, la oficina está armada mientras el encargado de limpieza trabaja en la cocina.
- Delimite el acceso al control de los modos de seguridad.
Por ejemplo, los empleados del departamento de marketing no tienen acceso al despacho de abogados.

Cómo habilitar y configurar el grupo de modos en el sistema de seguridad Ajax

Programa de seguridad: armado/desarmado del sistema de seguridad según una programación.

Cómo crear y configurar un escenario en el sistema de seguridad Ajax

Test de zona de detección: ejecución de la prueba de zona de detección para los detectores conectados. La prueba determina la distancia

suficiente para que los detectores registren las alarmas.

Qué es el Test de zona de detección

Jeweller: configuración del intervalo de ping entre detector y hub La configuración determina la frecuencia con la que el hub se comunica con los dispositivos y la rapidez con la que se detecta la pérdida de conexión.

Más información

- **Intervalo de ping del detector:** la frecuencia de sondeo de dispositivos conectados por el hub se establece en el rango de 12 a 300 s (36 s de forma predeterminada)
- **Número de paquetes no entregados para determinar un fallo de conexión:** un contador de paquetes no entregados (8 paquetes por defecto).

El tiempo antes de provocar la alarma por la pérdida de comunicación entre el hub y el dispositivo se calcula con la siguiente fórmula:

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

El intervalo de ping más corto (en segundos) implica una entrega más rápida de los eventos entre el hub y los dispositivos conectados; sin embargo, un intervalo de ping corto reduce la duración de la batería. Asimismo, las alarmas se transmiten inmediatamente, independientemente del intervalo de ping.

No se recomienda reducir la configuración predeterminada del período de ping y el intervalo.

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

--	--

Interval	Connection limit
12 segundos	39 dispositivos
24 segundos	79 dispositivos
36 segundos y más	100 dispositivos



Independientemente de la configuración, el hub admite 10 sirenas conectadas como máximo.

Servicio es un grupo de configuraciones del servicio del hub. Estos se dividen en 2 grupos: configuración general y configuración avanzada.

Configuración general

Zona horaria

Selección de la zona horaria en la que funciona el hub. Se utiliza para escenarios por programación. Por lo tanto, antes de crear escenarios, establezca la zona horaria correcta.

[Más información sobre los escenarios](#)

Brillo de LED

Ajuste del brillo de la luz de fondo LED del logotipo del hub. Se establece en el rango de 1 a 10. El valor predeterminado es 10.

Actualización automática del firmware

Configuración de actualizaciones automáticas del firmware OS Malevich.

- **Si está habilitado**, el firmware se actualiza automáticamente cuando está disponible una nueva versión, cuando el sistema no está armado y se conecta la alimentación externa.

- **Si está deshabilitado**, el sistema no se actualiza automáticamente. Si está disponible una nueva versión de firmware, la app ofrecerá actualizar OS Malevich.

Cómo se actualiza OS Malevich

Registro del sistema del hub



Los registros son archivos que contienen información sobre el funcionamiento del sistema. Pueden ayudar a resolver el problema en caso de errores o fallos.

La configuración le permite seleccionar el canal de transmisión para los registros del hub o deshabilitar su grabación:

- Ethernet
- No: el registro está deshabilitado



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

Cómo enviar un informe de errores

Configuración avanzada

La lista de configuraciones avanzadas del hub depende del tipo de app: estándar o PRO.

Sistema de seguridad Ajax	Ajax PRO
Conexión al servidor Configuración de sirenas Configuración de detectores de incendios Comprobación de la integridad del sistema	Asistente de configuración PD 6662 Conexión al servidor Configuración de sirenas Opciones de detectores de incendio Comprobación de la integridad del sistema Confirmación de alarma Restaurar después de la alarma

Asistente de configuración PD 6662

Abre una guía paso a paso sobre cómo configurar su sistema para cumplir con la norma de seguridad británica PD 6662:2017.

Más información sobre la norma PD 6662:2017

Cómo configurar el sistema para que cumpla con la norma PD 6662:2017

Conexión al servidor

El menú contiene configuraciones para la comunicación entre el hub y Ajax Cloud:

- **Intervalo de sondeo el servidor y el hub, seg.** Frecuencia de envío de pings desde el hub al servidor Ajax Cloud. Se establece en el rango de 10 a 300 seg. El valor recomendado y predeterminado es de 60 seg.
- **Retardo de la alarma de falla de conexión del servidor, seg.** Es un retardo para reducir el riesgo de una falsa alarma asociada a la pérdida de la conexión del servidor Ajax Cloud. Se activa tras 3 sondeos fallidos del servidor del hub. El retardo se fija 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 servidor Ajax Cloud se calcula usando la siguiente fórmula:

$$(Intervalo de ping * 4) + Filtro de tiempo$$

Con la configuración predeterminada, Ajax Cloud informa de la pérdida del hub tras 9 minutos:

$$(60 s * 4) + 300 s = 9 min$$

- **Reciba eventos de pérdida de conexión con el servidor sin alarma.** Las apps Ajax pueden notificar acerca de la pérdida de comunicación entre el hub y el servidor de dos maneras: con una señal de notificación push

estándar o con un sonido de sirena (habilitado de forma predeterminada). Cuando la opción está activa, la notificación llega con una señal de notificación push estándar.

- **Notificación de pérdida de conexión a través de canales.** El sistema de seguridad Ajax puede notificar tanto a los usuarios como a la central receptora de alarmas sobre la pérdida de conexión incluso a través de uno de los canales de conexión.

En este menú, puede elegir la pérdida de conexión de qué canales será informado por el sistema, así como el retardo para enviar dichas notificaciones:

- Ethernet
- Red móvil
- **Retardo de notificación de pérdida, min.:** tiempo del retardo antes de enviar la notificación sobre la pérdida de conexión a través de uno de los canales de comunicación. Se establece en el rango de 3 a 30 minutos.

El tiempo de recepción de una notificación sobre la pérdida de conexión a través de uno de los canales de comunicación se calcula con la siguiente fórmula:

$$(Intervalo\ de\ sondeo \times 4) + Filtro\ de\ tiempo + Retardo\ de\ notificación\ de\ pérdida$$

Configuración de sirenas

El menú contiene dos grupos de configuraciones de sirena: parámetros de activación de sirena e indicación de la sirena después de la alarma.


Parámetros de activación de la sirena

Si la tapa está abierta (hub o detector). Si está habilitada, el hub activa las sirenas conectadas si las carcassas del hub, del detector o de cualquier otro dispositivo Ajax están abiertas.

Si se pulsa el botón de emergencia en la app. Cuando la función está activa, el hub activa las sirenas conectadas si se ha pulsado el botón de

pánico en la app Ajax.



Puede deshabilitar la reacción de las sirenas al pulsar el botón de pánico en el mando SpaceControl, en la configuración de este (Dispositivos → SpaceControl → Configuración .

Configuración de la indicación de sirena después de la alarma



Esta configuración solo está disponible en las [app Ajax PRO](#)

La sirena puede informar sobre la activación en el sistema armado por medio de una indicación LED. Gracias a esta función, los usuarios del sistema y las patrullas de las centrales receptoras de alarmas que pasen pueden ver que se activó el sistema.

[Implementación de funciones en HomeSiren](#)

[Implementación de funciones en StreetSiren](#)

[Implementación de funciones en StreetSiren DoubleDeck](#)

Opciones de detectores de incendios

Menú de configuración de los detectores de incendios FireProtect y FireProtect Plus. Permite configurar la Interconexión de alarmas en FireProtect de detectores de incendios.

Esta función está recomendada por las normas europeas contra incendios, que requieren, en caso de incendio, una potencia de señal de advertencia de al menos 85 dB a 3 metros de la fuente de sonido. Tal potencia de sonido despierta incluso a una persona profundamente dormida durante un incendio. Y puede deshabilitar rápidamente los detectores de incendios activados con la app Ajax, Button o KeyPad/KeyPad Plus.

[Más información](#)

Comprobación de la integridad del sistema

La **Comprobación de integridad del sistema** es un parámetro que se encarga de comprobar el estado de todos los detectores y dispositivos de seguridad antes del armado. La comprobación está desactivada de forma predeterminada.

Más información

Confirmación de alarma



Esta configuración solo está disponible en las [app Ajax PRO](#)

La **Confirmación de alarma** es un evento especial que el hub envía a la CRA y a los usuarios del sistema si varios dispositivos determinados se han activado en un período de tiempo especificado. Al responder solo a las alarmas confirmadas, la central receptora de alarma y la policía reducen la cantidad de visitas por falsas alarmas.

Más información

Restaurar después de la alarma



Esta configuración solo está disponible en las [app Ajax PRO](#)

Esta función no permite armar el sistema si ha sido registrada previamente una alarma. Para armar, el sistema debe ser restaurado por un usuario autorizado o por un usuario PRO. Los tipos de alarmas que requieren la restauración del sistema se definen al configurar la función.

La función elimina las situaciones en las que el usuario arma el sistema con detectores que generan falsas alarmas.

Más información

Proceso de armado/desarmado



Esta configuración solo está disponible en las [app Ajax PRO](#)

El menú permite activar el armado en dos etapas, así como establecer el Retardo de transmisión de alarma para el proceso de desarmado del sistema de seguridad.

Qué es el Armado en dos etapas y por qué es necesario

Qué es el Retardo de transmisión de alarma y por qué es necesario

Desactivación automática de dispositivos



Esta configuración solo está disponible en las [app Ajax PRO](#)

El sistema de seguridad Ajax puede ignorar alarmas u otros eventos de dispositivos sin quitarlos del sistema. En ciertas configuraciones, las notificaciones sobre eventos de un dispositivo específico no se enviarán a la CRA ni a los usuarios del sistema de seguridad.

Hay dos tipos de **desactivación automática de dispositivos**: por temporizador y por cantidad de alarmas.

Qué es la Desactivación automática de dispositivos

También es posible desactivar manualmente un dispositivo específico. Obtener más información sobre cómo desactivar dispositivos manualmente [aquí](#).

Borrar el historial de notificaciones

Al hacer clic en el botón se eliminan todas las notificaciones del historial de eventos del hub.

Centro de supervisión: la configuración para la conexión directa a la central receptora de alarmas. Los parámetros son establecidos por los ingenieros de la central receptora de alarma. Tenga en cuenta que los eventos y alarmas pueden enviarse a la central receptora de alarmas incluso sin esta configuración.

Pestaña “Central receptora de alarmas”: ¿Qué es?

- **Protocolo:** la elección del protocolo que utiliza el hub para enviar alarmas a la central receptora de alarmas mediante una conexión directa. Protocolos disponibles: Ajax Translator (Contact-ID) y SIA.
- **Conectar a pedido.** Habilite esta opción si necesita conectar con la central receptora de alarmas (CRA) solamente al transmitir un evento. Si la opción está deshabilitada, la conexión se mantiene continuamente. La opción solo está disponible para el protocolo SIA.
- **Número objeto:** el número de un objeto en la central receptora de alarmas (hub).

Dirección IP principal

- La **Dirección IP** y el **Puerto** son parámetros de la dirección IP principal y el puerto del servidor de la central receptora de alarmas al que se envían eventos y alarmas.

Dirección IP secundaria

- La **Dirección IP** y el **Puerto** son parámetros de la dirección IP secundaria y el puerto del servidor de la central receptora de alarmas al que se envían eventos y alarmas.

Canales de emisión de alarmas

En este menú, se seleccionan los canales para el envío de alarmas y eventos a la central receptora de alarmas. Hub puede enviar alarmas y eventos a la central receptora de alarmas a través de **Ethernet** y **EDGE**. Le recomendamos que utilice todos los canales de comunicación a la vez, lo

que aumentará la fiabilidad de la transmisión y se asegurará de que no haya errores por parte de los operadores de telecomunicaciones.

- **Ethernet:** permite la transmisión de eventos y alarmas a través de Ethernet.
- **Celular:** permite la transmisión de eventos y alarmas a través de Internet móvil.
- **Informe periódico de prueba:** si está habilitado, el hub envía los informes de prueba con un período determinado a la central receptora de alarmas para el control adicional de la conexión de objetos.
- **Intervalo de ping de la central receptora de alarmas:** establece el período para enviar mensajes de prueba (de 1 minuto a 24 horas).

Cifrado

Configuración de cifrado de transmisión de eventos en el protocolo SIA. Se utiliza el cifrado AES de 128 bits.

- **Cifrado:** si está habilitado, se cifran los eventos y las alarmas que se transmiten a la central receptora de alarmas en formato SIA.
- **Clave de encriptación:** cifrado de clave de los eventos y alarmas transmitidos. Debe coincidir con el valor de la central receptora de alarmas.

Coordenadas del botón de pánico

- **Enviar coordenadas:** si está habilitada, al presionar un botón de pánico en la app se envían las coordenadas del dispositivo en el que está instalada la app y se presiona el botón de pánico, para la central receptora de alarmas.

Restauración de alarmas en la CRA

La configuración le permite seleccionar cuándo se enviará el evento de restauración de alarma a la CRA: inmediatamente/después de la restauración del detector (por defecto) o al desarmarlo.

[Más información](#)

Instaladores: configuración para usuarios PRO (instaladores y representantes de las centrales receptoras de alarmas) del sistema de seguridad. Determina quién tiene acceso a su sistema de seguridad, los derechos que se otorgan a los usuarios PRO y cómo el sistema de seguridad les notifica acerca de los eventos.

[Cómo añadir un PRO al hub](#)

Compañías de seguridad: una lista de centrales receptoras de alarmas en su zona. La región está determinada por los datos de GPS o la configuración regional de su smartphone.

Guía del usuario: abre la guía del usuario de Hub.

Importación de datos – un menú para transferir automáticamente dispositivos y configuraciones desde otro hub. **Tenga en cuenta que se encuentra en la configuración del hub en el que desea importar datos.**

[Más información sobre la importación de datos](#)

Desvincular hub: retira su cuenta del hub. Independientemente de esto, todas las configuraciones y los detectores conectados permanecen guardados.

Restablecer ajustes del Hub

Para volver a los ajustes de fábrica del hub, enciéndalo y pulse el botón de encendido durante 30 segundos (el logo empezará a parpadear en rojo).

Además, todos los detectores conectados, ajustes de estancias y ajustes de usuarios se eliminarán. Los perfiles de los usuarios permanecerán conectados al sistema.

Sistemas de seguridad de usuario

Tras añadir un hub a la cuenta, se convertirá en el administrador del dispositivo. Un hub puede tener hasta 50 usuarios/administradores. El administrador puede invitar a usuarios al sistema de seguridad y administrar sus derechos.

Eventos y notificaciones de alarma

El hub notifica al usuario de eventos usando tres métodos: notificaciones push del móvil, mensajes SMS y llamadas telefónicas.

Las notificaciones se configuran en el menú **“Usuarios”**:

Tipo de eventos	Para qué se usa	Tipo de notificaciones
Armado / desarmado	Las notificaciones se reciben tras el armado / desarmado	<ul style="list-style-type: none">• SMS• Notificación push
Alarma	Alertas de intrusión, incendio, inundación	<ul style="list-style-type: none">• SMS• Notificación push• Llamada
Eventos	Notifica de los eventos relacionados con Ajax WallSwitch, Relay	<ul style="list-style-type: none">• SMS

		<ul style="list-style-type: none"> • Notificación push
Fallos de funcionamiento	Avisa de pérdida de comunicación, interferencia, poca carga de la batería o apertura de la carcasa del detector	<ul style="list-style-type: none"> • SMS • Notificación push

- **Notificación push** – se envía mediante el servidor Ajax Cloud a la aplicación Ajax Security System si tiene conexión a internet.
- **Mensaje SMS** – se envía al número de teléfono indicado por el usuario durante el registro de la cuenta Ajax.
- La **llamada telefónica** es una llamada del hub al número especificado en la cuenta de la aplicación Ajax.

Solo se llama en caso de alarma para captar su atención y reducir la posibilidad de que no se atienda a una alerta crítica. Es recomendable que active este tipo de notificación. El hub llama consecutivamente a todos los usuarios que han habilitado este tipo de notificación en el orden especificado en los ajustes de usuario. Si ocurre una segunda alarma, el hub volverá a llamar, pero no más de 1 vez en 2 minutos.



La llamada se termina automáticamente cuando sea respondida. Es recomendable que guarde el número de teléfono asociado a la tarjeta SIM del hub en su lista de contactos.

Los ajustes de notificación solo se pueden cambiar por usuarios registrados.

Conectar el sistema Ajax a una compañía de seguridad



La lista de las organizaciones que conectan el sistema Ajax a la central receptora se encuentra en el menú **“Compañías de seguridad”** de la configuración del Hub.

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

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

Mantenimiento del sistema Ajax

Compruebe frecuentemente el correcto funcionamiento del sistema de seguridad Ajax.

Limpie la carcasa del Hub de polvo, telas de araña y otros contaminantes que puedan aparecer. Utilice un paño seco y suave adecuado para el mantenimiento del equipo.

No use sustancias que contengan alcohol, acetona, gasolina u otros disolventes activos para limpiar el Hub.

Cómo reemplazar la batería del hub

Equipo completo

1. Hub
2. Panel de fijación SmartBracket
3. Cable de alimentación
4. Cable Ethernet
5. Kit de instalación
6. Paquete de inicio para 2G *
7. Guía rápida de inicio

* No disponible en todos los países.

Requisitos de seguridad

Al instalar y utilizar el Hub Plus, siga las normas generales de seguridad eléctrica para el uso de aparatos eléctricos, así como los requisitos de las leyes reglamentarias sobre seguridad eléctrica.

¡Está terminantemente prohibido desmontar el dispositivo mientras esté encendido! No use el dispositivo con un cable de alimentación dañado.

Especificaciones técnicas

Número máximo de dispositivos conectados	100
Número máximo de grupos	9
Número máximo de usuarios	50
Videovigilancia	Hasta 10 cámaras o DVRs
Número máximo de usuarios	50
Número máximo de escenarios	5 <u>Más información</u>
<u>ReX</u> es (Repetidores)	1
Número de sirenas conectadas	hasta 10

Fuente de alimentación	110 – 240 V CA, 50/60 Hz
Unidad de acumulación	Li-ion 2 A·h (hasta 15 horas de operación autónoma*)
Consumo de energía de la red	10 W
Tamper anti-sabotaje	Si
Banda de frecuencia	868.0–868.6 MHz o 868.7–869.2 MHz dependiendo de la región de venta
Potencia radiada efectiva	8.20 dBm / 6.60 mW (límite 25 mW)
Modulación de la señal de radio	GFSK
Rango de la señal de radio	Hasta 2000 m (sin obstáculos) <u>Más información</u>
Canales de comunicación	GSM (850/900/1800/1900 MHz), Ethernet
Instalación	Interior
Rango de temperaturas de funcionamiento	De -10°C a +40°C
Humedad de funcionamiento	Hasta 75%
Dimensiones generales	163 × 163 × 36 mm
Peso	350 g
Vida útil	10 años
Certificación	Clase de seguridad 2, clase ambiental II SP2 (GSM-SMS), SP5 (LAN) DP3 de conformidad con los requisitos de las normas EN 50131-1, EN 50131-3, EN 50136-2, EN 50131-10, EN 50136-1, EN 50131-6, EN 50131-5-3

Cumplimiento de estándares

Garantía

Los dispositivos “AJAX SYSTEMS MANUFACTURING” LIMITED LIABILITY COMPANY tienen una garantía de 2 años tras la compra y no se aplica a la batería preinstalada.

Si el dispositivo no funciona correctamente, debería contactar primero con el servicio de soporte: ¡en la mitad de los casos los problemas técnicos se pueden

resolver de forma remota!

[Texto completo de la garantía](#)

[Contrato de usuario](#)

Soporte técnico: **support@ajax.systems**