

Manual de usuario del KeyPad

Actualizado June 16, 2021



KeyPad es un teclado táctil inalámbrico que controla el sistema de seguridad Ajax. Utilizado en espacios interiores. Arma y desarma una estancia, informa del estado del sistema, está protegido contra forzado de contraseña e incluye alarma silenciosa si se introduce el código a la fuerza.

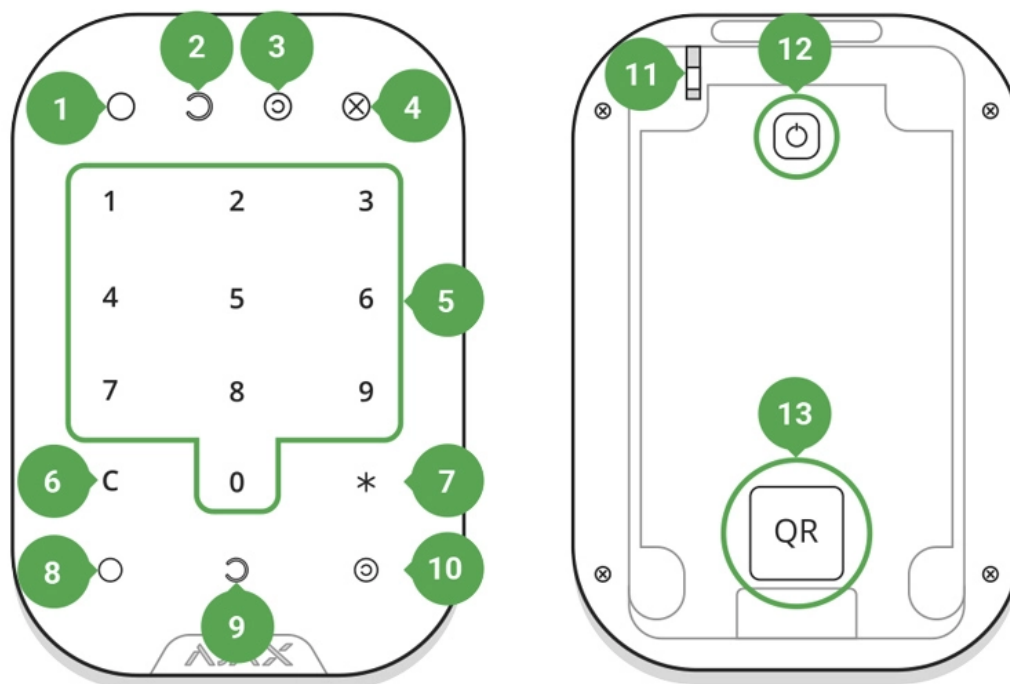
KeyPad solo funciona con el sistema de seguridad Ajax (no se puede usar en sistemas de seguridad de otros fabricantes), al conectarse al hub mediante el protocolo de seguridad Jeweller. Rango de comunicación: hasta 1700 metros sin obstáculos.



El dispositivo solo funciona con el hub y no es compatible con uartBridge o ocBridge Plus.

KeyPad se configura a través de una aplicación móvil para smartphones con iOS y Android.

Elementos funcionales



1. Indicador de modo armado
2. Indicador de modo desarmado
3. Indicador de modo noche
4. Indicador de fallo de funcionamiento
5. Bloque numérico de botones táctiles
6. Botón borrar
7. Botón de función
8. Botón armar
9. Botón desarmar
10. Botón modo noche
11. Interruptor antisabotaje
12. Botón de encendido/apagado
13. Código QR

Para quitar el panel SmartBracket, deslícelo hacia abajo (la pieza perforada es necesaria para activar el interruptor antisabotaje en caso de que se intente arrancar el dispositivo de la superficie).

Principio de operación de KeyPad

KeyPad es un teclado táctil que controla el sistema de seguridad Ajax.

KeyPad es un teclado fijo que se ubica dentro de una estancia. Permite armar el sistema con un código digital o pulsando un botón, activar el modo noche, desarmar la estancia y notificar a la compañía de seguridad privada del intento de forzado del sistema de seguridad (sin comprometer al usuario de ningún modo).

KeyPad está equipado con LED que indican el estado del sistema de seguridad, informan de cualquier problema con los detectores o de la interrupción de la comunicación con el hub. Los botones grandes y táctiles se encienden si el dispositivo se activa por contacto: el código se puede introducir sin luz externa. Vida útil de las pilas preinstaladas: hasta 2 años.

Para activar el teclado, toque el panel táctil, los botones se encenderán y se emitirá un sonido de encendido.

Si la batería está baja, la luz se encenderá al mínimo, independientemente de los ajustes.


Si no toca ningún botón en cuatro segundos, KeyPad reducirá el brillo y tras 12 segundos el dispositivo entrará en suspensión.



¡Si el dispositivo entra en suspensión borrará los comandos introducidos!

KeyPad permite usar códigos de una longitud entre 4 y 6 dígitos. El código introducido se enviará al hub tras pulsar los botones: (armar), (desarmar) y (modo noche). Los dígitos introducidos erróneamente se pueden borrar pulsando el botón (eliminar).

Si introduce un código incorrecto tres veces en 30 minutos, el teclado se bloqueará durante un tiempo establecido en los ajustes. El hub ignorará cualquier código introducido y notificará a los usuarios del sistema de seguridad del intento de adivinar la contraseña. El teclado se desbloqueará automáticamente cuando expire el tiempo de bloqueo o cuando el administrador lo desbloquee.

KeyPad también puede activar el modo armado del sistema pulsando el botón  (activar modo armado) sin introducir el código maestro. Estas características están desactivadas por defecto.

Si pulsa el botón * (Función) sin introducir la contraseña, el comando * se enviará al hub y se ejecutará la opción establecida en la aplicación.

KeyPad puede notificar a una compañía de seguridad privada si se desarma el sistema por la fuerza, mediante el **Código de coacción**. A diferencia del botón de pánico del mando, si se introduce dicho código, el usuario no se verá comprometido por la activación de la sirena, y el teclado y el mensaje de la aplicación notificarán de la eliminación exitosa del modo armado del sistema.

Indicación de funcionamiento de KeyPad

Cuando se enciende el teclado, se enciende el LED correspondiente al modo de funcionamiento del sistema de seguridad (O, C, (c)).

Los indicadores muestran el estado del sistema: modo armado, modo desarmado o modo noche.

La información se actualiza incluso si otro dispositivo de control cambia el estado del sistema, como por ejemplo el mando o la aplicación. Si el dispositivo se enciende por contacto, se actualiza el estado.

Evento	Indicación
El LED parpadea X	El indicador notifica de un fallo en el sistema de seguridad Ajax, y se enciende si KeyPad no se puede conectar al hub. Puede consultar la naturaleza del fallo en la aplicación Ajax Security System
Pulsar un botón táctil	Un pitido corto, el LED de estado de armado actual del sistema parpadea una vez

El sistema está en modo armado	Breve señal acústica, el LED se enciende: "Modo armado" / "Modo noche"
El sistema está en modo desarmado	Dos breves señales acústicas, el LED se enciende: "Modo armado desactivado"
Código maestro incorrecto	Larga señal acústica, la luz del bloque numérico parpadea 3 veces durante la señal acústica
Se detecta un problema activando el modo armado (no se encuentra un detector, por ejemplo)	Un pitido largo, el LED de estado de armado actual del sistema parpadea 3 veces
El hub no responde al comando, no hay conexión	Larga señal acústica, la luz del indicador de error se enciende durante la señal acústica
KeyPad está bloqueado debido a intentos de adivinar la contraseña	Larga señal acústica, los indicadores de modo armado, desarmado y noche parpadean simultáneamente
Batería baja	<p>Tras introducir el código correcto y activar el modo armado o desarmado del sistema, el indicador de error del teclado parpadeará suavemente. Los botones táctiles se bloquearán durante el tiempo de actividad del indicador.</p> <p>Si intenta encender el teclado con las pilas descargadas, emitirá una larga señal acústica, el indicador de error se encenderá y apagará suavemente y el dispositivo se apagará</p>

Conexión al hub

Antes de conectarlo:

1. Instale la aplicación Ajax en su smartphone siguiendo las recomendaciones de las instrucciones del hub. Cree una cuenta, añada el hub a la aplicación y cree al menos una estancia.
2. Vaya a la aplicación Ajax.
3. Encienda el hub y compruebe la conexión a internet (mediante cable Ethernet y/o conexión 2G).
4. Asegúrese de que el hub está desarmado y no empezará a actualizarse comprobando su estado en la aplicación móvil.



Solo los usuarios con permisos de administrador pueden añadir el dispositivo al hub

Cómo conectar KeyPad al hub:

1. Abra una estancia en la aplicación móvil o en la aplicación web y seleccione la opción «**Añadir dispositivo**».
2. Dele un nombre al dispositivo, escanee o escriba manualmente el **código QR** (situado en la carcasa y en la caja) y seleccione la estancia.
3. Cuando el hub empiece a buscar un dispositivo y comience la cuenta atrás, encienda el KeyPad pulsando el botón de encendido durante 3 segundos: el LED parpadeará una vez.

Para que el detector 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 al Ajax hub falla, KeyPad se apagará después de 5 segundos. Repita el intento de conexión.



El KeyPad no tiene contraseñas preestablecidas. Antes de usar el teclado, asegúrese de configurar las contraseñas necesarias: general, personal, así como la contraseña para desarmar bajo coacción.

Selección de la ubicación de KeyPad

Al seleccionar la ubicación de instalación para el KeyPad, se debe considerar la distancia con cualquier obstáculo que impida la transmisión de la señal de radio: paredes, entresijos u objetos de gran tamaño ubicados dentro de la habitación.






El dispositivo está destinado exclusivamente a la instalación en interiores.

No instale el KeyPad:

1. Cerca de equipo de transmisión de radio, incluidos los que operan en redes móviles 2G, 3G o 4G, routers Wi-Fi, transceptores, emisoras de radio, o el Ajax hub (que utilice red 2G).
2. Cerca del cableado eléctrico.
3. Cerca de objetos metálicos o espejos que puedan atenuar la señal.
4. Fuera de la estancia (al aire libre).
5. En estancias con temperatura o humedad que exceda los límites permisibles.
6. Más cerca de 1 metro del hub.



Compruebe la intensidad de la señal en el lugar de instalación

Durante la prueba se puede ver la intensidad de la señal en la aplicación y en el panel de KeyPad – LED azul  (modo armado),  (modo desarmado) y  (modo noche), así como la **X** en rojo (error).

Si la intensidad de señal alcanza solo una barra, no se puede garantizar la estabilidad de funcionamiento del sistema de seguridad. ¡Tome las medidas necesarias para mejorar la calidad de la señal! Al menos, mueva el dispositivo: reubicarlo incluso 20 cm puede mejorar significativamente la calidad de recepción.


Si luego de mover el dispositivo, la intensidad de la señal sigue siendo baja o inestable, utilice un repetidor de señal de radio ReX.

El panel táctil de KeyPad está diseñado para funcionar con el dispositivo instalado en la superficie. Si usa KeyPad manualmente, no podemos garantizar el correcto funcionamiento de los botones táctiles.


Estados

Parámetro	Valor
Temperatura	Temperatura del dispositivo. Se mide en el procesador y cambia gradualmente
Intensidad señal Jeweller	Intensidad de la señal entre el hub y el KeyPad
Nivel de batería	<p>Nivel de carga de la batería del dispositivo. Hay dos estados:</p> <ul style="list-style-type: none">• OK• Batería baja <p><u>Cómo se muestra la carga de la batería en las apps Ajax</u></p>
Tapa	Modo antisabotaje del detector, que reacciona a daños o separación de la carcasa
Conexión	Estado de la conexión entre el hub y el teclado
Desactivación temporal	Muestra el estado del dispositivo: activo, completamente deshabilitado por el usuario o solo las notificaciones sobre la activación del botón antisabotaje del dispositivo están desactivadas
Firmware	Versión del firmware del detector
ID del dispositivo	Identificador del dispositivo

Ajustes

1. Dispositivos 

2. KeyPad

3. Ajustes 


Ajuste	Valor
Primer campo	Nombre del dispositivo, se puede editar
Estancia	Seleccionar la estancia virtual a la que se asigna el dispositivo

Gestión de grupos	Selecciona el grupo de seguridad al que está agregado el KeyPad
Opción de acceso	<p>Seleccionar tipos de código de acceso para armar/desarmar</p> <ul style="list-style-type: none"> • Solo código del teclado • Solo código del usuario • Código del usuario y teclado
Código del teclado	Contraseña de KeyPad para armar/desarmar
Código de coacción	Seleccione un <u>código de coacción (alarma silenciosa)</u>
Botón de función	<p>Selección de la función del botón *</p> <ul style="list-style-type: none"> • Off — el botón Function está desactivado y no ejecuta ningún comando cuando se lo pulsa • Alarma — pulsando el botón Function, el sistema envía una alarma a la estación de monitoreo de la central receptora de alarmas y a todos los usuarios • Silenciar alarma de incendio interconectada — cuando se presiona, silencia la alarma de incendio de los detectores FireProtect/FireProtect Plus. La opción funciona solo si la alarma de incendios interconectada está habilitada <p><u>Más información</u></p>
Armar sin contraseña	Si está activada, permite armar el sistema sin contraseña al pulsar el botón de modo armado
Autobloqueo de acceso no autorizado	Si está activada, el teclado se bloqueará durante el tiempo establecido en los ajustes al introducir tres veces la contraseña incorrecta.
Tiempo de autobloqueo (min)	Tiempo de bloqueo tras varios intentos fallidos de contraseña
Brillo	Brillo del teclado
Volumen de botones	Volumen del teclado
Alertar con sirena al pulsar botón pánico	El ajuste aparece al seleccionar el modo de

	<p>funcionamiento Alarma para el botón Función.</p> <p>Si esta opción está habilitada, al presionar el botón Función se activan las sirenas instaladas en el objeto</p>
Test de intensidad señal Jeweller	Activa el modo test de intensidad de señal del dispositivo
Test de atenuación de señal	Activa del modo de test de atenuación de señal de KeyPad (disponible en dispositivos con firmware 3.50 y superior)
Desactivación temporal	<p>Permite al usuario desconectar el dispositivo sin eliminarlo del sistema.</p> <p>Existen dos opciones disponibles:</p> <ul style="list-style-type: none"> • Totalmente: el dispositivo no ejecutará comandos del sistema ni participará en escenarios de automatización, y el sistema ignorará las alarmas del dispositivo y otras notificaciones • Solo tapa: el sistema solo ignorará las notificaciones sobre la activación del botón antisabotaje del dispositivo <p><u>Más información sobre la desactivación temporal de dispositivos</u></p>
Guía del usuario	Abre el Manual de usuario de KeyPad
Desvincular dispositivo	Desconecta KeyPad del hub y elimina su configuración

Para cada usuario, se puede establecer una contraseña compartida o personal en el teclado.

Para configurar una contraseña personal:

1. Vaya a ajustes del perfil (**Hub** → **Ajustes**  → **Usuario** → **Ajustes de perfil**)
2. Haga clic en **"Ajustes de código de acceso"** (en este menú también puede ver el identificador del usuario)
3. Establezca el **Código de usuario** y el **Código de coacción**






¡Cada usuario ajusta su propia contraseña individual!


Gestión de la seguridad por contraseñas

Puede controlar la seguridad en todo el lugar o de grupos independientes mediante contraseñas comunes o personales (configuradas en la app).




Si se utiliza una contraseña personal, el nombre del usuario que armó o desarmó el sistema se muestra en las notificaciones y en el historial de eventos del hub. Si se utiliza una contraseña común, no se muestra el nombre del usuario que ha cambiado el modo de seguridad.


Gestión de la seguridad de todo el lugar utilizando una contraseña común

Introduzca la **contraseña común** y pulse la tecla de **armado**  / **desarmado**  / **activación del modo Noche** .

Por ejemplo: 1234 → 

Gestión de la seguridad de grupo con una contraseña común

Introduzca la **contraseña común**, pulse el icono *****, introduzca el **ID de grupo** y pulse la tecla de **armado**  / **desarmado**  / **activación del modo Noche** .

Por ejemplo: 1234 → * → 2 → 

¿Qué es el ID de grupo?




Si se asigna un grupo al KeyPad (**campo de permiso de Armado/Desarmado** en la configuración del teclado), no es necesario introducir el ID de grupo. Para gestionar el modo de armado de este grupo, es suficiente introducir una contraseña común o personal.


Tenga en cuenta que si se asigna un grupo al KeyPad, no podrá gestionar el **modo Noche** con una contraseña común.

En este caso, el **modo Noche** solo se puede gestionar con una contraseña personal (si el usuario tiene los derechos adecuados).

Derechos en el sistema de seguridad Ajax




Gestión de la seguridad de todo el lugar utilizando una contraseña personal


Introduzca el **ID de usuario**, pulse *****, introduzca la **contraseña personal** y pulse la tecla de **armado**  / **desarmado**  / **activación del modo Noche** .

Por ejemplo: 2 → ***** → 1234 → 

¿Qué es el ID de usuario?

Gestión de la seguridad de grupo usando una contraseña personal

Introduzca el **ID de usuario**, pulse *****, introduzca la **contraseña personal**, pulse *****, introduzca el **ID de grupo** y pulse la tecla de **armado**  / **desarmado**  / **activación del modo Noche** .

Por ejemplo: 2 → ***** → 1234 → ***** → 5 → 

¿Qué es el ID de grupo?

¿Qué es el ID de usuario?

Si se asigna un grupo al KeyPad (**campo de permiso de Armado/Desarmado** en la configuración del teclado), no es necesario introducir el ID de grupo. Para gestionar el modo de armado de este grupo, es suficiente introducir una contraseña personal.

Uso de una contraseña de coacción

Una **contraseña de coacción** le permite provocar una alarma silenciosa e imitar la desactivación de la alarma. Una alarma silenciosa significa que la app Ajax y las sirenas no sonarán para delatarle. Pero tanto una central receptora de

alarma como otros usuarios serán alertados al instante. Puede utilizar la contraseña de coacción **personal** y **común**.


¿Qué es una contraseña de coacción y cómo se usa?




Los escenarios y las sirenas reaccionan al desarmado bajo coacción de la misma manera que al desarmado normal.


Para utilizar una contraseña de coacción común:

Introduzca la **contraseña de coacción común** y pulse la tecla de **desarmado** .

Por ejemplo: 4321 → 

Para utilizar una contraseña de coacción personal:

Introduzca el **ID de usuario**, pulse *****, luego introduzca la **contraseña de coacción personal** y pulse la tecla de **desarmado** .

Por ejemplo: 2 → ***** → 4422 → 

Cómo opera la función de silenciar la alarma de incendios

El teclado KeyPad puede silenciar las alarmas interconectadas de los detectores de incendios al presionar el botón “Función” (si el ajuste correspondiente está activado). La reacción del sistema al pulsar un botón depende de la configuración y del estado del sistema:

- **La Interconexión de alarmas en FireProtect ya se ha propagado** — con la primera pulsación del botón Function, todas las sirenas de los detectores de incendios se silencian, excepto las que registraron la alarma. Al pulsar de nuevo el botón se silencian los detectores restantes.
- **El tiempo de retardo de la interconexión de alarmas está corriendo** — al pulsar el botón Function, se silencia la sirena del detector FireProtect/FireProtect Plus activado.

Pruebas de funcionamiento

El sistema de seguridad Ajax permite realizar pruebas para comprobar la funcionalidad de los dispositivos conectados.

Las pruebas no empiezan directamente, sino en un período de 36 segundos si se usan los ajustes por defecto. El tiempo hasta que comience la prueba depende de los ajustes del período de escaneo del detector (párrafo sobre los ajustes “**Jeweller**” en los ajustes del hub).

Test de intensidad señal

Test de atenuación

Instalación de KeyPad



¡Antes de instalar el detector, asegúrese de que ha seleccionado la ubicación idónea y de que sigue las directrices de este manual!



Se debe instalar KeyPad en una superficie vertical.

1. Fije el panel SmartBracket a la superficie usando los tornillos incluidos, use al menos dos puntos de sujeción (uno de ellos encima del interruptor antisabotaje). Si usa cualquier otro aditamento de fijación, asegúrese de que no daña o deforma el panel.



Solo se podrá usar cinta adhesiva de doble cara para fijar KeyPad temporalmente. La cinta se secará con el tiempo y podría hacer que el teclado se caiga y se dañe.

2. Ponga el KeyPad en el panel de fijación y ajuste el tornillo de montaje en la parte inferior de la carcasa.

En cuanto el teclado esté fijado al SmartBracket, el LED **X** (Error) parpadeará: esta será la señal de que el interruptor antisabotaje del detector se ha activado.

Si el LED **X** (error) del teclado no se activa tras la instalación en el SmartBracket, compruebe el estado del interruptor antisabotaje en la [aplicación Ajax Security System](#) y ajuste la firmeza del panel.

Si el teclado se arranca de la superficie o se retira del panel de fijación, recibirá la alerta correspondiente.

Mantenimiento de KeyPad y sustitución de la batería

Compruebe frecuentemente el correcto funcionamiento de KeyPad.

La batería instalada en el teclado asegura hasta por 2 años la operación autónoma (con una frecuencia de consulta del hub de 3 minutos). Si la batería de KeyPad está baja, el sistema de seguridad enviará las notificaciones correspondientes, y el indicador de “**Error**” se encenderá y apagará suavemente tras cada introducción de la contraseña correcta.

[Cuánto tiempo funcionan los dispositivos Ajax usando las baterías, y qué influye en esto](#)

[Reemplazo de la batería](#)

Equipo completo

1. KeyPad
2. Panel de fijación SmartBracket
3. Pilas AAA (preinstaladas) — 4 unidades
4. Kit de instalación
5. Guía rápida de inicio

Especificaciones técnicas

Tipo de sensor	Capacitivo
Tamper anti-sabotaje	Sí
Protección contra forzado de código de acceso	Sí
Banda de frecuencia	868.0–868.6 MHz o 868.7–869.2 MHz dependiendo de la región de venta
Compatibilidad	Solo funciona con Ajax hubs y repetidores de señal
Potencia máxima de radiofrecuencia de salida	Hasta 20 mW
Modulación de la señal de radio	GFSK
Rango de la señal de radio	Hasta 1700 m (sin obstáculos) Más información
Fuente de alimentación	4 pilas AAA
Voltaje de la fuente de alimentación	3 V (las baterías se instalan en pares)
Duración de la batería	Hasta 2 años
Método de instalación	Interior
Rango de temperaturas de operación	De -10°C a +40°C
Humedad de funcionamiento	Hasta 75%
Dimensiones generales	150 × 103 × 14 mm
Peso	197 g
Vida útil	10 años
Certificación	Clase de seguridad 2, clase ambiental II de conformidad con la norma EN 50131-1, EN 50131-3, 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**