

# Manual de usuario del KeyPad

Actualizado May 10, 2024



El **KeyPad** es un teclado táctil e inalámbrico que gestiona el sistema Ajax. Se utiliza en interiores. Puede armar y desarmar estancias, informar del estado del sistema, está protegido contra adivinación de código e incluye una alarma silenciosa si coaccionan a un usuario a introducir el código.

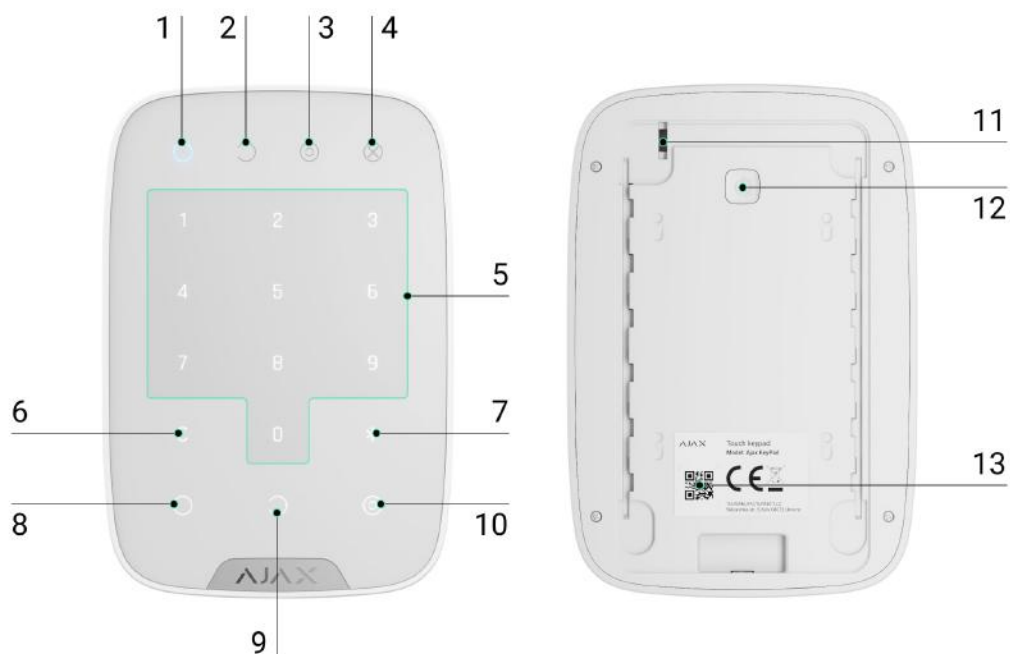
El KeyPad solo funciona con el sistema Ajax (no se puede usar en sistemas de seguridad de terceros), al conectarse al hub mediante el protocolo de seguridad Jeweller. Rango de comunicación: hasta 1.700 metros sin obstáculos.



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 **Armado**

2. Indicador de **Desarmado**

3. Indicador de **Modo Noche**

4. Indicador de **Fallo de funcionamiento**

5. Bloque numérico de botones táctiles

6. Botón **Restablecer**

7. **Botón de función**

8. Botón **Armar**

9. Botón **Desarmar**

10. Botón **Modo Noche**

11. Interruptor antisabotaje

12. Botón de encendido

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 del KeyPad

El KeyPad es un teclado táctil para gestionar el sistema Ajax. Puede gestionar los modos de seguridad de toda la instalación o de grupos de seguridad independientes, a la vez que permite la activación del **Modo Noche**. Admite la función de “alarma silenciosa”: el usuario informa a la CRA que se le coaccionan a desarmar el sistema, pero las sirenas o apps Ajax no emiten sonidos.

El KeyPad permite gestionar los modos de seguridad con los códigos. Antes de ingresar un código, debe activar (“despertar”) el teclado con un toque. Una vez que se activa el dispositivo, el botón de indicación del estado de seguridad se enciende y el teclado emite un pitido.

### El KeyPad admite los siguientes tipos de códigos:





- **El código del teclado:** un código común, se establece para el teclado. Cuando se utiliza, todos los eventos se envían a la app Ajax por parte del teclado.
- **El código del usuario:** un código personal, se establece para un usuario conectado al hub. Cuando se utiliza, todos los eventos se envían a la app Ajax por parte del usuario.
- **El código de acceso:** se establece para una persona no registrada en el sistema. Cuando se utiliza, los eventos se envían a la app Ajax por parte de la persona a la que se le ha sido asignado este código.
- **El Código URR** es un código de acceso para las unidades de respuesta rápida (URR) que se activa tras la alarma y es válido durante un tiempo determinado. Cuando el código se activa y se utiliza, los eventos se envían a las apps Ajax con un nombre relacionado con este código.



La cantidad de códigos personales, de códigos de acceso y de códigos URR depende del modelo del hub.

El brillo y el volumen de botones se ajustan en la [Configuración](#) del teclado. Si la batería se descarga, la luz de fondo se enciende al nivel mínimo independientemente de la configuración. Al cambiar al modo de ahorro de energía, el teclado restablece los comandos ingresados.

Si transcurren 4 segundos sin que toque el teclado, el Keypad reducirá el brillo de la luz de fondo y, después de 8 segundos, entrará en modo de ahorro de energía y apagará la pantalla.

El 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 restablecer pulsando el botón  (Restablecer).

El Keypad también permite gestionar los modos de seguridad sin introducir el código, si la función **Armar sin código** está habilitada en la configuración. Dicha función está desactivada por defecto.

## Botón de función

El teclado Keypad tiene un **Botón de función** que opera en 3 modos:

- **Apagado:** el botón está desactivado y no ocurre nada después de presionarlo.
- **Alarma:** después de pulsar el **Botón de función**, el sistema envía una alarma a la Central Receptora de Alarmas (CRA) y a todos los usuarios.
- **Silenciar alarma de incendios interconectada:** después de presionar el **Botón de función**, la sirena de los [detectores de incendio Ajax](#) se silenciará. Solo disponible si está habilitada la Alarma de incendios interconectada (Hub → Configuración → Servicio → Ajustes de detectores de incendio).

## Código de coacción

El código de coacción permite simular la desactivación de las alarmas. A diferencia del botón de pánico, si se introduce dicho código, el usuario no se verá comprometido por la activación de la sirena, y el teclado y la app Ajax notificarán del desarmado del sistema con éxito.

### **Disponibles hay los siguientes tipos de códigos de coacción:**

- **El código del teclado:** un código de coacción común. Cuando se utiliza, los eventos se envían a la app Ajax por parte del teclado.
- **El código del usuario:** un código de coacción personal, se establece para cada usuario conectado al hub. Cuando se utiliza, los eventos se envían a la app Ajax por parte del usuario.
- **El código de acceso:** códigos de coacción. Se establecen para personas no registradas en el sistema. Cuando se utiliza, los eventos se envían a la app Ajax por parte de la persona a la que se le ha sido asignado este código.

### **Más información**

## **Autobloqueo de acceso no autorizado**

Al ingresar un código incorrecto tres veces en un minuto, el teclado se bloqueará por el tiempo especificado en la configuración. Durante este período de tiempo, el hub ignorará todos los códigos e informará a los usuarios del sistema de seguridad y a la CRA sobre los intentos de adivinar el código.

El teclado se desbloqueará automáticamente transcurrido el tiempo de bloqueo establecido en la configuración. Pero un usuario o un PRO con derechos de administrador puede desbloquear el teclado en la aplicación Ajax.

## **Armado en dos etapas**

El KeyPad admite el armado del sistema en dos etapas. Cuando esta función está habilitada, el sistema solo se armará después de volver a armarse con el SpaceControl o después de restaurar el detector final (por ejemplo, al cerrar la puerta de entrada en la que está instalado el DoorProtect).

# Protocolo de transmisión de datos Jeweller

El teclado utiliza el protocolo de radio Jeweller para transmitir eventos y alarmas. Este es un protocolo de transferencia de datos inalámbrica y bidireccional que proporciona una comunicación rápida y fiable entre el hub y los dispositivos conectados.

Jeweller admite el cifrado de bloque con clave flotante y la autenticación de dispositivos en cada sesión para evitar el sabotaje y la suplantación del dispositivo. El protocolo proporciona un sondeo regular de los dispositivos por parte del hub a intervalos de 12 a 300 segundos (se establece en la app Ajax), para gestionar la comunicación con todos los dispositivos y mostrar sus estados en las apps Ajax.

## Más sobre Jeweller

# Transmisión de eventos a la CRA

El sistema Ajax puede transmitir alarmas a la app de monitoreo PRO Desktop, así como a la central receptora de alarmas (CRA) en SurGard (Contact ID), SIA (DC-09), ADEMCO 685 y otros formatos de protocolo propietarios. La lista de las CRAs a las que se puede conectar el sistema Ajax está disponible en el enlace.

El KeyPad puede transmitir los siguientes eventos:

- Código de coacción introducido.
- Botón de pánico presionado (si el Botón de función opera en modo del **Botón de función**).
- El teclado está bloqueado debido a un intento de adivinar el código.
- Alarma / recuperación del interruptor antisabotaje.
- Pérdida / restauración de la conexión con el hub.

- Desactivación / activación del teclado.
- Intento fallido de armar el sistema de seguridad (con la verificación de integridad habilitada).

Al recibir una alarma, el operador de la CRA sabe qué sucedió y a dónde hace falta enviar a una unidad de respuesta rápida. La direccionabilidad de cada dispositivo Ajax permite enviar a PRO Desktop o a la CRA no solo eventos, sino también el tipo de dispositivo, el grupo de seguridad, el nombre asignado y la estancia de ubicación. La lista de parámetros transmitidos puede diferir según el tipo de la CRA y el protocolo de comunicación con la CRA seleccionado.



El ID del dispositivo y el número de bucle (zona) se pueden encontrar en sus estados en la app Ajax.

## 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 <b>X</b>	El indicador notifica de un fallo en el sistema Ajax, y se enciende si KeyPad no se puede conectar al hub. Puede consultar la naturaleza del fallo en la <a href="#">aplicación Ajax Security System</a>
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 sonora, el LED se enciende: <b>Modo armado / Modo Noche</b>
El sistema está en modo desarmado	Dos breves señales sonoras, el LED se enciende: <b>Modo armado desactivado</b>
Código maestro incorrecto	Larga señal sonora, la luz del bloque numérico parpadea 3 veces durante la señal sonora
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 sonora, la luz del indicador de error se enciende durante la señal sonora
El KeyPad está bloqueado debido a un intento de adivinar el código	Larga señal sonora, los indicadores de modo armado, desarmado y Modo Noche parpadean simultáneamente
Batería baja	<p>Tras introducir el código correcto y activar el modo armado o desarmado del sistema, el <b>indicador de error</b> 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 baterías descargadas, emitirá una larga señal sonora, el indicador de error se encenderá y apagará suavemente y el dispositivo se apagará.</p>

## Notificaciones sonoras sobre fallos de funcionamiento

Si algún dispositivo está sin conexión o la batería está baja, el KeyPad puede notificar a los usuarios del sistema con una señal sonora. Los indicadores LED **X** de los teclados parpadearán. Las notificaciones sobre fallos de funcionamiento se mostrarán en el historial de eventos, el texto de los SMS o las notificaciones push.

Para habilitar las notificaciones sonoras sobre fallos de funcionamiento, utilice las [apps Ajax PRO y PRO Desktop](#):

1. Haga clic en **Dispositivos** , seleccione un hub y abra su configuración   
Haga clic en **Servicio** → **Sonidos y alertas**
2. Habilite las opciones: **Si algún dispositivo tiene batería baja** y **Si algún dispositivo está sin conexión**.
3. Haga clic en **Atrás** para guardar la configuración.



La configuración de las notificaciones sonoras sobre fallos de funcionamiento está disponible para todos los hubs con la versión de firmware OS Malevich 2.15 y posterior.

Las notificaciones sonoras sobre fallos de funcionamiento son compatibles con el KeyPad con la versión de firmware 5.57.1.1 y posterior.

Evento	Indicación	Nota
Si algún dispositivo está sin conexión.	Dos pitidos breves, el indicador de <b>Fallo de funcionamiento X</b> parpadea dos veces.  El pitido suena una vez al minuto hasta que todos los dispositivos en el sistema estén en línea.	Los usuarios pueden posponer la indicación sonora por 12 horas.

<p>Si el KeyPad está sin conexión.</p>	<p>Dos pitidos breves, el indicador de <b>Fallo de funcionamiento X</b> parpadea dos veces.</p> <p>El pitido suena una vez al minuto hasta que el teclado en el sistema esté en línea.</p>	<p>Es imposible posponer la indicación sonora.</p>
<p>Si algún dispositivo tiene la batería baja.</p>	<p>Tres pitidos breves, el indicador de <b>Fallos de funcionamiento X</b> parpadea tres veces.</p> <p>El pitido suena una vez al minuto hasta que la carga de la batería esté restaurada o el dispositivo esté eliminado.</p>	<p>Los usuarios pueden posponer la indicación sonora por 4 horas.</p>

Las notificaciones sonoras sobre fallos de funcionamiento aparecerán una vez que la indicación del teclado esté completada. Si se producen varios fallos de funcionamiento en el sistema, el teclado notificará sobre la pérdida de conexión entre el dispositivo y el hub primero.

## Conexión al hub

### Antes de conectarlo:

1. Instale la [app 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 app 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 app 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 app móvil o en la app web y seleccione la opción «**Añadir dispositivo**».
2. Cree un nombre para el dispositivo, escanee o escriba manualmente el **código QR** (ubicado en la carcasa y en la caja) y seleccione la estancia.
3. Cuando el hub empiece a buscar un dispositivo y comience la cuenta regresiva, 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 una sola instalación protegida).

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, el KeyPad se apagará después de 5 segundos. Repita el intento de conexión.



El KeyPad no tiene códigos preestablecidos. Antes de usar el teclado, asegúrese de configurar los códigos necesarios: código del teclado (común), códigos de usuarios (personales), así como códigos de coacción (común y personales).

## 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, entrepisos u objetos de gran tamaño ubicados dentro de la estancia.






El dispositivo está destinado exclusivamente a la instalación en interiores.

### **No instale el KeyPad:**

1. Cerca del equipamiento 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 la red 2G).
2. Cerca del cableado eléctrico.
3. Cerca de objetos metálicos o espejos que puedan atenuar la señal.
4. Fuera de la instalación (en exteriores).
5. En lugares 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 app y en el panel del KeyPad – LED azul  (modo armado),  (modo desarmado) y  (Modo Noche), así como la **X** en rojo (error).

Si la intensidad de la 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.

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


## Estados

1. Dispositivos 

2. KeyPad


Parámetro	Significado
Temperatura	<p>Temperatura del dispositivo. Se mide en el procesador y cambia gradualmente.</p> <p>El error aceptable entre el valor en la app y la temperatura ambiente es de 2 °C.</p> <p>El valor se actualiza una vez que el dispositivo haya identificado un cambio de temperatura de al menos 2 °C.</p>

	<p>Puede configurar un escenario por temperatura para gestionar los dispositivos de automatización.</p> <p><b><u>Más información</u></b></p>
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"> <li>• <b>OK.</b></li> <li>• <b>Batería baja.</b></li> </ul> <p><b><u>Cómo se muestra la carga de la batería en las apps Ajax</u></b></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.
ReX	Muestra el estado de uso del <b><u>repetidor de señal de radio</u></b> .
Desactivación permanente	Muestra el estado del dispositivo: activo, completamente deshabilitado por el usuario o solo las notificaciones sobre la activación del interruptor antisabotaje del dispositivo están desactivadas.
Desactivación temporal única	Muestra el estado de la función de desactivación temporal única del dispositivo hasta el primer desarmado: activo, completamente desactivado por el usuario o solo las notificaciones sobre la activación del interruptor antisabotaje del dispositivo están desactivadas.
Firmware	Versión del firmware del teclado.
ID dispositivo	Identificador del dispositivo.

1. Dispositivos 

2. KeyPad

3. Configuración 

Parámetro	Significado
Nombre	Nombre del dispositivo, se puede editar.
Estancia	Seleccionar la estancia virtual a la que se asigna el dispositivo.
Gestión de grupos	Seleccionar el grupo de seguridad al que está asignado el KeyPad.
Opciones de acceso	<p>Seleccionar la forma de verificación para armar/desarmar:</p> <ul style="list-style-type: none"><li>• Solo códigos del teclado.</li><li>• Solo códigos del usuario.</li><li>• Códigos del teclado y de usuario.</li></ul> <div data-bbox="833 1220 1450 1524" style="border: 1px solid black; padding: 10px;"><p> Para activar los <b>Códigos de acceso</b> establecidos para personas no registradas en el sistema, elija una de las siguientes opciones en el teclado: <b>Solo códigos del teclado</b> o <b>Códigos del teclado y de usuario</b>.</p></div>
Código del teclado	Establecer un código para armar/desarmar.
Código de coacción	Establecer un <u><b>código de coacción para una alarma silenciosa</b></u> .
Botón de función	Seleccionar la función del botón *: <ul style="list-style-type: none"><li>• <b>Apagado</b>: el <b>Botón de función</b> está desactivado y no ejecuta ningún comando cuando se lo pulsa.</li></ul>

- **Alarma:** pulsando el **Botón de función**, el sistema envía una alarma a la CRA y a todos los usuarios.
- **Silenciar alarma de incendio interconectada:** después de presionar el botón, se silenciará la alarma de los detectores de incendio Ajax. La opción funciona solo si la alarma de incendio interconectada está habilitada.

### Más información

Armar sin código	Si está activada, permite armar el sistema sin código al pulsar el botón <b>Armar</b> .
Autobloqueo de acceso no autorizado	Si está habilitado, el teclado se bloqueará durante el tiempo preestablecido al introducir el código incorrecto tres veces seguidas en 1 minuto. Durante este tiempo, el sistema no se puede desarmar utilizando el KeyPad.
Tiempo de autobloqueo, min	Tiempo de bloqueo tras varios intentos fallidos de ingresar un código.
Brillo	Brillo de la retroiluminación del teclado.
Volumen de botones	Volumen del zumbador.
Alertar con sirena al presionar el botón de pánico	El ajuste aparece al seleccionar el modo de funcionamiento <b>Alarma</b> para el <b>Botón de función</b> .  Si esta opción está habilitada, al presionar el <b>Botón de función</b> se activan las sirenas instaladas en la estancia.
Test de intensidad señal Jeweller	Activa el modo Test de intensidad señal del dispositivo.
Test de atenuación de señal	Activa del modo de Test de atenuación de señal del KeyPad (disponible para los dispositivos con la versión de <b>firmware 3.50 y posterior</b> ).
Desactivación permanente	Permite al usuario desactivar el dispositivo sin eliminarlo del sistema.  Hay tres opciones disponibles:

	<ul style="list-style-type: none"> <li>• <b>No:</b> el dispositivo funciona en modo normal y transmite todos los eventos.</li> <li>• <b>Totalmente:</b> el dispositivo no ejecuta los comandos del sistema ni participa en los escenarios de automatización, y el sistema ignora las alarmas y otras notificaciones del dispositivo.</li> <li>• <b>Solo tapa:</b> el sistema ignora las notificaciones sobre la activación del interruptor antisabotaje del dispositivo.</li> </ul> <p><b><u>Más información</u></b></p>
Desactivación temporal única	<p>Muestra el estado de la función de desactivación temporal única del teclado.</p> <p>Hay tres opciones disponibles:</p> <ul style="list-style-type: none"> <li>• <b>No:</b> el teclado funciona en modo normal.</li> <li>• <b>Solo tapa:</b> las notificaciones sobre la activación del interruptor antisabotaje del teclado están desactivadas hasta el primer desarmado.</li> <li>• <b>Totalmente:</b> el teclado está completamente excluido del funcionamiento del sistema hasta el primer desarmado. El dispositivo no sigue los comandos del sistema ni notifica sobre las alarmas u otros eventos.</li> </ul> <p><b><u>Más información</u></b></p>
Guía del usuario	Abre el manual de usuario del KeyPad.
Eliminar dispositivo	Desconecta el dispositivo del hub y elimina su configuración.

## Configuración de códigos

El sistema Ajax permite establecer un código del teclado, así como códigos personales para usuarios añadidos al hub.

Con la actualización de firmware OS Malevich 2.13.1, también proporcionamos la posibilidad de crear un código para personas no conectadas al hub. Es cómodo, por ejemplo, para otorgar a una empresa de limpieza el acceso a gestionar la seguridad. A continuación podrá encontrar más información de cómo establecer y usar cada tipo de códigos.


### Para establecer un código del teclado

1. Vaya a la configuración del teclado.
2. Elija la opción **Código del teclado**.
3. Establezca un código del teclado necesario.

### Para establecer un código de coacción del teclado

1. Vaya a la configuración del teclado.
2. Elija la opción **Código de coacción**.
3. Establezca un código de coacción del teclado necesario.


### Para establecer un código personal para un usuario registrado

1. Vaya a la configuración de perfil: **Hub** → **Configuración**  → **Usuario** → **Configuración de usuario**.  
En este menú se puede ver también el ID de usuario.
2. Elija la opción **Ajustes de códigos de acceso**.
3. Establezca el **Código del usuario** y el **Código de coacción**.



¡Cada usuario ajusta su propio código personal!

### Para establecer un código de acceso para una persona no registrada en el sistema

1. Vaya a la configuración del hub: **Hub** → **Configuración** .
2. Elija la opción **Códigos de acceso del teclado**.
3. Cree un **Nombre de usuario** y un **Código de acceso**.

Si desea establecer un código de coacción, configurar acceso a los grupos, Modo Noche, ID del código, temporalmente desactivar o borrar este código, elijalo en la lista e introduzca cambios.



El código de acceso puede establecerse o configurarse por un PRO o un usuario con derechos de administrador. Dicha función se admite por los hubs con la versión de firmware OS Malevich 2.13.1 y posterior. El panel de control Hub no admite los códigos de acceso.

## Para configurar el código URR

Solo un PRO con permisos para configurar el sistema puede crear y configurar los códigos URR en las [apps Ajax PRO](#). Puede encontrar más información sobre la configuración de esta función en [este artículo](#).



Los códigos URR son compatibles con los hubs (excepto el modelo Hub) con la versión de firmware OS Malevich 2.17 y posterior.

## Gestión de la seguridad por códigos

Puede gestionar la seguridad de toda la instalación o de grupos separados mediante códigos generales, personales o URR , así como mediante códigos de acceso (se configuran por un PRO o un usuario con permisos de administrador).

Si se utiliza un código personal o un código de acceso, 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 un código URR, se muestra el nombre del código URR. Si se utiliza un código común, no se muestra el nombre del usuario que ha cambiado el modo de seguridad.




Los **códigos de acceso del teclado** se admiten por los hubs con la versión de firmware OS Malevich 2.13.1 y posterior. El panel de control Hub no admite los códigos de acceso.


Los **códigos URR** son compatibles con los hubs (excepto el modelo Hub) con la versión de firmware OS Malevich 2.17 y posterior.


## Gestión de la seguridad de toda la instalación utilizando un código del teclado común

Introduzca el **código del teclado común** y pulse la tecla de **armado**  / **desarmado**  / **Modo Noche** .

Por ejemplo: 1234 → 

## Gestión de la seguridad de grupo con un código del teclado común

Introduzca el **código común**, pulse el icono **\***, introduzca el **ID de grupo** y pulse la tecla de **armado**  / **desarmado**  / **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 un código común o personal.


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

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

### Derechos en el sistema Ajax




## Gestión de la seguridad de toda la instalación utilizando un código del usuario personal


Introduzca el **ID de usuario**, pulse **\***, introduzca el **código del usuario personal** y pulse la tecla de **armado**  / **desarmado**  / **Modo Noche** .

Por ejemplo: 2 → \* → 1234 → 

[¿Qué es el ID de usuario?](#)

## Gestión de la seguridad de grupo usando un código del usuario personal

Introduzca el **ID de usuario**, pulse **\***, introduzca el **código personal**, pulse **\***, introduzca el **ID de grupo** y pulse la tecla de **armado**  / **desarmado**  / **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 un código del usuario personal.

## Gestión de seguridad de la instalación entera con un código de acceso

Introduzca el **código de acceso** y presione el botón de **armado**  / **desarmado**  / **Modo Noche** .

Por ejemplo: 1234 → 

# Gestión de seguridad de un grupo con un código común

Introduzca el **código de acceso**, presione \*icono de estrella\*, introduzca el **ID de un grupo** y presione el botón de **armado**  / **desarmado**  / **Modo Noche** .

Por ejemplo: 1234 → \* → 2 → 

¿Qué es el ID de grupo?

## Uso de un código de coacción

Un **código de coacción** permite provocar una alarma silenciosa e imitar la desactivación de la alarma. Una alarma silenciosa significa que la app Ajax y las sirenas no le delatarán si alguien le fuerza a introducir el código. Pero tanto la CRA como otros usuarios serán alertados al instante. Puede utilizar el código de coacción **personal** y **común**. También, en el menú **Códigos de acceso de los teclados** es posible configurar el código de coacción para personas no registradas en el sistema.


Qué es el código 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 un código de coacción común:**

Introduzca el **código de coacción** común y pulse el botón de **desarmado** .


Por ejemplo: 4321 → 


**Para utilizar un código de coacción personal del usuario registrado:**

Introduzca el **ID de usuario**, pulse \*, luego introduzca el **código de coacción personal** y pulse el botón de **desarmado** .

Por ejemplo: 2 → \* → 4422 → 

## Para utilizar el código de coacción de una persona no registrada en el sistema:

Introduzca un **código de coacción** establecido en el menú **Códigos de acceso del teclado** y presione el botón de **desarmado** .




Por ejemplo: 4567 → 


## Uso del código URR

El código URR se activa tras activarse la alarma durante el tiempo establecido en la configuración del hub, y es válido durante un periodo especificado. Esto garantiza que dicho código solo se utilizará en caso de riesgo, a diferencia de los códigos del teclado o de usuario.




### Cómo configurar el código URR


#### Gestionar la seguridad de la instalación utilizando el código URR:

Introduzca el **Código URR** y pulse el botón **armado**  / **desarmado**  / **Modo Noche** .

Por ejemplo: 1234 → 

#### Gestionar la seguridad del grupo utilizando el código URR:

Introduzca el **Código URR**, pulse \*, introduzca el **ID de grupo**, y pulse el botón **armado**  / **desarmado**  / **Modo Noche** .

Por ejemplo: 1234 → \* → 2 → 

## Función Silenciar alarma de incendios interconectada

El teclado KeyPad puede silenciar las alarmas de incendios interconectadas al presionar el **Botón de función** (si el ajuste correspondiente está activado). La

reacción del sistema al pulsar el botón depende de la configuración y el estado del sistema:

- **Alarma de incendios interconectada activada:** con la primera pulsación del **Botón de función**, 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 de función**, se silencia la sirena de los detectores de incendio Ajax activado.

## Más información sobre la Alarma de incendios interconectada



Con la actualización [OS Malevich 2.12](#), los usuarios pueden silenciar las alarmas de incendio en sus grupos sin que esto afecte a los detectores en los grupos a los que no tienen acceso.

[Más información](#)

## Pruebas de funcionamiento

El sistema 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 usa la configuración por defecto. El tiempo hasta que comience la prueba depende de los ajustes del intervalo de ping del detector (pestaña **Jeweller** en la configuración del hub).

### Test de intensidad señal Jeweller

### Test de atenuación de señal

## Instalación del KeyPad



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



Se debe instalar el KeyPad en una superficie vertical.

1. Fije el panel de montaje 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 dañe ni deforme el panel.



Solo se podrá usar cinta adhesiva de doble cara para fijar el 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 montaje 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 de la tapa en la [app Ajax Security System](#) y ajuste la firmeza del panel.

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

## Mantenimiento del KeyPad y reemplazo de la batería

Compruebe el correcto funcionamiento del KeyPad con regularidad.

La batería instalada en el KeyPad garantiza hasta 2 años de funcionamiento autónomo (con un intervalo de ping del hub de 3 minutos). Si la batería del KeyPad

está baja, el sistema de seguridad enviará las notificaciones correspondientes, y el indicador de fallos de funcionamiento se encenderá y se apagará suavemente tras cada introducción del código correcto.

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

### Reemplazo de la batería

## Especificaciones técnicas

### Todas las especificaciones técnicas del KeyPad Jeweller

### Cumplimiento de normas

## Garantía

La garantía de los productos de Limited Liability Company «Ajax Systems Manufacturing» es válida durante 2 años tras la compra.

Si el dispositivo no funciona correctamente, póngase en contacto con el soporte técnico de Ajax primero. En la mayoría de los casos, los problemas técnicos se pueden resolver de forma remota.

### Obligaciones de la garantía

### Contrato de usuario

## Póngase en contacto con el soporte técnico Ajax

- Correo electrónico
- Telegram
- **Número de teléfono: 0 (800) 331 911**

Suscríbese a nuestro boletín sobre una vida más segura. Sin correo basura

**Suscribirse**