Manual de usuario del Superior KeyPad Plus G3 Jeweller

Actualizado 26 de mayo de 2026



El **Superior KeyPad Plus G3 Jeweller** es un teclado inalámbrico diseñado para gestionar sistemas Ajax. Los usuarios pueden autenticarse mediante mandos Tag, tarjetas Pass y códigos. El dispositivo está diseñado solo para uso en interiores.

El teclado funciona en un sistema Ajax e intercambia datos con el hub mediante el protocolo seguro de comunicación por radio Jeweller.

El Superior KeyPad Plus G3 Jeweller es un dispositivo de la línea de productos Superior. Solo los partners acreditados de Ajax Systems pueden vender, instalar y mantener los productos Superior.

Comprar el Superior KeyPad Plus G3 Jeweller

Elementos funcionales



1. Indicador de **Armado**.
2. Indicador de **Desarmado**.
3. Indicador de **Modo Noche**.
4. Indicador de **Fallo de funcionamiento**.
5. Lector de Pass/Tag.
6. Teclado numérico.
7. Botón de **Función**.
8. Botón de **Restablecimiento**.
9. Botón **Armar**.
10. Botón **Desarmar**.
11. Botón Modo Noche.
12. Panel de montaje SmartBracket. Para retirar el panel, desatornille el tornillo de fijación y deslice el panel hacia abajo.
13. Pieza perforada del panel de montaje. Es necesaria para activar el interruptor antisabotaje ante cualquier intento de arrancar el dispositivo de la superficie. No la rompa.
14. Interruptor antisabotaje.
15. Botón de encendido.
16. Código QR con el ID del dispositivo. Se utiliza para añadir el dispositivo al hub.

17. Tornillo de fijación para fijar el teclado en el SmartBracket.

Hubs compatibles

Se requiere un hub Ajax con OS Malevich 2.35 y posterior para que el teclado funcione.

Comprobar la compatibilidad de los dispositivos

Principio de funcionamiento



El Superior KeyPad Plus G3 Jeweller cuenta con grandes botones táctiles, un lector para autorización sin contacto e indicadores LED. El teclado se utiliza para controlar los modos de seguridad, enviar una alarma de pánico o silenciar la alarma de incendio.

El Superior KeyPad Plus G3 Jeweller tiene indicadores LED que muestran el modo de seguridad actual y los fallos de funcionamiento del teclado (si los hubiera). El estado de seguridad solo se muestra cuando el teclado está activo (la retroiluminación del dispositivo está encendida).



El Superior KeyPad Plus G3 Jeweller puede utilizarse en condiciones de poca luz, ya que dispone de retroiluminación. La pulsación de los botones va acompañada de una señal sonora. El brillo de la retroiluminación y el volumen del teclado se pueden ajustar en la configuración. Si no se toca el teclado durante 4 segundos, el Superior KeyPad Plus G3 Jeweller reduce el brillo de la retroiluminación. Tras 8 segundos de inactividad, entra en modo de ahorro de energía y apaga la pantalla.

Si la carga de la batería es baja, la retroiluminación se enciende al nivel mínimo, independientemente de los ajustes.

Control de seguridad

El Superior KeyPad Plus G3 Jeweller puede armar y desarmar todo el sitio o grupos específicos y activar el **Modo Noche**. Los usuarios pueden controlar la seguridad utilizando el Superior KeyPad Plus G3 Jeweller mediante:

1. **Tarjetas o mandos**. Para identificar a los usuarios de forma rápida y segura, el Superior KeyPad Plus G3 Jeweller utiliza la tecnología DESFire®. DESFire® s basa en la norma internacional ISO 14443 y combina el cifrado de 128 bits y la protección contra el copiado. El Tag y el Pass admiten esta tecnología y son compatibles con el Superior KeyPad Plus G3 Jeweller.

2. **Códigos**. El Superior KeyPad Plus G3 Jeweller admite códigos generales, códigos personales y códigos para usuarios no registrados.

Códigos de acceso

- **Código del teclado** es un código general configurado para el teclado. Cuando se utiliza, todos los eventos se envían a las apps Ajax por parte del teclado.
- **Código de usuario** es un código personal configurado para los usuarios conectados al hub. Cuando se utiliza, todos los eventos se envían a las apps Ajax por parte del usuario.
- **Código de acceso del teclado** es un código configurado para una persona que no está registrada en el sistema. Cuando se utiliza, los eventos se envían a las apps Ajax con un nombre relacionado con este código.
- **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 periodo determinado. Cuando el código se activa y se utiliza, los eventos se envían a las apps Ajax con un nombre relacionado con este código.

> El número de códigos personales, códigos de acceso al teclado y códigos URR depende del modelo del hub.
>
> Comprobar la compatibilidad de los dispositivos

Los permisos de acceso y los códigos pueden ajustarse en las apps Ajax. Si el código se ve comprometido, puede cambiarse a distancia, por lo que no es necesario invitar a un instalador al sitio. Si un usuario pierde su Pass o Tag, un administrador o un PRO con permisos de configuración del sistema puede bloquear instantáneamente el dispositivo en la app. Mientras tanto, un usuario puede utilizar un código personal para controlar el sistema.

Control de seguridad de los grupos

El Superior KeyPad Plus G3 Jeweller permite controlar la seguridad de los grupos (si el Modo Grupo está activado). Un administrador o un PRO con permisos para configurar el sistema también puede ajustar la configuración del teclado para

determinar qué grupos se compartirán (grupos de teclado). Para obtener más información sobre cómo gestionar la seguridad de los grupos, consulte esta sección.

Botón de Función

El Superior KeyPad Plus G3 Jeweller tiene el botón de **Función** que funciona en uno de tres modos:

- **Desactivado**: el botón de **Función** está desactivado y no ocurre nada cuando el usuario pulsa este botón.
- **Pánico**: tras pulsar el botón de **Función**, el sistema envía una alarma a la central receptora de alarmas y a todos los usuarios.
- **Silenciar alarma de incendio**: tras pulsar el botón de **Función**, el sistema silencia la alarma de los detectores de incendio Ajax. Solo disponible si está habilitada la función de Alarma de incendio interconectada (Hub → Configuración → Servicio → Configuración de detectores de incendio).

Código de coacción

El Superior KeyPad Plus G3 Jeweller admite un **código de coacción** que permite al usuario simular la desactivación de la alarma. En este caso, ni la app Ajax ni las sirenas instaladas en la instalación revelarán sus acciones. No obstante, la compañía de seguridad y otros usuarios del sistema de seguridad serán alertados de la incidencia.

Más información

Autobloqueo de acceso no autorizado

Si se introduce un código incorrecto o se utiliza un dispositivo de acceso no verificado tres veces seguidas en el plazo de 1 minuto, el teclado se bloqueará durante el tiempo especificado en su configuración. Durante este tiempo, el hub ignorará todos los códigos y dispositivos de acceso, al tiempo que informará a los usuarios del sistema de seguridad sobre intentos de acceso no autorizado.

Un PRO o un usuario con permisos de configuración del sistema puede desbloquear el teclado a través de la app antes de que transcurra el tiempo de bloqueo establecido.

Armado en dos etapas

El Superior KeyPad Plus G3 Jeweller puede participar en el armado en dos etapas, pero no puede utilizarse como dispositivo de segunda etapa. El proceso de armado en dos etapas mediante Tag o Pass es similar al uso de un código personal o general en el teclado.

Más información

Fire alarm muting

El Superior KeyPad Plus G3 Jeweller puede silenciar una alarma de incendio interconectada pulsando el botón de **Función** (si el parámetro correspondiente está activado). La reacción del sistema al pulsar el botón depende de la configuración y del estado del sistema:

- **La alarma de incendio interconectada ya se ha propagado**: con la primera pulsación del botón, se silencian las alarmas de todos los detectores de incendio, excepto los que registraron la alarma. Al pulsar el botón otra vez, se silencian los detectores restantes.
- **El tiempo de retardo de las alarmas interconectadas está corriendo**: al pulsar el botón de **Función**, se silencia la sirena de los detectores de incendio Ajax activados.

Tenga en cuenta que la opción solo está disponible si la función de **Alarma de incendio interconectada** está habilitada.

Más información

Protocolo de transmisión de datos Superior Jeweller

Superior Jeweller es un protocolo de radio mejorado para dispositivos Superior, que garantiza el cumplimiento de la norma **Grade 3** (EN 50131). Aplica cifrado avanzado y

salto de frecuencia. El salto de frecuencia completo solo está disponible cuando todos los dispositivos del sistema utilizan Superior Jeweller. Si al menos un dispositivo funciona con el protocolo Jeweller normal, el sistema estará limitado al **Grade 2**: el cifrado se mantiene, pero el salto está desactivado. Los dispositivos Superior también pueden funcionar con el protocolo Jeweller normal, según el hub.

Más información

Comunicación cifrada avanzada

La comunicación entre el Superior KeyPad Plus G3 Jeweller y el hub está protegida por un algoritmo de cifrado avanzado que garantiza la confidencialidad y la integridad de los datos. Esto significa que todos los datos sensibles del mensaje están cifrados, y cada mensaje incluye un código de autenticación único que permite al sistema comprobar que los datos no han sido modificados durante la transmisión. El sistema puede detectar manipulaciones y rechazar mensajes falsificados o alterados, garantizando una protección robusta contra ataques tanto pasivos como activos. Esto garantiza una comunicación segura entre el dispositivo y el hub, así como una protección fiable del sistema y de los datos.

Más información sobre la comunicación cifrada avanzada

Salto de frecuencia

Para cumplir con los requisitos de Grade 3, el Superior KeyPad Plus G3 Jeweller utiliza el **salto de frecuencia** para la comunicación por radio con el hub (o el repetidor de señal de radio). Al utilizar este método, el hub y los dispositivos añadidos a él cambian su frecuencia de funcionamiento según un patrón especificado. La secuencia de saltos abarca un conjunto definido de canales dentro de las bandas operativas, y los dispositivos cambian de frecuencia de forma sincronizada con el hub. Aunque algunos canales se vean afectados por inhibición, los mensajes pueden transmitirse con éxito a través de otros canales. El salto de frecuencia aumenta la fiabilidad y el rendimiento del sistema, y garantiza su resistencia a las interferencias intencionadas y a los intentos de inhibición.

El salto de frecuencia no crea retardos ni pausas durante la comunicación por radio y no reduce la velocidad de transmisión de datos. Si se añaden repetidores al sistema,

se utiliza el salto de frecuencia para todas las comunicaciones por radio: «dispositivo ↔ repetidor» y «repetidor ↔ hub».

> ⚠ El sistema utiliza el salto de frecuencia para la comunicación por radio solo si todos los dispositivos inalámbricos admiten este método.
>
> Si al menos un dispositivo añadido al sistema no admite el salto de frecuencia, el hub y todos los dispositivos cambian a las frecuencias de funcionamiento de ese dispositivo y no utilizan el salto de frecuencia para la comunicación por radio.

Más información sobre el salto de frecuencia

Más información sobre la inhibición

Transmisión de eventos a la CRA

El sistema Ajax puede transmitir alarmas a la app de monitorización Ajax PRO Desktop, así como a la central receptora de alarmas (CRA) en los formatos **SurGard (Contact ID), SIA (DC-09), ADEMCO 685** y otros protocolos.

El Superior KeyPad Plus G3 Jeweller puede transmitir los siguientes eventos:

1. Armado/desarmado del sistema.
2. Introducción del código de coacción.
3. Pulsación del botón de pánico.
4. Bloqueo del teclado debido a un intento de acceso no autorizado.
5. Intento fallido de armar el sistema de seguridad (si la comprobación de integridad del sistema está activada).
6. Alarma antisabotaje. Recuperación del interruptor antisabotaje.
7. Pérdida y restablecimiento de la conexión con el hub.
8. Desactivación permanente/activación del dispositivo.
9. Desactivación temporal única/activación del dispositivo.

Cuando se recibe una alarma, el operador de la central receptora de alarmas sab exactamente lo que ha ocurrido y adónde enviar una unidad de respuesta rápida. La direccionabilidad de los dispositivos Ajax permite enviar eventos a **Ajax PRO Desktop** o a la CRA con el tipo de dispositivo, su nombre, grupo de seguridad y estancia virtual.

La lista de parámetros transmitidos puede variar en función del tipo de la CRA y del protocolo de comunicación seleccionado.

Puede encontrar el ID del dispositivo y el número de bucle (zona) en los estados del dispositivo.

Seleccionar el lugar de instalación



Al elegir dónde colocar el Superior KeyPad Plus G3 Jeweller, tenga en cuenta los parámetros que afectan a su funcionamiento:

- Intensidad señal Jeweller

Al diseñar el sistema de la instalación, siga las recomendaciones de colocación del dispositivo. El sistema Ajax debe ser diseñado e instalado por profesionales. Aquí encontrará una lista de partners recomendados.

Lo mejor es colocar el Superior KeyPad Plus G3 Jeweller en interiores, cerca de l entrada. Esto permite a los usuarios desarmar el sitio antes de entrar en las instalaciones o hasta que expiren los retardos al entrar. Los usuarios también pueden armar rápidamente el sitio al salir de las instalaciones.

La altura de instalación recomendada es de 1.3–1.5 metros por encima del suelo. Instale el teclado en una superficie plana y vertical. Esto garantiza que el Superior KeyPad Plus G3 Jeweller esté bien fijado a la superficie y ayuda a evitar falsas alarmas antisabotaje.

⚠ Al sostener el Superior KeyPad Plus G3 Jeweller en las manos o utilizarlo sobre una mesa, no podemos garantizar que los botones táctiles funcionen correctamente.

Intensidad de la señal

La intensidad de la señal viene determinada por el número de paquetes de datos no entregados o dañados durante un periodo de tiempo determinado. El icono ||| en la pestaña **Dispositivos** – en las apps Ajax indica la intensidad de la señal:

- **tres barras**: intensidad de la señal excelente;
- **dos barras**: intensidad de la señal buena;
- **una barra**: intensidad de la señal baja, no se garantiza un funcionamiento estable;
- **icono tachado**: sin señal.

⚠ Compruebe la intensidad de la señal Jeweller antes de la instalación final. Con una intensidad de señal de una o cero barras, no garantizamos que el dispositivo funcione correctamente. Reubique el dispositivo, ya que cambiar su posición incluso 20 cm puede mejorar considerablemente la intensidad de la señal. Si la señal sigue siendo mala o inestable después de la reubicación, utilice un repetidor de señal de radio.

Consulte la sección Pruebas de funcionamiento para saber cómo ejecutar el test de intensidad señal Jeweller.

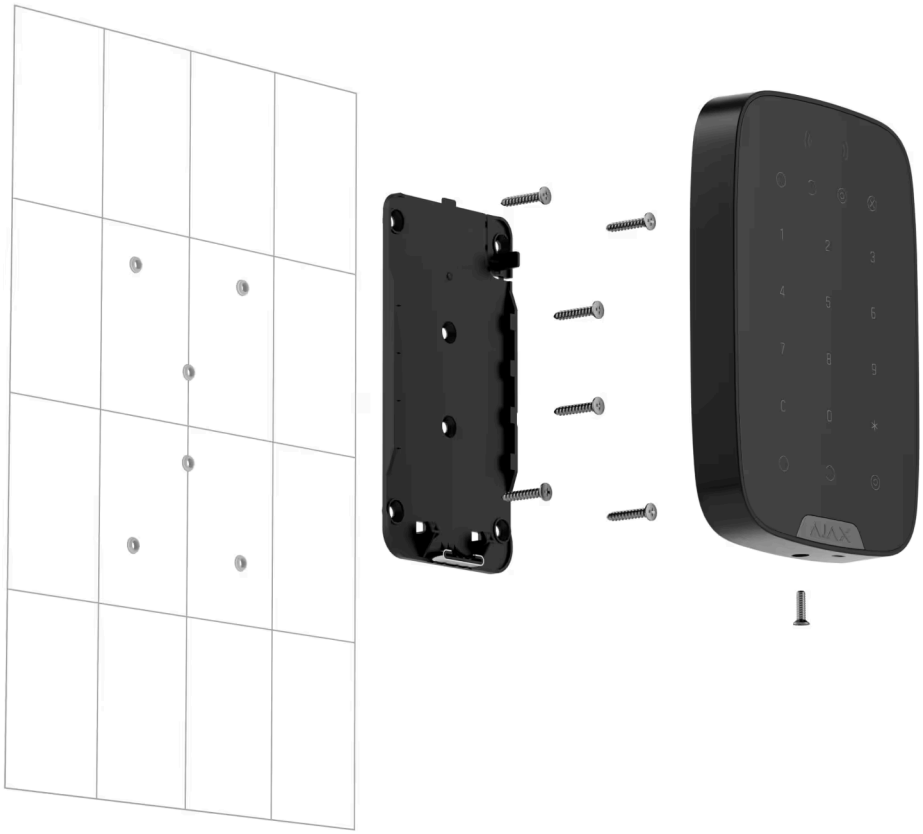
Qué es el test de intensidad de señal Jeweller

Dónde no deberá instalar el teclado

1. En exteriores. Esto puede provocar fallos en el dispositivo.

2. En lugares donde los cables de alimentación o Ethernet, objetos de decoración u otras cosas puedan obstruir el teclado.
3. En lugares con temperatura y humedad fuera de los límites permisibles. Esto puede dañar el dispositivo.
4. A menos de 1 m del hub o del repetidor de señal de radio.
5. En lugares con intensidad de señal Jeweller baja o inestable.

Instalación



⚠ Antes de instalar el Superior KeyPad Plus G3 Jeweller asegúrese de haber seleccionado la ubicación óptima que cumpla con los requisitos de este manual.

Para instalar el dispositivo:

1. Desatornille el tornillo de fijación situado en la parte inferior del dispositivo y retire el panel de montaje SmartBracket del teclado.

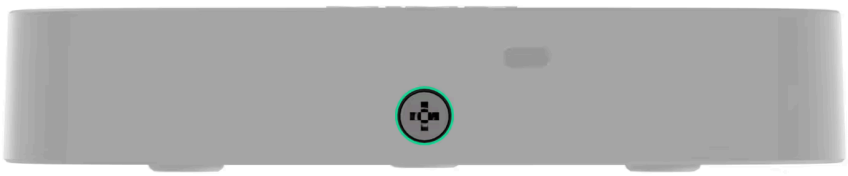
2. Añada el dispositivo al sistema.
3. Fije temporalmente el panel SmartBracket con cinta adhesiva de doble cara u otros sujetadores temporales.

> La cinta adhesiva de doble cara solo puede utilizarse para una instalación temporal. El dispositivo fijado con la cinta puede despegarse de la superficie en cualquier momento. Mientras el dispositivo esté fijado con la cinta, la alarma antisabotaje no se activará cuando el dispositivo se separe de la superficie.

4. Coloque el teclado en el panel de montaje SmartBracket. El indicador LED **X** del dispositivo parpadeará, mostrando que la carcasa del dispositivo está cerrada.
5. Ejecute pruebas de funcionamiento.
6. Si los tests se realizan correctamente, retire el teclado del SmartBracket.
7. Fije el panel SmartBracket a la superficie con los tornillos suministrados. Utilice todos los puntos de fijación.

> Cuando utilice otros elementos de fijación, asegúrese de que no dañen ni deformen el panel.

8. Coloque el teclado en el panel de montaje SmartBracket.
9. Apriete el tornillo de fijación en la parte inferior de la carcasa del teclado. El tornillo es necesario para una fijación más fiable y para proteger el teclado de un desmontaje rápido.



Añadir al sistema

⚠ El hub y el dispositivo que funcionan con frecuencias de radio diferentes son incompatibles. El rango de frecuencias de radio del dispositivo puede variar según la región. Recomendamos adquirir y utilizar dispositivos Ajax en la misma región. Puede verificar el rango de frecuencias de radio operativas con el servicio de asistencia técnica.

Compruebe la compatibilidad del dispositivo antes de añadirlo al sistema. Solo los partners verificados pueden añadir y configurar dispositivos Superior en las apps Ajax PRO.

Tipos de cuentas y sus permisos

Antes de añadir un dispositivo

1. Instale una app Ajax PRO.
2. Inicie sesión en una cuenta PRO o cree una nueva.
3. Seleccione un espacio o cree uno nuevo.
4. Añada al menos una estancia virtual.
5. Añada un hub compatible al espacio. Asegúrese de que el hub esté encendido y tenga acceso a Internet a través de Ethernet, Wi-Fi y/o red móvil.
6. Compruebe los estados en la app Ajax para asegurarse de que el espacio está desarmado y el hub no está iniciando una actualización.

Añadir al hub

1. Abra una app Ajax PRO. Seleccione un espacio al que desea añadir el dispositivo.
2. Vaya a la pestaña **Dispositivos** – y pulse **Añadir dispositivo**.
3. Asigne un nombre al dispositivo.
4. Escanee el código QR o introduzca manualmente el ID del dispositivo. El código QR con el ID está ubicado en la carcasa del dispositivo. También se duplica en el embalaje del dispositivo.



5. Seleccione una estancia virtual y un grupo de seguridad (si el Modo Grupo está activado).
6. Pulse **Añadir** y comenzará la cuenta regresiva.
7. Encienda el dispositivo pulsando el botón de encendido durante 3 segundos.



Si la conexión falla, inténtelo de nuevo en 5 segundos. Si ya se ha añadido el número máximo de dispositivos al hub, recibirá una notificación de error cuando intente añadir uno más.

Una vez añadido al hub, el dispositivo aparecerá en la lista de dispositivos del hub en la app Ajax. La frecuencia de actualización de los estados de los dispositivos en la lista depende de la configuración de **Jeweller** o **Jeweller/Fibra** y es de 36 segundos por defecto.

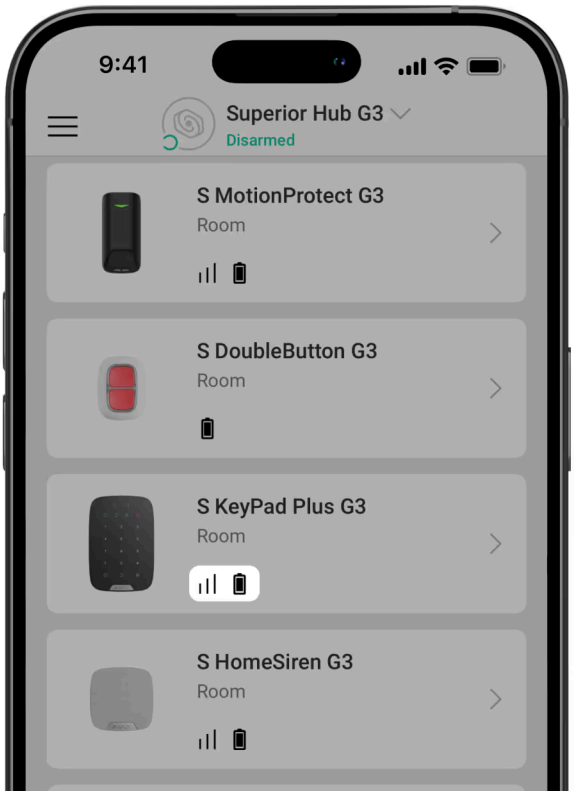
El Superior KeyPad Plus G3 Jeweller solo funciona con un hub. Al vincularse con un nuevo hub, deja de enviar eventos al antiguo. Añadir el teclado a un hub nuevo no lo elimina automáticamente de la lista de dispositivos del hub antiguo. Esto debe hacerse a través de la app Ajax.

Pruebas de funcionamiento

Un sistema Ajax proporciona varios tipos de tests para ayudar a seleccionar el lugar correcto de instalación de los dispositivos. Para el Superior KeyPad Plus G3 Jeweller, están disponibles los siguientes tests:

- Test de intensidad señal Jeweller: para determinar la intensidad y la estabilidad de la señal entre el hub (o el repetidor de señal de radio) y el dispositivo a través del protocolo inalámbrico de transmisión de datos Jeweller en el lugar de instalación del dispositivo.
- Test de atenuación de la señal: para disminuir o aumentar la potencia del transmisor de radio; para comprobar la estabilidad de la comunicación entre el dispositivo y el hub, se simula el entorno cambiante del sitio.

Iconos

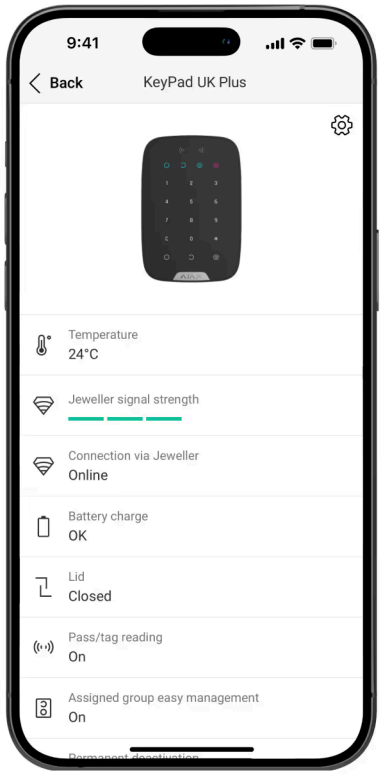


Los iconos en la app Ajax muestran algunos de los estados del Superior KeyPad Plus G3 Jeweller. Los iconos pueden comprobarse en la pestaña **Dispositivos** .

Ícono	Significado
	Intensidad de la señal Jeweller. Muestra la intensidad de la señal entre el hub y el dispositivo. El valor recomendado es de 2–3 barras. Más información
	Nivel de carga de la batería del dispositivo. Más información
RE	El dispositivo funciona a través del repetidor de señal de radio. Más información
	La **Lectura de pass/tag** está activada en la configuración del teclado.
	El dispositivo está en el modo de test de atenuación de señal. Más información
	El dispositivo se ha desactivado permanentemente. Más información

	Las notificaciones de alarma antisabotaje se han desactivado permanentemente. Más información
	El dispositivo se ha desactivado hasta el primer desarmado del sistema. Más información
	Las notificaciones de alarma antisabotaje se han desactivado hasta el primer desarmado del sitio. Más información
Offline	El dispositivo ha perdido la conexión con el hub o el hub ha perdido la conexión con el servidor Ajax Cloud.
Not transferred	El dispositivo no se ha transferido al nuevo hub. Más información

Estados



Los estados muestran información sobre el dispositivo y sus parámetros de funcionamiento. Los estados del Superior KeyPad Plus G3 Jeweller se pueden

encontrar en apps Ajax:

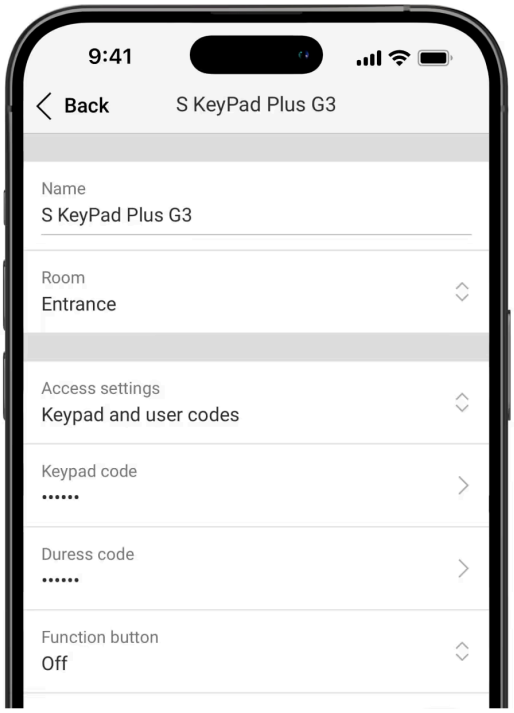
1. Vaya a la pestaña **Dispositivos** .
2. Seleccione el **Superior KeyPad Plus G3 Jeweller** en la lista.

Parámetro	Significado
Importación de datos	Muestra el error al transferir datos al nuevo hub: • **Error**: el dispositivo no se ha transferido al nuevo hub. Más información
Fallo de funcionamiento	Al pulsar sobre (i), se abre la lista de fallos de funcionamiento del dispositivo. El campo solo se muestra si se detecta un fallo de funcionamiento.
Temperatura	Temperatura del dispositivo. Se mide por el procesador y cambia en función de la temperatura ambiente. Puede crear un escenario por temperatura para controlar los dispositivos de automatización. Más información
Intensidad señal Jeweller	Intensidad de la señal Jeweller entre el dispositivo y el hub (o el repetidor de señal de radio). El valor recomendado es de 2–3 barras. Jeweller es un protocolo para la transmisión de eventos y alarmas.
Conexión vía Jeweller	Estado de la conexión a través del canal Jeweller entre el dispositivo y el hub (o el repetidor): • **En línea**: el dispositivo está conectado al hub (o al repetidor). Estado normal. • **Sin conexión**: el dispositivo ha perdido la conexión con el hub (o el repetidor). Compruebe la conexión del dispositivo.
Potencia transmisor	Muestra la potencia seleccionada del transmisor. El parámetro aparece cuando se selecciona la opción **Máx.** o **Atenuación** en el menú **Test de atenuación de señal**. Más información
<Range extender name>	Estado de la conexión del dispositivo al repetidor de señal de radio: • **En línea**: el dispositivo está conectado al repetidor. • **Sin conexión**: el dispositivo ha perdido la conexión con el repetidor. El campo se muestra si el dispositivo funciona a través del repetidor de señal de radio.

Carga de batería	Nivel de carga de la batería del dispositivo. Hay dos estados disponibles: • **OK**. • **Batería baja**. Cuando las baterías necesitan ser reemplazadas, las apps Ajax y la compañía de seguridad recibirán las notificaciones correspondientes. Más información
Tapa	Estado del interruptor antisabotaje del dispositivo que reacciona ante cualquier intento de arrancar el dispositivo de la superficie o abrir su carcasa: • **Abierto**: el dispositivo ha sido retirado del panel de montaje SmartBracket o la integridad de su carcasa ha sido comprometida. Compruebe si el dispositivo esté bien montado. • **Cerrado**: el dispositivo está instalado en el panel de montaje SmartBracket. La integridad de la carcasa del dispositivo ni del panel de montaje no está comprometida. Estado normal. Más información
Lectura de pass/tag	Muestra si el lector de tarjetas y mandos está activado.
Cambio fácil del modo armado	Muestra la configuración de la función de **Cambio fácil del modo armado**: • **Desactivado**: cada intento de armado o desarmado debe confirmarse introduciendo el código de acceso o acercando el dispositivo de acceso. • **Armado/desarmado utilizando dispositivos de acceso sin confirmar la acción con los botones**: permite a los usuarios cambiar los modos de seguridad mediante dispositivos de acceso sin confirmación pulsando los botones del teclado. • **Desarmado sin botón desarmar**: el sistema o sus grupos, cuya seguridad se gestiona con un código de acceso o dispositivos de acceso, se desarmarán sin confirmación pulsando los botones del teclado. ⚠ Debe establecer una longitud de código de acceso fija en la configuración del hub en la app Ajax PRO.
Cifrado avanzado	Estado de la comunicación con cifrado avanzado entre el dispositivo y el hub o el repetidor de señal de radio: • **Activo**: la comunicación del dispositivo está protegida por cifrado avanzado. • **Inactivo**: la comunicación del dispositivo funciona sin cifrado avanzado. Más información

Desactivación permanente	Estado de la función de desactivación permanente del dispositivo: • **No**: el dispositivo funciona en modo normal y transmite todos los eventos. • **Totalmente**: el administrador del hub ha excluido completamente el dispositivo del funcionamiento del sistema. El dispositivo no ejecuta comandos del sistema ni reporta alarmas u otros eventos. • **Solo tapa**: el administrador del hub ha desactivado las notificaciones sobre la activación de la alarma antisabotaje. Más información
Desactivación temporal única	Muestra el estado de la función de desactivación temporal única del dispositivo: • **No**: el dispositivo funciona en modo normal. • **Totalmente**: el dispositivo está completamente excluido del funcionamiento del sistema mientras el modo armado está activo. El dispositivo no ejecuta comandos del sistema ni reporta alarmas u otros eventos. • **Solo tapa**: las notificaciones sobre la activación de la alarma antisabotaje están desactivadas mientras el modo armado está activo. Más información
Firmware	Versión del firmware del dispositivo.
ID dispositivo	ID del dispositivo. También disponible en el código QR en la carcasa del dispositivo y en su caja de embalaje.
Dispositivo №	Número de dispositivo. Este número se transmite a la CRA en caso de alarma o evento.

Configuración



Para cambiar la configuración del Superior KeyPad Plus G3 Jeweller en las apps Ajax:

1. Vaya a la pestaña **Dispositivos** .
2. Seleccione el **Superior KeyPad Plus G3 Jeweller** en la lista.
3. Vaya a la **Configuración** .
4. Establezca los parámetros necesarios.
5. Pulse **Atrás** para guardar la nueva configuración.

Configuración	Significado
Nombre	Nombre del dispositivo. Se muestra en la lista de dispositivos del hub, el texto de los SMS y las notificaciones en el historial de eventos. Para cambiar el nombre del dispositivo, pulse sobre el campo de texto. El nombre puede contener hasta 24 caracteres latinos o hasta 12 caracteres cirílicos.
Estancia	Seleccionar la estancia virtual a la que el Superior KeyPad Plus G3 Jeweller está asignado. El nombre de la estancia se muestra en el texto de los SMS y de las notificaciones en el historial de eventos.
Gestión de grupos	Seleccionar el grupo de seguridad controlado por el dispositivo. Puede seleccionar todos los grupos o solo uno. El campo se muestra cuando el Modo Grupo está activado.

	Si la función de Grupo seguido está configurada para grupos, su estado de seguridad puede cambiar automáticamente en función de sus ajustes y de los estados de los iniciadores.
Opciones de acceso	Seleccionar el método de armado/desarmado: • Solo códigos del teclado. • Solo códigos del usuario. • Códigos del teclado y de usuario. Para activar los **Códigos de acceso del teclado** configurados para personas que no están registradas en el sistema, seleccione las opciones en el teclado: **Solo códigos del teclado** o **Códigos del teclado y de usuario**.
Código del teclado	Seleccionar un código general para el control de seguridad. Contiene de 4 a 6 dígitos.
Código de coacción	Seleccionar un código de coacción general para la alarma silenciosa. Contiene de 4 a 6 dígitos. Más información
Botón de Función	Seleccionar la función del botón (botón de **Función**): • **Desactivado**: el botón de función está desactivado y no ejecuta ningún comando al pulsarlo. • **Pánico**: tras pulsar el botón de función, el sistema envía una alarma a la CRA y a todos los usuarios. • **Silenciar alarma de incendio**: cuando se pulsa, el sistema silencia la alarma de los detectores de incendio Ajax. Solo disponible si la función de **Alarma de incendio interconectada** está habilitada. Más información
Protección contra pulsación accidental	Cuando está habilitado, el botón de **Función** debe pulsarse dos veces para enviar una alarma de pánico. Este parámetro está disponible si el **botón de Función** está establecido en **Pánico**.
Autobloqueo de acceso no autorizado	Cuando está habilitado, el teclado se bloqueará durante un tiempo preestablecido al introducir un código incorrecto o al utilizar dispositivos de acceso no verificados más de tres veces seguidas en 1 minuto. Un PRO o un usuario con permisos para configurar el sistema puede desbloc el teclado a través de la app antes de que transcurra el tiempo de bloqueo establecido.

Tiempo de autobloqueo, min	Seleccionar el período de bloqueo del teclado tras intentos de acceso no autorizados: • 3 minutos • 5 minutos • 10 minutos • 20 minutos • 30 minutos • 60 minutos • 90 minutos • 180 minutos Disponible si la opción de **Autobloqueo de acceso no autorizado** está habilitada.
Brillo	Ajustar el brillo de la retroiluminación de los botones del teclado. La retroiluminación solo funciona cuando el teclado está activo. Esta opción no afecta al nivel de brillo de los indicadores del lector Pass/Tag y de los modos de seguridad.
Volumen de botones	Seleccionar el volumen de los botones del teclado al pulsarlos.
Lectura de pass/tag	Cuando está habilitado, el modo de seguridad se puede controlar con dispositivos de acceso **Pass** y **Tag**.
Confirmación de autorización con código de acceso	Cuando está habilitado, los usuarios solo pueden armar o desarmar el sistema cuando hayan sido autorizados correctamente con dos formas de identificación, es decir, utilizando Pass o Tag e introduciendo el código de acceso correcto. Más información
Tiempo de confirmación	Seleccionar el tiempo máximo para confirmar la autorización con una contraseña tras la confirmación del dispositivo de acceso. Disponible si está habilitada la opción de **Confirmación de autorización con código de acceso**.
Cambio fácil del modo armado	Permite a los usuarios armar/desarmar el sistema sin confirmación pulsando los botones del teclado. Hay tres opciones disponibles: • **Desactivado**: cada intento de armado o desarmado debe confirmarse introduciendo el código de acceso o acercando el dispositivo de acceso. • **Armado/desarmado utilizando dispositivos de acceso sin confirmar la acción con los botones**: permite a los usuarios cambiar los modos de seguridad del sistema utilizando los dispositivos de acceso sin confirma... con los botones del teclado. • **Desarmado sin botón desarmar**: el sistema o sus grupos, cuya seguridad se gestiona con un código de acceso o dispositivos de acceso, se desarmarán

	sin confirmación pulsando los botones del teclado. ⚠ Debe establecer una longitud de código de acceso fija en la configuración del hub en la app Ajax PRO.
Armar sin código	Cuando está habilitado, el usuario puede armar la instalación sin introducir un código ni acercar el dispositivo de acceso personal. Si está deshabilitado, introduzca un código o acerque el dispositivo de acceso para armar el sistema. La pantalla para introducir el código aparece después de pulsar el botón ◯ **Armar**.
Activación automática con un retardo al entrar	Activa el teclado después de que cualquier dispositivo de seguridad inicie el Retardo al entrar. La función de activación automática también puede reducir la duración de la batería del teclado.
Alertar con sirena al presionar el botón de pánico	El parámetro se muestra si se selecciona la opción **Pánico** para el botón de **Función**. Cuando la opción está habilitada, las sirenas conectadas al sistema de seguridad emiten una alerta cuando se pulsa el botón (botón de **Función**).
Test de intensidad señal Jeweller	Cambia el dispositivo al modo de Test de intensidad señal Jeweller. El test permite comprobar la intensidad de la señal entre el hub (o el repetidor de señal de radio) y el dispositivo a través del protocolo inalámbrico de transmisión de datos Jeweller para seleccionar el lugar de instalación óptimo. Más información
Test de atenuación de señal	Cambia el dispositivo al modo de test de atenuación de señal. Más información
Restablecer pass/tag	Permite eliminar de la memoria del dispositivo todos los hubs relacionados con un Tag o un Pass. Más información
Guía del usuario	Abre el manual de usuario del Superior KeyPad Plus G3 Jeweller en la app Ajax.
Desactivación permanente	Permite al usuario desactivar los eventos del dispositivo sin eliminarlo del sistema. Hay tres opciones disponibles: • **No**: el dispositivo funciona en modo normal y transmite todos los eventos.

	• **Totalmente**: el dispositivo no ejecuta comandos del sistema ni participa en escenarios de automatización; el sistema ignora las alarmas y otras notificaciones del dispositivo. • **Solo tapa**: el sistema solo ignorará las notificaciones sobre la activación de la alarma antisabotaje del dispositivo. Más información
Desactivación temporal única	Permite al usuario desactivar los eventos del dispositivo hasta el primer desarmado. Hay tres opciones disponibles: • **No**: el dispositivo funciona en modo normal y transmite todos los eventos. • **Totalmente**: el dispositivo está completamente excluido del funcionamiento del sistema hasta el primer desarmado. El dispositivo no ejecuta comandos del sistema ni reporta alarmas u otros eventos. • **Solo tapa**: las notificaciones sobre la activación de la alarma antisabotaje están desactivadas hasta el primer desarmado. Más información
Eliminar dispositivo	Desvincula el dispositivo, lo desconecta del hub y elimina su configuración.

Configuración de códigos

En las apps Ajax PRO, en la configuración del hub, puede establecer los requisitos para la longitud de los códigos de acceso utilizados para la autorización de los usuarios y el acceso al sistema. Puede seleccionar la opción **Flexible (de 4 a 6 símbolos)** o definir la longitud fija del código: **4 símbolos**, **5 símbolos** o **6 símbolos**.

Al establecer una longitud de código fija, se restablecerán todos los códigos de acceso configurados previamente.

La longitud de código fija es necesaria para la función de **Cambio fácil del modo armado** que permite desarmar el sistema sin pulsar el botón **Desarmar** del teclado después de introducir un código de acceso o utilizar un dispositivo de acceso.

Códigos de acceso del teclado

Para configurar el código del teclado y el código de coacción del teclado:

1. En la app Ajax, vaya a la pestaña **Dispositivos** .
2. Seleccione el teclado para el que desea configurar un código de acceso.
3. Vaya a su **Configuración** .
4. En el menú de **Opciones de acceso**, seleccione la opción de **Solo códigos del teclado** o **Códigos del teclado y de usuario**.
5. Vaya al menú **Código del teclado**.
6. Establezca el código del teclado. Contiene de 4 a 6 dígitos.
7. Pulse **Hecho**.
8. Vaya al menú **Código de coacción**.
9. Establezca el código de coacción del teclado. Contiene de 4 a 6 dígitos.
10. Pulse **Hecho**.

Códigos de acceso de los usuarios

Para establecer un código personal y un código personal de coacción:

1. Seleccione el espacio en la app Ajax.
2. Vaya al menú **Configuración** .
3. Abra el menú **Usuarios**.
4. Busque su cuenta en la lista y pulse sobre ella.
5. Vaya al menú de **Configuración códigos de acceso**.
6. Establezca el **Código de usuario**. Contiene de 4 a 6 dígitos.
7. Pulse **Guardar**.
8. Establezca el **Código de coacción**. Contiene de 4 a 6 dígitos.
9. Pulse **Guardar**.
10. Pulse **Atrás** para guardar la configuración.

Códigos de usuarios no registrados

Para establecer un código de acceso para un usuario sin cuenta:

1. Seleccione el hub en la app Ajax.
2. Vaya al menú **Configuración** .
3. Vaya al menú **Códigos de acceso del teclado**.

4. Pulse **Añadir código**. Establezca el **Nombre** y el **Código de acceso**. Contiene de 4 a 6 dígitos.
5. Pulse **Añadir** para guardar los datos.

Para establecer un código de coacción para un usuario sin cuenta:

1. Seleccione el menú **Códigos de acceso del teclado** en la configuración del hub.
2. Seleccione el usuario no registrado necesario.
3. Pulse **Añadir código de coacción**. Establezca el código. Contiene de 4 a 6 dígitos.
4. Pulse **Hecho**.

Para los usuarios no registrados, un administrador o un PRO con permisos para configurar el sistema puede ajustar el acceso a la gestión de la seguridad. Primero, active el Modo Grupo. Luego, seleccione el menú **Códigos de acceso del teclado** en la configuración del hub, busque el usuario necesario y configure los parámetros correspondientes en el menú **Gestión de la seguridad**.

Código URR

Solo un PRO con permisos para configurar el sistema puede crear y configurar los códigos URR en las apps Ajax PRO. Encontrará más información sobre la configuración de esta función en este artículo.

Tarjetas y mandos

El Superior KeyPad Plus G3 Jeweller puede funcionar con mandos Tag, tarjetas Pass y dispositivos de terceros que admitan la tecnología DESFire®.

Antes de añadir dispositivos de terceros que soporten DESFire®, asegúrese de que tienen suficiente memoria libre para gestionar el nuevo teclado. A ser posible, el dispositivo de terceros debe estar preformateado.

En este artículo encontrará información sobre cómo restablecer **Tag** o **Pass**.

El número máximo de dispositivos Pass y Tag añadidos depende del modelo del hub. Los dispositivos Pass y Tag añadidos no afectan al límite total de dispositivos del hub.

Comprobar la compatibilidad de los dispositivos

Añadir Tag o Pass

1. Abra la app Ajax.
2. Seleccione el espacio con hub al que desea añadir Tag o Pass.
3. Vaya a la pestaña **Dispositivos** .

> Asegúrese de que la función de **Lectura de pass/tag** esté habilitada en la configuración de al menos un teclado.

4. Pulse **Añadir dispositivo**.
5. Seleccione **Añadir pass/tag**.
6. Especifique el tipo (Tag o Pass), el color, el nombre del dispositivo y el usuario (si es necesario).
7. Pulse **Siguiente**. Después de eso, el hub cambiará al modo de registro de dispositivos.
8. Acérquese a cualquier teclado compatible con la función de **Lectura de pass/tag** habilitada. Pulse el botón **Desarmar** para cambiar el teclado al modo de registro de dispositivos de acceso.
9. Acerque el Pass o el Tag con el lado ancho hacia el teclado durante unos segundos. Si la adición se realiza correctamente, recibirá una notificación en la app Ajax.

Si la conexión falla, inténtelo de nuevo en 5 segundos. Tenga en cuenta que si ya ha añadido al hub el número máximo de dispositivos Tag o Pass, recibirá la notificación correspondiente en la app Ajax al añadir un nuevo dispositivo.

> Tanto el Tag como el Pass pueden funcionar con varios hubs al mismo tiempo. El número máximo de hubs es de 13. Si ya ha añadido a un hub el número máximo de

dispositivos, recibirá la notificación correspondiente al intentar añadir otro Tag o Pass. Para añadir dicho mando/tarjeta a un nuevo hub, deberá restablecerlos.

Si necesita añadir otro Tag o Pass, pulse **Añadir otro pass/tag** en la app. Repita los pasos 6–9.

Eliminar (restablecer) Tag o Pass

⚠ El restablecimiento borrará todos los ajustes y conexiones de mandos y tarjetas. En este caso, el Tag y el Pass restablecidos solo se eliminan del hub desde el que se ha realizado el restablecimiento. En otros hubs, el Tag o el Pass siguen apareciendo en la app, pero no se pueden utilizar para gestionar los modos de seguridad. Estos dispositivos deben eliminarse manualmente.

1. Abra la app Ajax.
2. Seleccione el espacio.
3. Vaya a la pestaña **Dispositivos** .
4. Seleccione un teclado compatible de la lista de dispositivos.

ⓘ Asegúrese de que la función de **Lectura de pass/tag** esté habilitada en la configuración del teclado.

5. Vaya a la configuración del teclado pulsando el icono .
6. Pulse **Restablecer pass/tag**.
7. Pulse **Continuar**.
8. Acérquese a cualquier teclado compatible con la función de **Lectura de pass/tag** habilitada. Pulse el botón **Desarmar** para cambiar el teclado al modo de restablecimiento de dispositivos de acceso.
9. Acerque el Pass o el Tag con el lado ancho hacia el teclado durante unos segundos. Si el formateo se realiza correctamente, recibirá una notificación (app Ajax. Si el formateo falla, inténtelo de nuevo.

Si necesita restablecer otro Tag o Pass, pulse **Restablecer otro pass/tag** en la app. Repita el paso 9.

Control de la seguridad

Mediante códigos, Tag o Pass, puede controlar el **Modo Noche** y la seguridad de todo el sitio o de grupos separados. Un usuario o un PRO con permisos para configurar el sistema puede establecer códigos de acceso. En esta sección encontrará más información sobre cómo añadir un Tag o un Pass al hub.

Si se utiliza un código personal o de acceso, un Tag o un Pass, el nombre del usuario que ha cambiado el modo de seguridad se muestra en el historial de eventos del hub y en la lista de notificaciones. Si se utiliza un código común, se muestra el nombre del teclado desde el que se ha cambiado el modo de seguridad.

> El Superior KeyPad Plus G3 Jeweller se bloquea durante el tiempo establecido en los ajustes si se introduce un código incorrecto o se acerca un dispositivo de acceso no verificado tres veces seguidas en el plazo de 1 minuto. Las notificaciones correspondientes se envían a los usuarios y a la central receptora de alarmas. Un usuario o un PRO con permisos para configurar el sistema puede desbloquear el Superior KeyPad Plus G3 Jeweller en la app Ajax.

La secuencia de pasos para cambiar el modo de seguridad con el teclado depende de si las opciones **Armar sin código**, **Confirmación de autorización con código de acceso** y **Cambio fácil del modo armado** están habilitadas en los ajustes del Superior KeyPad Plus G3 Jeweller.

Utilizando Tag o Pass

1. Active el teclado acercando la mano frente a él.
2. Acerque el Tag o el Pass al lector de tarjetas/mandos del teclado.
3. Introduzca el código necesario si la función de **Confirmación de autorización código de acceso** está habilitada.
4. Pulse el botón **Armar**, **Desarmar** o **Modo Noche** del teclado.

Si la opción de **Cambio fácil del modo armado** está habilitada, no es necesario pulsar el botón **Armar**, **Desarmar** o **Modo Noche** después de leer el dispositivo de acceso.

Utilizando códigos de acceso

Los códigos introducidos incorrectamente pueden borrarse pulsando el botón **Restablecer**.

Código	Ejemplo	Nota
Gestión de los modos de armado del sitio		
Código del teclado Código de coacción del teclado	1234 → ◯ / ◯ / ◎	
Código de usuario Código de coacción del usuario	5 → → 1234 → ◯ / ◯ / ◎	**5** es el ID de usuario
Código de usuario no registrado Código de coacción de usuario no registrado	1234 → ◯ / ◯ / ◎	
Código URR	1234 → ◯ / ◯ / ◎	
Gestión de los modos de armado del grupo		
Código del teclado Código de coacción del teclado	1234 → → 2 → ◯ / ◎	**2** es el ID del grupo
Código de usuario Código de coacción del usuario	5 → → 1234 → → 2 → ◯ / ◎	**5** es el ID de usuario **2** es el ID del grupo
Código de usuario no registrado Código de coacción de usuario no registrado	1234 → → 2 → ◯ / ◎	**2** es el ID del grupo
Código URR	1234 → → 2 → ◯ / ◎	**2 es el ID del grupo**

Más información sobre el ID de usuario

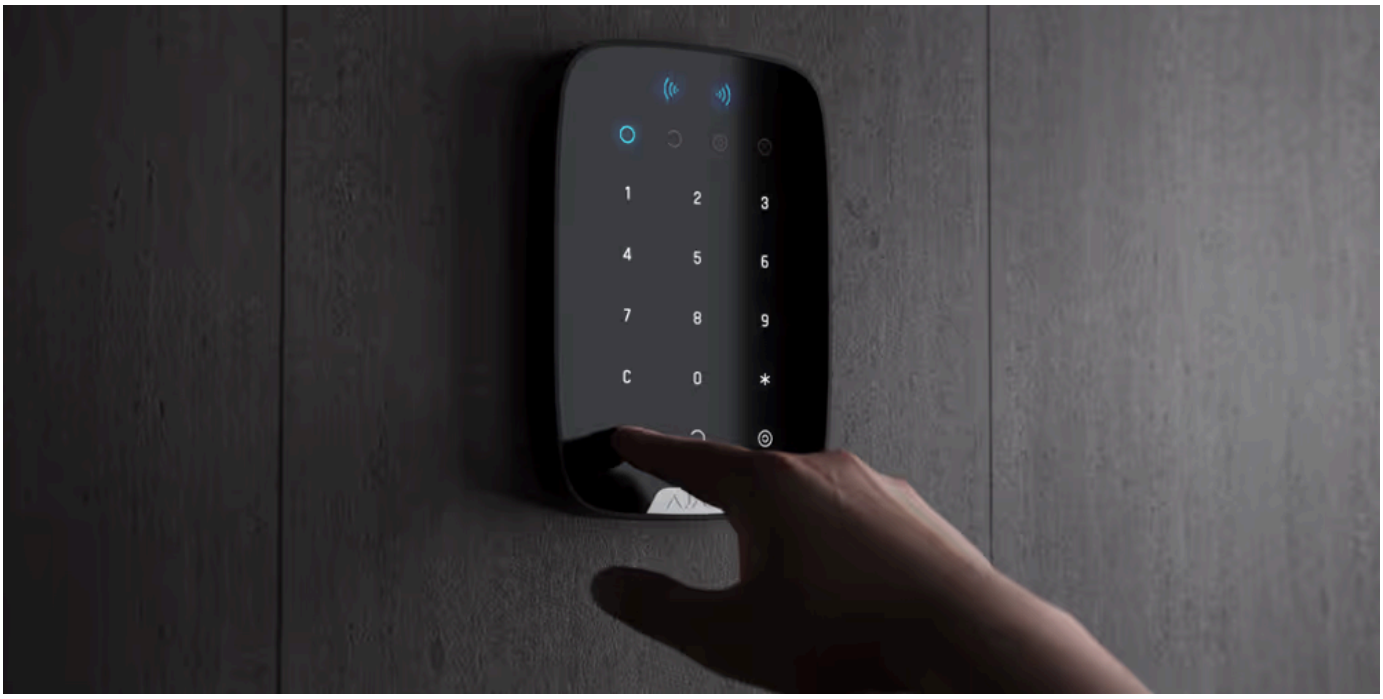
Más información sobre el ID de grupo

Confirmación de autorización con código de acceso

La **Confirmación de autorización con código de acceso** es una función que permite configurar la autenticación de dos factores para los usuarios cuando controlan los modos de seguridad del sistema. Esta definición significa que los usuarios deben utilizar primero un dispositivo de acceso (Pass o Tag) y después introducir un código de acceso para confirmar su autorización al sistema.

Más información sobre la Confirmación de autorización con un código de acceso

Indicación



El Superior KeyPad Plus G3 Jeweller puede informar del modo de seguridad actual, las pulsaciones de botones, los fallos de funcionamiento y el estado mediante indicación LED y sonido. La retroiluminación muestra el modo de seguridad actual después de activar el teclado. La información sobre el modo de seguridad actual es relevant incluso si el modo de armado es cambiado por otro dispositivo: un mando, otro teclado o una app.

Puede activar el teclado deslizando la mano por el panel táctil de arriba a abajo. Cuando se activa, la retroiluminación del teclado se encenderá y sonará un pitido (si está activado).

Evento	Indicación	Nota
Encendido del dispositivo	Todos los indicadores y la retroiluminación del teclado numérico se encienden brevemente. Luego, suena un pitido de tres tonos y se encienden el LED de modo de seguridad del sistema actual y la retroiluminación del teclado numérico. Después de eso, la retroiluminación del teclado numérico se apaga suavemente y suena un doble pitido	
Encendido del dispositivo que no se ha añadido al hub	Todos los indicadores y la retroiluminación del teclado numérico se encienden brevemente. Después de eso, el LED X parpadea 6 veces y luego parpadea 3 veces rápidamente	El teclado se apaga al finalizar la indicación
Apagado del dispositivo	El LED X se enciende durante cerca de 1 seg y luego parpadea 3 veces	El sistema envía una notificación cuando se apaga el teclado mediante el botón de encendido
El dispositivo se ha eliminado del hub	El LED X parpadea 6 veces y luego parpadea 3 veces rápidamente	El teclado se apaga al finalizar la indicación
Se ha perdido la conexión con el hub o el repetidor de señal de radio	El LED X parpadea	
La tapa del dispositivo está abierta (el panel SmartBracket está retirado)	El LED X parpadea brevemente una vez	
Pulsación del botón táctil	Pitido corto, el LED de estado de seguridad del sistema parpadea una vez	El volumen depende de la configuración del teclado
Sistema armado	Pitido corto, se enciende el LED **Armado** o de **Modo Noche**	
Sistema desarmado	Dos pitidos cortos, se enciende el LED **Desarmado**	
Se ha introducido un código incorrecto o se ha intentado cambiar el modo de seguridad	Pitido largo, la retroiluminación del teclado numérico parpadea 3 veces	

mediante una tarjeta/mando desconectado o desactivado		
No se ha podido activar el modo de seguridad (**Comprobación de integridad del sistema** fallida)	Pitido largo, el LED de estado de seguridad actual parpadea 3 veces	
El sistema requiere confirmar la autorización con una contraseña después de la confirmación del dispositivo de acceso. Disponible si está habilitada la función de Confirmación de autorización con código de acceso	El LED de estado de seguridad actual parpadea durante el tiempo establecido para la confirmación	
El teclado se ha bloqueado debido a un intento de introducción de código incorrecto o a un intento de utilizar una tarjeta/mando no autorizado	Pitido largo, durante el cual los LED de estado de seguridad y la retroiluminación del teclado parpadean 3 veces	
El hub no responde	Pitido largo, el LED X se enciende	
La carga de la batería es baja	Después de cambiar el modo de seguridad, se enciende el LED X. Los botones táctiles están bloqueados durante este tiempo. Al intentar activar el teclado con las baterías descargadas, emite un pitido largo, el LED X se enciende y se apaga suavemente, y luego el teclado se apaga.	Cómo sustituir las baterías

Notificaciones sonoras de fallos de funcionamiento

El Superior KeyPad Plus G3 Jeweller puede notificar a los usuarios del sistema con un sonido audible si algún dispositivo está sin conexión o la batería está baja. El LED X del teclado parpadeará. Las notificaciones de fallos de funcionamiento se mostrarán en el historial de eventos, el texto de SMS o las notificaciones push.

Para activar las notificaciones sonoras de fallos de funcionamiento, en una app Ajax PRO:

1. Vaya a la pestaña **Dispositivos** .
2. Seleccione el hub y vaya a su configuración .
3. Vaya a **Servicio** → **Sonidos y alertas**.

4. Habilite las opciones: **Si algún dispositivo tiene batería baja** y **Si algún dispositivo está sin conexión**.
5. Pulse **Atrás** para guardar la configuración.

Evento	Indicación	Nota
Si algún dispositivo está sin conexión	Dos señales sonoras cortas, el LED X parpadea dos veces. Emite un pitido por minuto hasta que todos los dispositivos del sistema estén en línea.	Los usuarios pueden retrasar la indicación sonora durante 12 horas
Si el Superior KeyPad Plus G3 Jeweller está sin conexión	Dos señales sonoras cortas, el LED X parpadea dos veces. Emite un pitido por minuto hasta que el teclado del sistema esté en línea.	Es imposible retrasar la indicación sonora
Si algún dispositivo tiene batería baja	Tres señales sonoras cortas, el LED X parpadea tres veces. Emite un pitido por minuto hasta que se restablece la batería o se retira el dispositivo.	Los usuarios pueden retrasar la indicación sonora durante 4 horas

Las notificaciones sonoras de fallos de funcionamiento aparecen cuando finaliza la indicación del teclado. Si se producen varios fallos de funcionamiento en el sistema, el teclado notificará primero la pérdida de conexión entre el dispositivo y el hub.

Fallos de funcionamiento

Cuando el dispositivo detecta un fallo de funcionamiento (por ejemplo, se ha perdido la conexión a través del protocolo Jeweller), se muestra un contador de fallos de funcionamiento en la app Ajax, en la esquina superior izquierda del icono del dispositivo.

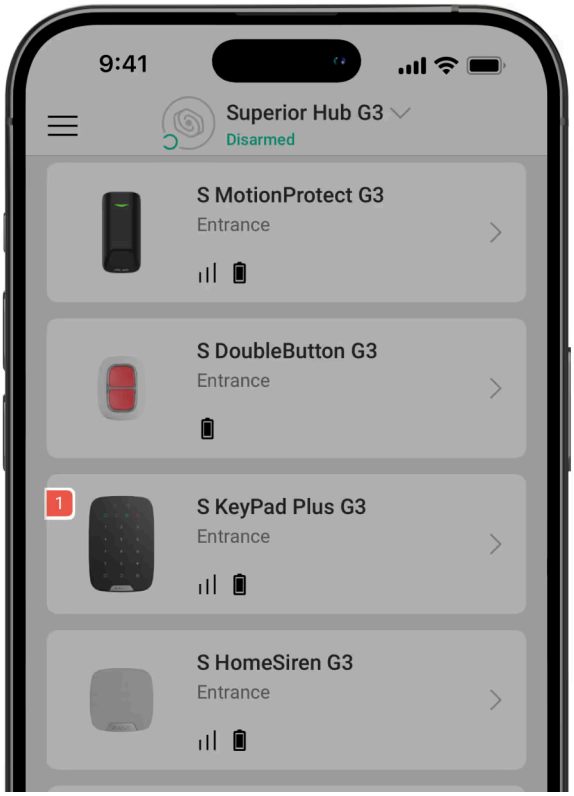
Todos los fallos de funcionamiento pueden verse en los estados del dispositivo. Los campos con fallos de funcionamiento se resaltarán en rojo.

Se muestra un fallo de funcionamiento si ocurre lo siguiente:

- La temperatura del dispositivo está fuera de los límites permisibles.
- La tapa del dispositivo está abierta (alarma antisabotaje activada).

- Se ha perdido la conexión con el hub o el repetidor de señal de radio vía Jeweller.
- La batería del dispositivo está baja.

Mantenimiento



Compruebe regularmente el funcionamiento del dispositivo. La frecuencia óptima de las comprobaciones es de una vez cada tres meses. Limpie la carcasa del dispositivo de polvo, telarañas y otros contaminantes a medida que vayan apareciendo. Utilice toallitas suaves y secas adecuadas para el mantenimiento del equipamiento.

No utilice sustancias que contengan alcohol, acetona, gasolina y otros disolventes activos para limpiar el dispositivo.

Si la batería del teclado está baja, el sistema envía las notificaciones correspondientes, y el indicador X **Fallo de funcionamiento** se enciende suavemente y se apaga después de cada introducción correcta del código.

El Superior KeyPad Plus G3 Jeweller puede funcionar hasta 2 meses después de la señal de batería baja. No obstante, le recomendamos que sustituya las baterías

inmediatamente después de recibir la notificación. Se recomienda utilizar baterías de litio. Tienen una gran capacidad y se ven menos afectadas por las temperaturas.

Cómo sustituir las baterías del Superior KeyPad Plus G3 Jeweller

Especificaciones técnicas

Todas las especificaciones técnicas

Cumplimiento de normas

Configuración conforme a los requisitos EN 50131

Garantía

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

Si el dispositivo no funciona correctamente, le recomendamos que contacte primero con el servicio de asistencia, ya que la mayoría de los problemas técnicos pueden resolverse en remoto.

Obligaciones de la garantía

Contrato de usuario

Póngase en contacto con el soporte técnico:

- correo
- Telegram

Fabricado por «AS Manufacturing» LLC



¿Necesita ayuda?

Descubra todo el potencial de un sistema Ajax gracias a nuestros manuales detallados, artículos, herramientas y preguntas frecuentes. Si necesita ayuda inmediata, nuestro chatbot con IA y nuestro equipo de asistencia técnica profesional están a su disposición 24/7.

Hacer una pregunta

Suscribirse

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

Suscribirse

Solicitar ayuda adicional

support@ajax.systems
@AjaxSystemsSupport_Bot
Hacer una pregunta

Trustpilot
Valoración 4.8

4.500.000
personas en todo el mundo bajo la protección de Ajax

Sugerir una función

Productos

- Protección contra intrusiones
- Videovigilancia
- Protección contra incendios
- Confort y automatización
- Todos los productos
- Servicios
- Integraciones con el sistema
- Productos Ajax Ready
- Protocolo cableado Fibra
- Protocolos de radio Ajax

Software

- Ajax Security System
- Ajax PRO: Tool for Engineers
- Ajax Desktop
- Ajax PRO Desktop
- Ajax TV
- Ajax Translator PRO
- Ajax Cloud Signaling
- Ajax Media Player
- Escenarios

Disponible en App Store

Disponible en Google Play

Soluciones

- Historias de clientes
- Soluciones por tipo de instalación
- Sistema comercial de detección y alarma de incendios
- Solución inalámbrica de Grade 3
- Solución de videovigilancia
- La integración con las cerraduras inteligentes Yale

Asistencia

- Guías y artículos
- Cumplimiento de normas

Herramientas

- Compatibilidad de dispositivos Ajax
- Compatibilidad con el software de monitorización

Modernización y renovación
Por qué Ajax
Cómo funciona Ajax

Disponibilidad de los Servicios Ajax
Calculadora de almacenamiento de vídeo
Calculadora de dispositivos de vídeo
Calculadora de duración de la batería
Calculadora de alcance de comunicación por radio
Configurador de interruptores y enchufes
Calculadora de alimentación Fibra
Todas las herramientas web

Soluciones de monitorización e integraciones

Monitorización de alarmas de intrusión
Videovigilancia y verificación visual de alarmas
Audioverificación de alarmas

Compañía

Blog
Acerca de nosotros
Página de prensa
Eventos
Empleo
Ajax Next
Reseñas y feedback

Para los partners

Para los partners
Ajax Academy
Partner Portal
Canal de Ajax PRO

España Política de privacidad Informar de una vulnerabilidad Libro blanco del RGPD Declaración NDAA
Política de Cookies Política contra el correo no deseado Ajax Services T&C Contrato de usuario final Garantía

© 2026 AJAX SYSTEMS CH. All rights reserved