

Manual do utilizador de Superior KeyPad Plus G3 Jeweller

Atualizado 24 de março de 2026



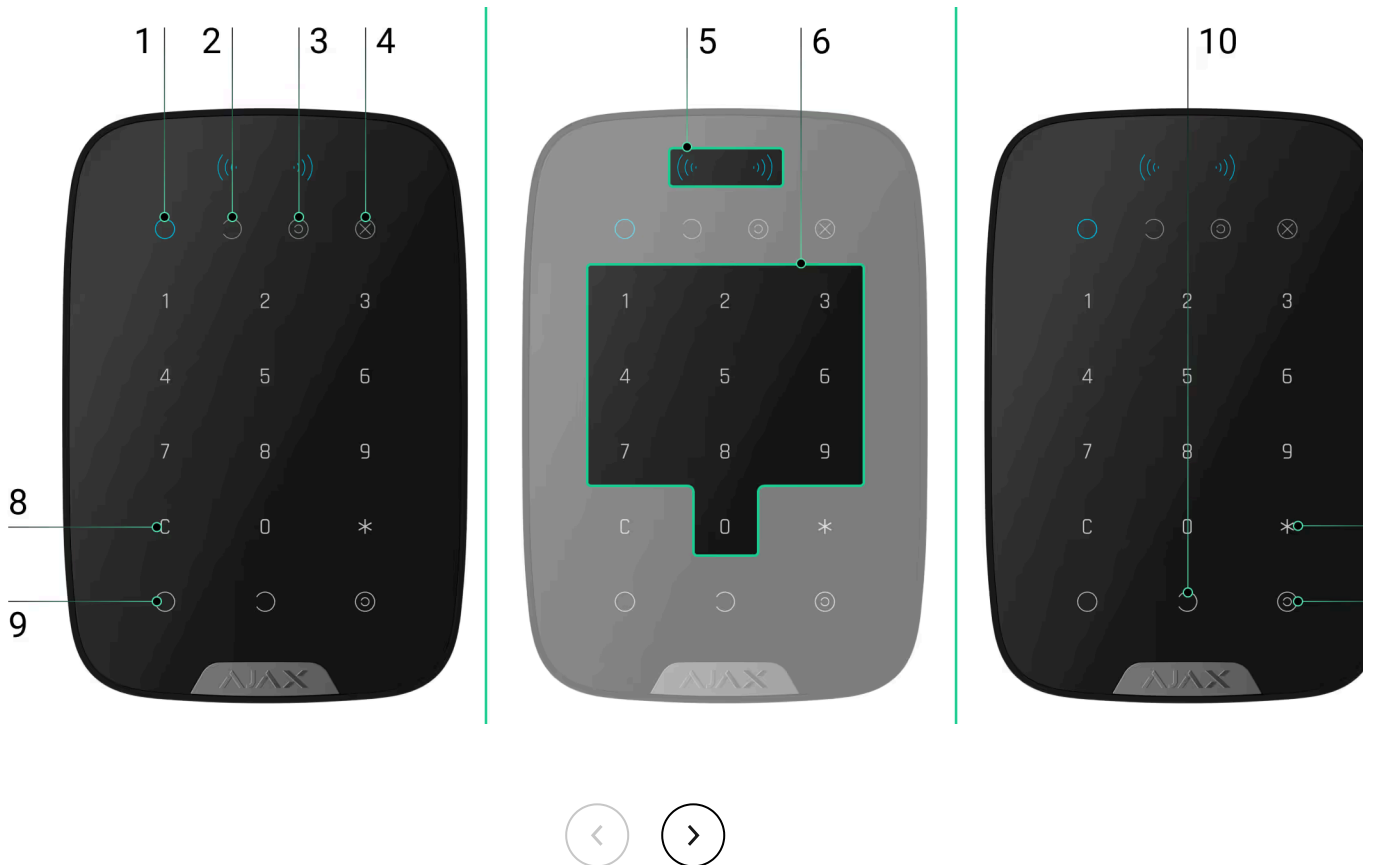
Superior KeyPad Plus G3 Jeweller é um teclado sem fios concebido para gerir sistemas Ajax. Os utilizadores podem autenticar-se utilizando comandos Tag, cartões Pass e códigos. O dispositivo destina-se apenas a utilização em interiores.




O teclado funciona num sistema Ajax e troca dados com o hub utilizando o protocolo seguro de comunicação por rádio Jeweller.

Superior KeyPad Plus G3 Jeweller é um dispositivo da linha de produtos Superior. Apenas os parceiros acreditados de Ajax Systems podem vender, instalar e manter os produtos Superior.

› [Comprar Superior KeyPad Plus G3 Jeweller](#)

Elementos funcionais



1. Indicador **Armado**.
2. Indicador **Desarmado**.
3. Indicador **Modo noturno**.
4. Indicador **Avaria**.
5. Leitor de Pass/Tag.
6. Bloco de botões numéricos.
7. Botão de **Função**.
8. Botão de **Reposição**.
9.  Botão **Armar**.
10.  Botão **Desarmar**.
11.  Botão Modo noturno.
12. Painel de instalação SmartBracket. Para retirar o painel, desaparafuse o parafuso de fixação e deslize o painel para baixo.
13. Parte perfurada do painel de instalação. É necessário que o botão de tamper anti-sabotagem seja acionado em caso de tentativa de retirar o dispositivo da superfície. Não partir.
14. Botão de tamper anti-sabotagem.
15. Botão de alimentação.
16. Código QR com o ID do dispositivo. É utilizado para adicionar o detetor ao hub.

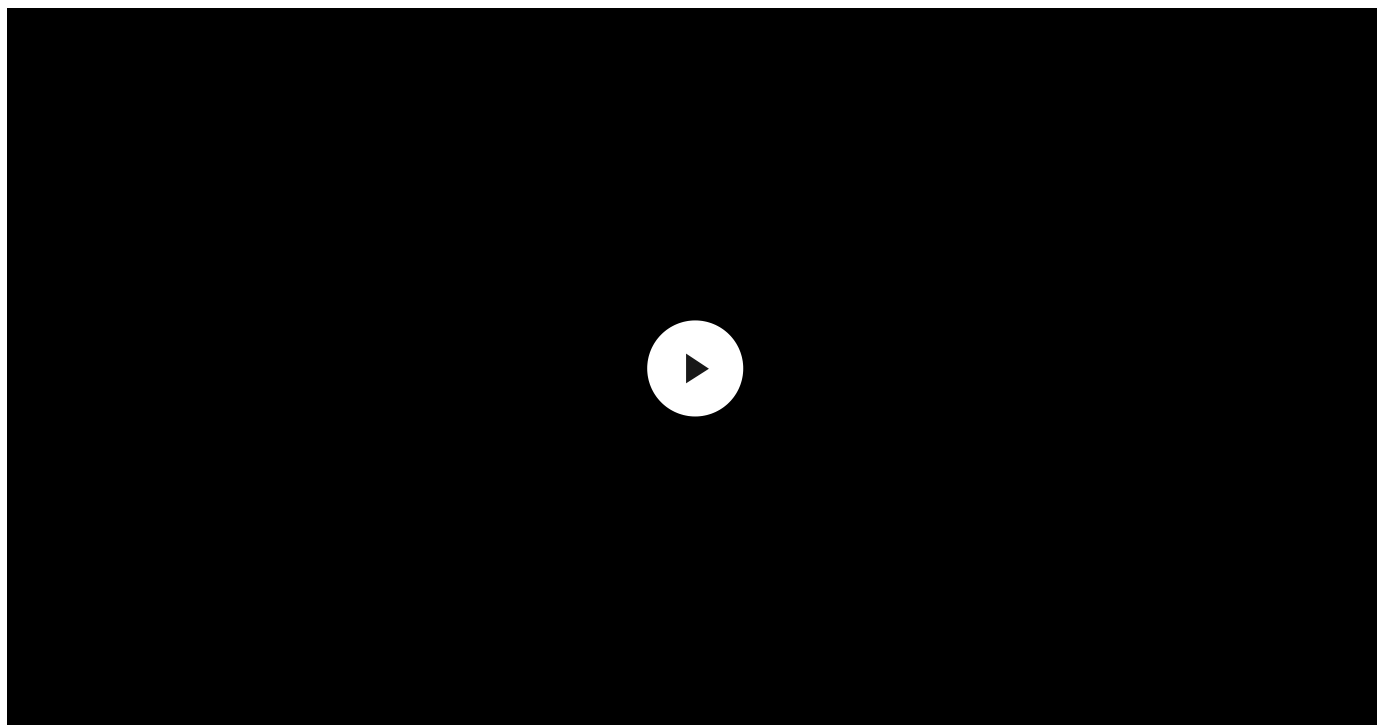
17. Parafuso de fixação para segurar o teclado no SmartBracket.

Hubs compatíveis

Para que o teclado funcione, é necessário um hub Ajax com OS Malevich 2.35 e superior.

Verifique a compatibilidade do dispositivo

Princípio do funcionamento



Superior KeyPad Plus G3 Jeweller possui grandes botões táteis, um leitor para autorização sem contacto e indicadores LED. O teclado é utilizado para controlar os modos de segurança, enviar um alarme de pânico ou silenciar o alarme de incêndio.

Superior KeyPad Plus G3 Jeweller possui indicadores LED que mostram o modo de segurança atual e as avarias do teclado (se houver). O estado de segurança só é apresentado quando o teclado está ativo (a retroiluminação do dispositivo está ligada).



Superior KeyPad Plus G3 Jeweller pode ser utilizado em condições de pouca luz, uma vez que possui retroiluminação. A pressão dos botões é acompanhada por um sinal sonoro. O brilho da retroiluminação e o volume do teclado podem ser ajustados nas definições. Se o teclado não for utilizado durante 4 segundos, Superior KeyPad Plus G3 Jeweller reduz o brilho da luz de retroiluminação. Após 8 segundos de inatividade, entra em modo de poupança de energia e desliga o ecrã.

i Se a carga das pilhas estiver baixa, a retroiluminação liga-se no nível mínimo, independentemente das definições.

Controlo de segurança

Superior KeyPad Plus G3 Jeweller pode armar e desarmar todo o local ou grupos específicos e ativar **Modo noturno**. Os utilizadores podem controlar a segurança através de Superior KeyPad Plus G3 Jeweller:

1. **Cartões ou comandos.** Para identificar os utilizadores de forma rápida e segura, Superior KeyPad Plus G3 Jeweller utiliza a tecnologia DESFire®. DESFire® baseia-se na norma internacional ISO 14443 e combina encriptação de 128 bits e proteção contra cópia. Tag e Pass suportam esta tecnologia e são compatíveis com Superior KeyPad Plus G3 Jeweller.

2. **Códigos.** Superior KeyPad Plus G3 Jeweller suporta códigos gerais, códigos pessoais e códigos para utilizadores não registados.

Códigos de acesso

- **Código do teclado** é um código geral configurado para o teclado. Quando utilizado, todos os eventos são enviados para apps Ajax em nome do teclado.
- **Código de utilizador** é um código pessoal configurado para os utilizadores conectados ao hub. Quando utilizado, todos os eventos são enviados para apps Ajax em nome do utilizador.
- **Código de acesso do teclado** é um código configurado para uma pessoa que não está registada no sistema. Quando utilizado, os eventos são enviados para apps Ajax com um nome associado a este código.
- **Código URR** é um código de acesso às unidades de resposta rápida (URR) ativadas após o alarme e válido por um período determinado. Quando o código é ativado e utilizado, os eventos são entregues às apps Ajax com um título associado a este código.



O número de códigos pessoais, códigos de acesso ao teclado e códigos URR depende do modelo do hub.

[Verifique a compatibilidade do dispositivo](#)

Os direitos de acesso e os códigos podem ser ajustados nas apps Ajax. Se o código for comprometido, pode ser alterado remotamente, por isso não é necessário chamar um instalador ao local. Se um utilizador perder o seu Pass ou Tag, um administrador ou um PRO com direitos de configuração do sistema pode bloquear o dispositivo instantaneamente na app. Entretanto, um utilizador pode utilizar um código pessoal para controlar o sistema.


Controlo de segurança dos grupos

Superior KeyPad Plus G3 Jeweller permite controlar a segurança dos grupos (se Modo de grupo estiver ativado). Um administrador ou PRO com direitos para configurar o sistema também pode ajustar as definições do teclado para determinar

que grupos serão partilhados (grupos de teclados). Pode saber mais sobre a gestão da segurança do grupo [nesta secção](#).

Botão de Função

Superior KeyPad Plus G3 Jeweller possui o botão de **Função** funciona num dos três modos:

- **Desligado** – o botão de **Função** está desativado e nada acontece quando o utilizador o premir.
- **Pânico** – depois de premido o botão de **Função**, o sistema envia um alarme para a estação de monitorização da empresa de segurança e para todos os utilizadores.
- **Silenciar alarme de incêndio** – depois de premido o botão de **Função**, o sistema silencia o alarme dos detetores de incêndio Ajax. Disponível apenas se a funcionalidade [Alarme de detetores de incêndio interligados](#) estiver ativada (Hub → Definições  → Serviço → Definições dos detetores de incêndio).

Código de coação

Superior KeyPad Plus G3 Jeweller suporta um **código de coação** que permite a um utilizador simular a desativação do alarme. Neste caso, nem a [app Ajax](#) nem as [sirenes](#) instaladas no estabelecimento revelarão as suas ações. Ainda assim, a empresa de segurança e outros utilizadores do sistema de segurança serão alertados para o incidente.

[Saiba mais](#)

Bloqueio automático de acesso não autorizado

Se um código incorreto for introduzido ou um dispositivo de acesso não verificado for utilizado três vezes consecutivas num intervalo de 1 minuto, o teclado será bloqueado durante o tempo especificado nas respetivas [definições](#). Durante este tempo, o hardware ignorará todos os códigos e dispositivos de acesso, informando os utilizadores do sistema de segurança sobre a tentativa de acesso não autorizado.

Um PRO ou um utilizador com direitos de configuração do sistema pode desbloquear o teclado através da app antes de expirar o tempo de bloqueio especificado.

Armar em duas fases

Superior KeyPad Plus G3 Jeweller pode participar no armamento em duas fases, mas não pode ser utilizado como dispositivo de segunda fase. O processo de armar em duas fases utilizando Tag ou Pass é semelhante à utilização de um código pessoal ou geral no teclado.

[Saiba mais](#)

Silenciar o alarme de incêndio

Superior KeyPad Plus G3 Jeweller pode silenciar um alarme de incêndio interligado premindo o botão **Função** (se a definição necessária estiver ativada). A reação do sistema ao premir o botão depende das definições e do estado do sistema:

- **Alarmes dos detetores de incêndio interligados já se propagaram** — ao premir o botão pela primeira vez, todas as sirenes dos detetores de incêndio são silenciadas, exceto as que registaram o alarme. Premir novamente o botão silencia os restantes detetores.
- **O tempo de atraso dos alarmes interligados dura** — ao premir o botão de **Função**, a sirene dos detetores de incêndio Ajax acionados é silenciada.

Tenha em atenção que a opção só está disponível se a funcionalidade **Alarme de detetores de incêndio interligados** estiver ativada.

[Saiba mais](#)

Protocolo de transferência de dados Superior Jeweller

Superior Jeweller é um protocolo de rádio atualizado para os dispositivos Superior que garante a conformidade com a norma **Grade 3** (EN 50131). Possui a **criptação** avançada e **salto de frequência**. O salto de frequência completo está disponível apenas quando todos os dispositivos do sistema utilizam Superior Jeweller. Se pelo

menos um dispositivo funcionar com o protocolo Jeweller normal, o sistema ficará limitado a **Grade 2**: a encriptação permanece, mas o salto está desativado. Os dispositivos Superior também podem funcionar com o protocolo Jeweller normal, consoante o hub.

[Saiba mais](#)

Comunicação encriptada avançada

A comunicação entre Superior KeyPad Plus G3 Jeweller e o hub é protegida por um esquema de encriptação avançado que garante a confidencialidade e a integridade dos dados. Isto significa que todos os dados sensíveis da mensagem são encriptados e que cada mensagem inclui um código de autenticação que permite ao sistema verificar se os dados não foram alterados durante a transmissão. O sistema consegue detetar de forma fiável a tentativa de sabotagem e rejeitar mensagens falsificadas ou alteradas, garantindo uma proteção robusta contra ataques passivos e ativos. Isto garante uma comunicação segura entre o dispositivo e o hub, bem como uma proteção fiável do sistema e dos dados.

[Saiba mais sobre comunicação encriptada avançada](#)

Salto de frequência

Para cumprir os requisitos de Grade 3, Superior KeyPad Plus G3 Jeweller utiliza **salto de frequência** para a comunicação rádio com o hub (ou o repetidor de sinal de rádio). Com este método, o hub e os dispositivos adicionados a este alteram a sua frequência de funcionamento de acordo com um padrão definido. A sequência de saltos abrange um conjunto definido de canais dentro das bandas de operação, e os dispositivos mudam de frequência em sincronia com o hub. Mesmo que alguns canais sejam afetados por inibição, as mensagens podem ser transmitidas com sucesso através de outros canais. O salto de frequência melhora a fiabilidade e o desempenho do sistema e garante a sua resistência a interferências intencionais e a tentativas de inibição.

O salto de frequência não causa atrasos ou pausas durante a comunicação rádio nem reduz a velocidade de transferência de dados. Se [repetidores](#) forem adicionados ao

sistema, o salto de frequência é utilizado para todas as comunicações rádio: «dispositivo ↔ repetidor» e «repetidor ↔ hub».



O sistema utiliza salto de frequência para a comunicação rádio apenas se todos os dispositivos sem fios suportarem este método.

Se pelo menos um dispositivo adicionado ao sistema não suportar o salto de frequência, o hub e todos os dispositivos mudarão para as frequências de funcionamento desse dispositivo e não utilizarão o salto de frequência para a comunicação rádio.

[Saiba mais sobre salto de frequência](#)

[Saiba mais sobre inibição](#)

Envio de eventos para a central de monitorização

O sistema Ajax pode transmitir alarmes para a app de monitorização [Ajax PRO Desktop](#), bem como para a central recetora de alarmes (CRA), nos formatos **SurGard** (Contact ID), SIA (DC-09), ADEMCO 685 e [outros protocolos](#).

Superior KeyPad Plus G3 Jeweller pode transmitir os seguintes eventos:

1. Armar/desarmar o sistema.
2. Introdução do código de coação.
3. Pressão no botão de pânico.
4. Teclado bloqueado devido a tentativa de acesso não autorizado.
5. Tentativa sem êxito de armar o sistema de segurança (com a [verificação da integridade do sistema](#) ativada).
6. Alarme de tamper. Recuperação do botão de tamper.
7. Perda e restabelecimento da ligação ao hub.
8. Desativação/ativação permanente do dispositivo.
9. Desativação/ativação única do dispositivo.

Quando o alarme é recebido, o operador da estação de monitorização da empresa de segurança sabe o que aconteceu e sabe exatamente para onde enviar uma unidade de resposta rápida. O endereçamento dos dispositivos Ajax permite enviar eventos

para Ajax PRO Desktop ou para a CRA, incluindo o tipo de dispositivo, o seu nome, o grupo de segurança e a divisão virtual. A lista de parâmetros transmitidos pode variar consoante o tipo de CRA e o protocolo de comunicação selecionado.



Pode encontrar o ID do dispositivo e o número do bucle (zona) nos estados do dispositivo.

Seleção do local de instalação



Ao escolher o local onde colocar Superior KeyPad Plus G3 Jeweller, tenha em consideração os parâmetros que afetam o seu funcionamento:

- Intensidade do sinal Jeweller

Considere as recomendações de colocação ao desenvolver um projeto para o sistema de segurança da instalação. O sistema Ajax deve ser concebido e instalado por especialistas. Uma lista de parceiros recomendados está disponível aqui.

Superior KeyPad Plus G3 Jeweller deve ser colocado no interior, perto da entrada. Isto permite aos utilizadores desarmar o local antes de entrarem nas instalações ou até



que os atrasos de entrada expirem. Os utilizadores podem também armar rapidamente o local quando saem das instalações.

A altura de instalação recomendada é de 1,3–1,5 metros acima do chão. Instale o teclado numa superfície plana e vertical. Isto assegura que Superior KeyPad Plus G3 Jeweller está bem fixo à superfície e ajuda a evitar falsos alarmes de tamper anti-sabotagem.



Ao segurar Superior KeyPad Plus G3 Jeweller nas suas mãos ou ao utilizá-lo numa mesa, não podemos garantir que os botões táteis funcionem corretamente.

Intensidade do sinal

A intensidade do sinal é determinada pelo número de pacotes de dados não entregues ou corrompidos durante um determinado período de tempo. O ícone  no separador **Dispositivos**  nas apps Ajax indica a intensidade do sinal:

- **três barras** – excelente intensidade de sinal;
- **duas barras** – boa intensidade de sinal;
- **uma barra** – fraca intensidade de sinal, não é garantido um funcionamento estável;
- **ícone riscado** – sem sinal.



Verifique a intensidade do sinal do Jeweller antes da instalação definitiva. Com uma intensidade de sinal de uma ou zero barras, não garantimos o funcionamento estável do dispositivo. Considere a possibilidade de mudar o dispositivo de lugar, uma vez que o ajuste da sua posição, mesmo que seja apenas 20 cm, pode melhorar significativamente a intensidade do sinal. Se o sinal continuar a ser fraco ou instável após a realocização, considere a utilização do [repetidor do sinal de rádio](#).

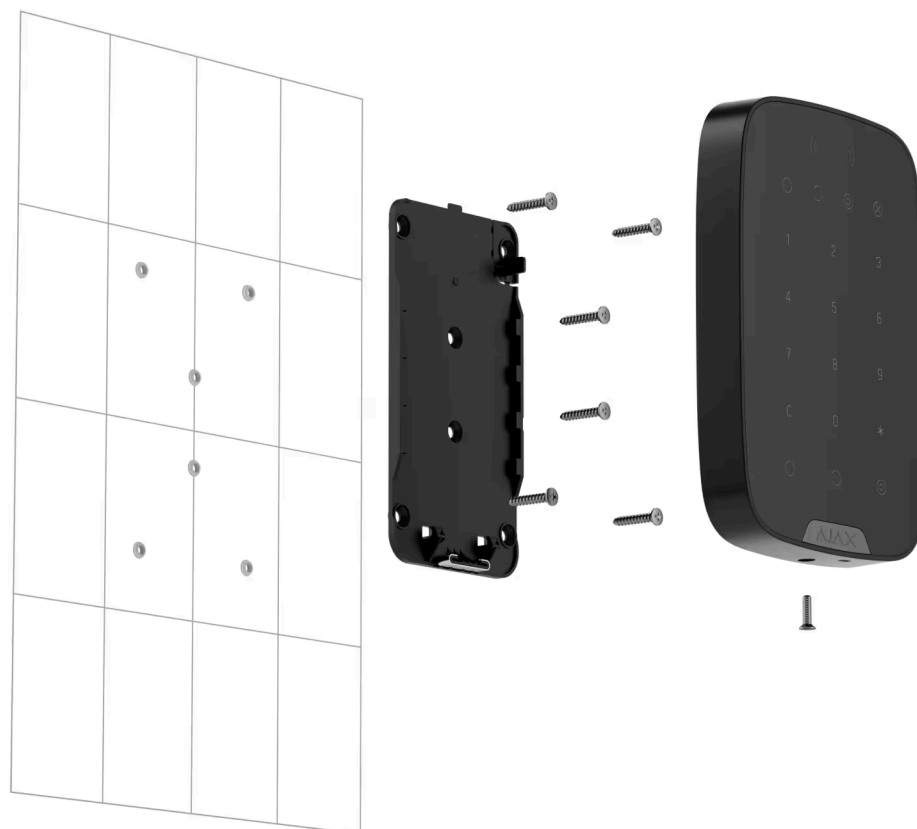
Consulte a secção [Teste de funcionalidade](#) para saber como executar o teste de intensidade do sinal de Jeweller.

[O que é o teste de intensidade de sinal Jeweller](#)

Onde não instalar o teclado

1. No exterior. Isto pode levar à falha do dispositivo.
2. Em locais onde os cabos de alimentação ou Ethernet, objetos de decoração ou outros possam obstruir o teclado.
3. Dentro de instalações com temperatura e humidade fora dos limites permitidos. Isto pode danificar o dispositivo.
4. Mais perto do que 1 m do hub ou do repetidor de sinal de rádio.
5. Em locais com uma intensidade de sinal Jeweller baixa ou instável.

Instalação



Antes de instalar Superior KeyPad Plus G3 Jeweller, certifique-se de que selecionou local ideal, em conformidade com os requisitos deste manual.

Para instalar o dispositivo:

1. Desaperte o parafuso de fixação na parte inferior do dispositivo e retire o painel de instalação SmartBracket do teclado.
2. Adicione o dispositivo ao sistema.
3. Fixe temporariamente o painel SmartBracket utilizando fita adesiva de dupla face ou outros fixadores temporários.



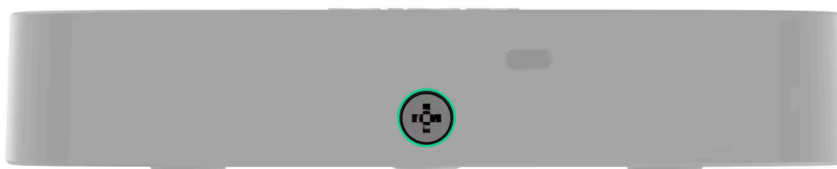
A fita adesiva de dupla face só pode ser utilizada para instalação temporária. O dispositivo fixado com a fita adesiva pode soltar-se da superfície em qualquer altura. Desde que o dispositivo esteja colado com a fita, o alarme de tamper anti-sabotagem não será acionado quando o dispositivo se soltar da superfície.

4. Coloque o teclado no painel de instalação SmartBracket. O indicador LED do dispositivo **X** pisca, mostrando que a carcaça do dispositivo está fechada.
5. Execute o teste de funcionalidade.
6. Se os testes forem bem-sucedidos, retire o teclado do SmartBracket.
7. Fixe o painel de instalação SmartBracket na superfície utilizando os parafusos incluídos. Utilize todos os pontos de fixação.



Se utilizar outros elementos de fixação, certifique-se de que não danificam ou deformam o painel.

8. Coloque o teclado no painel de instalação SmartBracket.
9. Aperte o parafuso de fixação na parte inferior da carcaça do detetor. O parafuso é necessário para uma fixação mais fiável e para proteger o teclado de uma desmontagem rápida.



Adicionar ao sistema



O hub e o dispositivo que operam em diferentes radiofrequências são incompatíveis. O alcance da frequência de rádio do dispositivo pode variar consoante a região. Recomendamos comprar e utilizar dispositivos Ajax na mesma região. Pode verificar a gama de radiofrequências de funcionamento com o [serviço de suporte técnico](#).


Verifique a compatibilidade dos dispositivos antes de adicionar o dispositivo ao sistema. Apenas parceiros verificados podem adicionar e configurar dispositivos Superior nas [apps Ajax PRO](#).

[Tipos de contas e respetivos direitos](#)

Antes de adicionar um dispositivo

1. Instale um [app Ajax PRO](#).
2. Inicie sessão na sua [conta PRO](#) ou crie uma nova.
3. Selecione um [espaço](#) ou crie um novo.
4. Adicione pelo menos uma [sala virtual](#).
5. Adicione um [hub compatível](#) ao espaço. Certifique-se de que o hub está ligado e tem acesso à Internet através de Ethernet, Wi-Fi e/ou rede móvel.
6. Verifique os estados na app Ajax para garantir que o espaço está desarmado e que o hub não está a iniciar uma atualização.

Adicionar ao hub

1. Abra a [app Ajax PRO](#). Selecione um [espaço](#) ao qual pretende adicionar o dispositivo.
2. Aceda ao separador **Dispositivos**  e toque em **Adicionar dispositivo**.
3. Atribua um nome ao dispositivo.
4. Digitalize o código QR ou introduza o ID manualmente. Um código QR com identificação está na carcaça do dispositivo. Também, está duplicado na embalagem do dispositivo.



5. Selecione a sala virtual e o grupo de segurança (se o Modo de grupo estiver ativado).
6. Toque em **Adicionar** – a contagem decrescente começará.
7. Ligue o dispositivo mantendo premido o botão de alimentação durante 3 segundos.



Se a ligação falhar, tente novamente dentro de 5 segundos. Se o número máximo de dispositivos já tiver sido adicionado ao hub, receberá uma notificação de erro ao tentar adicionar mais.

Uma vez adicionado ao hub, o dispositivo aparecerá na lista de dispositivos do hub na app Ajax. A frequência de atualização dos estados dos dispositivos na lista depende das definições **Jeweller** ou **Jeweller/Fibra** e é de 36 segundos por defeito.



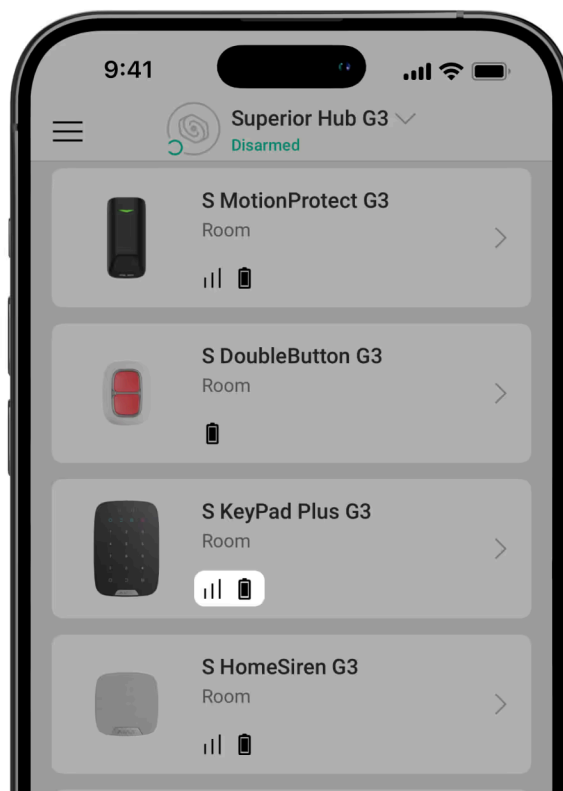
Superior KeyPad Plus G3 Jeweller funciona apenas com um hub. Quando emparelhado com um novo hub, deixa de enviar eventos para o antigo. A adição do teclado a um novo hub não o remove automaticamente da lista de dispositivos do hub antigo. Isto deve ser feito através da app Ajax.


Teste de funcionalidade







O sistema Ajax oferece vários tipos de testes para ajudar a seleccionar o local de instalação correto para os dispositivos. Para Superior KeyPad Plus G3 Jeweller, estão disponíveis os seguintes testes:






- Teste de intensidade do sinal Jeweller – para determinar a intensidade e estabilidade do sinal entre o hub (ou o repetidor do sinal de rádio) e o dispositivo através do protocolo de transferência de dados Jeweller sem fios no local de instalação do dispositivo.
- Teste de atenuação do sinal – para diminuir ou aumentar a potência do transmissor de rádio; para verificar a estabilidade da comunicação entre o dispositivo e o hub, é simulada a mudança de ambiente no local.

Ícones

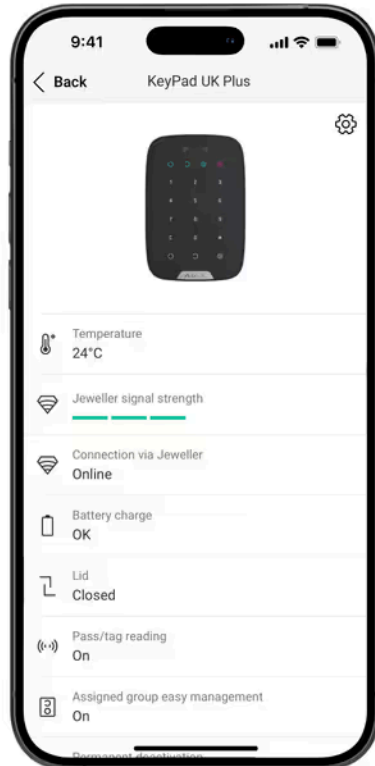


Os ícones na app Ajax apresentam alguns dos estados de Superior KeyPad Plus G3 Jeweller. É possível verificar os ícones no separador **Dispositivos** .


Ícone	Significado
	Intensidade do sinal Jeweller. Apresenta a intensidade do sinal entre o hub e o dispositivo. O valor recomendado é de 2–3 barras. Saiba mais
	Nível de carga da bateria do dispositivo. Saiba mais
	O detetor funciona através do repetidor do sinal. Saiba mais
	A leitura de Pass/Tag está ativada nas definições do teclado.
	O dispositivo está no modo de teste de atenuação do sinal. Saiba mais
	O dispositivo está permanentemente desativado. Saiba mais


	<p>As notificações de alarme de tamper são permanentemente desativadas.</p> <p>Saiba mais</p>
	<p>O dispositivo fica desativado até ao primeiro desarme do sistema.</p> <p>Saiba mais</p>
	<p>As notificações de alarme de tamper são desativadas até que o local seja desarmado pela primeira vez.</p> <p>Saiba mais</p>
	<p>O dispositivo perdeu a ligação com o hub ou o hub perdeu a ligação com o servidor Ajax Cloud.</p>
	<p>O dispositivo não foi transferido para o novo hub.</p> <p>Saiba mais</p>

Estados




Os estados incluem informações sobre o dispositivo e os seus parâmetros de funcionamento. Os estados de Superior KeyPad Plus G3 Jeweller podem ser encontrados nas apps Ajax:

1. Aceda ao separador **Dispositivos** .
2. Selecione **Superior KeyPad Plus G3 Jeweller** na lista.

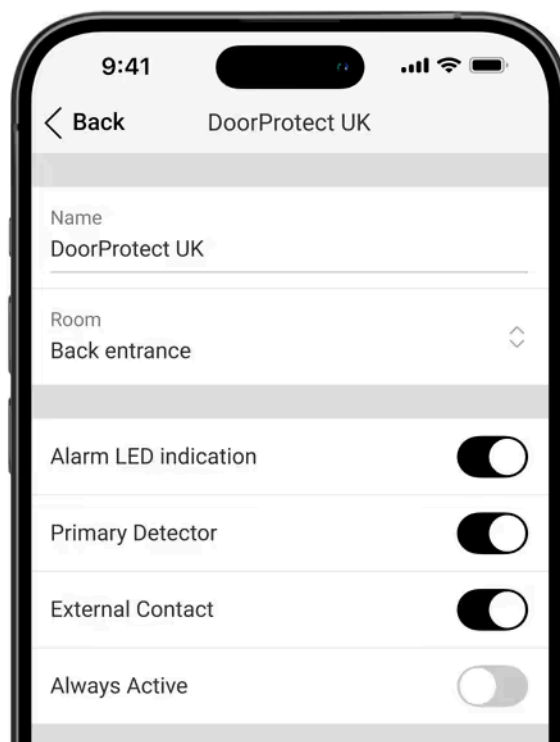
Parâmetro	Significado
Importação de dados	<p>Apresenta o erro aquando da transferência de dados para o novo hub:</p> <ul style="list-style-type: none">• Falha – o dispositivo não foi transferido para o novo hub. <p>Saiba mais</p>
Avaria	<p>Tocar em  abre a lista de todas as avarias.</p> <p>O campo só aparece se for detetada uma avaria.</p>
Temperatura	<p>Temperatura do dispositivo. É medida pelo processador e muda consoante a temperatura ambiente.</p> <p>É possível criar um cenário por temperatura para controlar dispositivos de automatização.</p> <p>Saiba mais</p>
Intensidade do sinal Jeweller	<p>Intensidade do sinal do Jeweller entre o dispositivo e o hub (ou o repetidor do sinal de rádio). O valor recomendado é de 2–3 barras.</p> <p>Jeweller é um protocolo para a transmissão de eventos e alarmes.</p>
Ligação através de Jeweller	<p>Estado da ligação através do canal Jeweller entre o dispositivo e o hub (ou o repetidor):</p> <ul style="list-style-type: none">• Online – o dispositivo está ligado ao hub (ou ao repetidor). Estado normal.• Offline – o dispositivo não está ligado ao hub (ou ao repetidor). Verifique a ligação do dispositivo.
Potência do transmissor	<p>Apresenta a potência selecionada do transmissor.</p> <p>O parâmetro aparece quando a opção Máx ou Atenuação é selecionada no menu Teste de atenuação do sinal.</p>

	<p>Saiba mais</p>
<Range extender name>	<p>Estado da ligação do dispositivo ao <u>repetidor do sinal de rádio</u>:</p> <ul style="list-style-type: none"> • Online – o dispositivo está ligado ao repetidor. • Offline – o dispositivo não está ligado ao repetidor. <p>O campo aparece se o detetor funcionar através do repetidor do sinal.</p>
Carga da bateria	<p>O nível de carga da bateria do dispositivo. Estão disponíveis dois estados:</p> <ul style="list-style-type: none"> • OK. • Bateria fraca. <p>Quando as baterias tiverem de ser substituídas, os utilizadores e a empresa de segurança receberão as notificações adequadas.</p> <p>Saiba mais</p>
Tampa	<p>O estado do botão de tampo do dispositivo que responde à separação ou abertura da carcaça do dispositivo:</p> <ul style="list-style-type: none"> • Aberto – o detetor é removido do painel de instalação SmartBracket, ou a sua integridade é comprometida. Verifique a montagem do detetor. • Fechado – o dispositivo está instalado no painel de instalação SmartBracket. A integridade da carcaça do dispositivo e do painel de instalação não está comprometida. Estado normal. <p>Saiba mais</p>
Leitura de Pass/Tag	<p>Apresenta se o leitor de cartões e comandos está ativado.</p>
Gestão fácil do modo armado	<p>Mostra a configuração para a funcionalidade Gestão fácil do modo armado:</p> <ul style="list-style-type: none"> • Desativado – cada tentativa de armar ou desarmar deve ser confirmada introduzindo o código de acesso ou apresentando o dispositivo de acesso.



	<ul style="list-style-type: none"> • Armar/desarmar utilizando um dispositivo de acesso sem confirmar a ação com botões – permite aos utilizadores alternar os modos de segurança do sistema utilizando dispositivos de acesso sem confirmação, premindo os botões do teclado. • Desarmar sem botão de desarme – o sistema ou os seus grupos, cuja segurança é gerida com um código de acesso ou dispositivos de acesso, serão desarmados sem confirmação, premindo os botões do teclado. <div style="border: 1px solid yellow; border-radius: 10px; padding: 10px; margin-top: 10px;">  Deve ser definido um comprimento fixo para o código de acesso nas definições do hub na app Ajax PRO. </div>
<p>Encriptação avançada</p>	<p>O estado da comunicação com encriptação avançada entre o dispositivo e o hub ou repetidor de sinal de rádio:</p> <ul style="list-style-type: none"> • Ativo – a comunicação do dispositivo é protegida por encriptação avançada. • Inativo – a comunicação do dispositivo funciona sem encriptação avançada. <p>Saiba mais</p>
<p>Desativação permanente</p>	<p>Apresenta o estado da definição de desativação permanente do dispositivo:</p> <ul style="list-style-type: none"> • Não – o dispositivo funciona normalmente e transmite todos os eventos. • Inteiramente – o dispositivo é completamente excluído da operação do sistema pelo administrador do hub. O dispositivo não executa comandos do sistema e não comunica alarmes ou outros eventos. • Apenas tampa – o administrador do hub desativou as notificações sobre a ativação de alarme de tamper. <p>Saiba mais</p>
<p>Desativação única</p>	<p>Apresenta o estado da definição de desativação única do dispositivo:</p>


	<ul style="list-style-type: none"> • Não – o dispositivo funciona no modo normal. • Inteiramente – o dispositivo é completamente excluído do funcionamento do sistema enquanto o modo armado está ativo. O dispositivo não executa comandos do sistema e não comunica alarmes ou outros eventos. • Apenas tampa – as notificações sobre o acionamento do alarme de tamper anti-sabotagem estão desativadas enquanto o modo armado está ativo. <p>Saiba mais</p>
Firmware	Versão do firmware do dispositivo.
ID do dispositivo	ID do dispositivo. Também disponível no código QR na carcaça do dispositivo e na sua caixa de embalagem.
Número do Dispositivo	Número do dispositivo. Este número é transmitido à CRA em caso de alarme ou evento.

Definições






Para alterar as definições de Superior KeyPad Plus G3 Jeweller na app Ajax:

1. Aceda ao separador **Dispositivos** .
2. Selecione **Superior KeyPad Plus G3 Jeweller** na lista.
3. Aceda a **Definições** .
4. Defina as definições necessárias.
5. Toque em **Voltar** para guardar as novas definições.

Definições	Significado
Nome	<p>Nome do dispositivo. Apresentado na lista de dispositivos do hub, texto SMS e notificações no historial de eventos.</p> <p>Para alterar o nome do dispositivo, toque no campo de texto.</p> <p>O nome pode conter até 24 caracteres latinos ou até 12 caracteres cirílicos.</p>
Sala	<p>Seleção da divisão virtual à qual Superior KeyPad Plus G3 Jeweller está atribuído.</p> <p>O nome da sala é apresentado no texto de SMS e notificações no feed de eventos.</p>
Gestão de grupos	<p>Seleção do grupo de segurança controlado pelo dispositivo. Pode seleccionar todos os grupos ou apenas um.</p> <p>O campo aparece quando o <u>Modo de grupo</u> está ativado.</p> <div data-bbox="813 1518 1468 1870" style="border: 1px solid #00c000; border-radius: 10px; padding: 10px;"><p> Se a funcionalidade <u>Grupo seguido</u> estiver configurada para grupos, o seu estado de segurança pode mudar automaticamente em função das suas definições e dos estados dos iniciadores.</p></div>
Definições de acesso	<p>Seleção do método de armar/desarmar:</p> <ul style="list-style-type: none">• Apenas códigos de teclado.• Apenas códigos de utilizador.

	<ul style="list-style-type: none"> • Códigos de teclado e de utilizador. <p>Para ativar os Códigos de acesso do teclado configurados para pessoas que não estão registadas no sistema, seleccione as opções no teclado: Apenas códigos do teclado ou Códigos do teclado e do utilizador.</p>
Código do teclado	Seleção de um código geral para o controlo de segurança. Contém 4 a 6 dígitos.
Código de coação	Seleção de um código de coação geral para o alarme silencioso. Contém 4 a 6 dígitos. <u>Saiba mais</u>
Botão de Função	Seleção da função do botão (botão de Função): <ul style="list-style-type: none"> • Desativado – o botão de função está desativado e não executa nenhum comando quando premido. • Pânico – após pressionar o botão de função, o sistema envia um alerta para a CRA e para todos os utilizadores. • Silenciar alarme de incêndio – quando premido, o sistema silencia o alarme dos detetores de incêndio Ajax. Disponível apenas se a funcionalidade Alarme de detetores de incêndio interligados estiver ativada. <u>Saiba mais</u>
Proteção contra pressão acidental	Quando ativado, o Botão de função deve ser premido duas vezes para enviar um alarme de pânico. Esta definição está disponível se o Botão de função estiver definido para Pânico .
Bloqueio automático de acesso não autorizado	Quando ativado, o teclado será bloqueado durante um período de tempo predefinido se for introduzido um código incorreto ou se forem utilizados dispositivos de acesso não verificados mais de três vezes seguidas no espaço de 1 minuto. PRO ou um utilizador com direitos para configurar o sistema pode desbloquear o teclado através d antes de expirar o tempo de bloqueio especifica
Tempo de bloqueio automático, min	Seleção do período de bloqueio do teclado após tentativas de acesso não autorizado:

	<ul style="list-style-type: none"> • 3 minutos • 5 minutos • 10 minutos • 20 minutos • 30 minutos • 60 minutos • 90 minutos • 180 minutos <p>Disponível se a opção de Auto-bloquear de acesso não autorizado estiver ativada.</p>
Brilho	<p>Ajuste do brilho da retroiluminação dos botões do teclado. A retroiluminação funciona apenas quando o teclado está ativo.</p> <p>Esta opção não afeta o nível de brilho do leitor de Pass/Tag nem dos indicadores dos modos de segurança.</p>
Volume dos botões	Seleção do volume do botão do teclado quando premido.
Leitura de Pass/Tag	Quando ativada, o modo de segurança pode ser controlado com dispositivos de acesso Pass e Tag .
Confirmação de autorização com um código de acesso	<p>Quando a função está ativada, os utilizadores só podem armar ou desarmar o sistema se tiverem sido autorizados com duas formas de identificação, ou seja, utilizando Pass ou Tag e introduzindo o código de acesso adequado.</p> <p><u>Saiba mais</u></p>
Tempo para confirmação	<p>Seleção do tempo máximo para confirmar a autorização com uma palavra-passe após a confirmação do dispositivo de acesso.</p> <p>Disponível se a opção Confirmação de autorização com um código de acesso estiver ativada.</p>
Gestão fácil do modo armado	<p>Permite aos utilizadores armar/desarmar o sistema sem confirmação, premindo os botões do teclado.</p> <p>Estão disponíveis três opções:</p> <ul style="list-style-type: none"> • Desativado – cada tentativa de armar ou desarmar deve ser confirmada introduzindo o código de acesso ou apresentando o dispositivo de acesso.

	<ul style="list-style-type: none"> • Armar/desarmar utilizando um dispositivo de acesso sem confirmar a ação com botões – permite que os utilizadores alternem os modos de segurança do sistema usando dispositivos de acesso sem confirmação com os botões do teclado. • Desarmar sem botão de desarme – o sistema ou os seus grupos, cuja segurança é gerida com um código de acesso ou dispositivos de acesso, serão desarmados sem confirmação, premindo os botões do teclado. <div style="border: 1px solid yellow; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Deve ser definido um comprimento fixo para o código de acesso nas definições do hub na app Ajax PRO.</p> </div>
<p>Armar sem código</p>	<p>Quando ativado, o utilizador pode armar o local sem introduzir um código ou apresentar o dispositivo de acesso pessoal.</p> <p>Se estiver desativada, introduza um código ou apresente o dispositivo de acesso para armar o sistema. O ecrã para introduzir o código aparece depois de premir o botão  Armar.</p>
<p>Ativação automática durante o Atraso ao Entrar</p>	<p>Ativa o teclado após qualquer dispositivo de segurança iniciar <u>Atraso ao entrar</u>.</p> <p>A função de ativação automática também pode reduzir a vida útil das pilhas do teclado.</p>
<p>Alerta com uma sirene se o botão de pânico for premido</p>	<p>A definição é apresentada se a opção Pânico estiver selecionada para o botão de Função.</p> <p>Quando a opção está ativada, as sirenes ligadas ao sistema de segurança emitem um alerta quando o botão  (botão de Função) é premido.</p>
<p>Teste de intensidade de sinal do Jeweller</p>	<p>Passa o dispositivo para o modo de teste de intensidade do sinal do Jeweller.</p> <p>O teste permite-lhe verificar a intensidade do sinal entre o hub (ou o repetidor de sinal de rádio) e o dispositivo através do protocolo de transferência de dados sem fios Jeweller para selecionar o local de instalação ideal.</p>

	<p>Saiba mais</p>
Teste de atenuação do sinal	<p>Passa o dispositivo para o modo de teste de atenuação do sinal.</p> <p>Saiba mais</p>
Repor Pass/Tag	<p>Permite apagar da memória do dispositivo todos os hubs associados a Tag ou Pass.</p> <p>Saiba mais</p>
Guia do utilizador	<p>Abre o manual do utilizador de Superior KeyPad Plus G3 Jeweller na app Ajax.</p>
Desativação permanente	<p>Permite ao utilizador desativar o dispositivo sem o retirar do sistema.</p> <p>Estão disponíveis três opções:</p> <ul style="list-style-type: none"> • Não – o dispositivo funciona em modo normal e transmite todos os eventos. • Inteiramente – o dispositivo não executará comandos do sistema nem participará em cenários de automatização, e o sistema ignorará os alarmes do dispositivo e outras notificações. • Apenas tampa – o sistema ignora apenas as notificações sobre a ativação do alarme de tamper do dispositivo. <p>Saiba mais</p>
Desativação única	<p>Permite ao utilizador desativar eventos do dispositivo até ao primeiro desarme.</p> <p>Estão disponíveis três opções:</p> <ul style="list-style-type: none"> • Não – o dispositivo funciona em modo normal e transmite todos os eventos. • Inteiramente – o dispositivo é completamente excluído dos funcionamentos do sistema até ao primeiro desarme. O dispositivo não executa comandos do sistema e não comunica alarmes ou outros eventos. • Apenas tampa – as notificações sobre o alarme de tamper sendo desativadas até primeiro desarmar. <p>Saiba mais</p>

Eliminar dispositivo

Desemparelha o dispositivo, desliga-o do hub e elimina as suas definições.

Definição de códigos



i Nas apps Ajax PRO, nas definições do hub, é possível definir os requisitos para o comprimento dos códigos de acesso utilizados para autorização do utilizador e acesso ao sistema. Pode seleccionar a opção **Flexível (4 a 6 símbolos)** ou definir o comprimento de código fixo: **4 símbolos, 5 símbolos ou 6 símbolos**.

A definição de um comprimento de código fixo irá repor todos os códigos de acesso previamente configurados.

O comprimento fixo do código é necessário para a funcionalidade **Gestão fácil do modo armado**, que permite desarmar o sistema sem premir o botão **Desarmar** no teclado após introduzir um código de acesso ou utilizar um dispositivo de acesso.


Códigos de acesso ao teclado

Para definir os códigos de coação do teclado e do teclado:

1. Na app Ajax, aceda ao separador **Dispositivos** .
2. Selecione o teclado para o qual pretende configurar um código de acesso.
3. Aceda às **Definições** .
4. Selecione a opção **Apenas códigos do teclado** ou **Códigos do teclado e do utilizador** no menu **Definições de acesso**.
5. Aceda ao menu **Código do teclado**.
6. Defina o código do teclado. Contém de 4 a 6 dígitos.
7. Toque em **Concluído**.
8. Aceda ao menu **Código de coação**.
9. Defina o código de coação do teclado. Contém de 4 a 6 dígitos.
10. Toque em **Concluído**.


Códigos de acesso do utilizador

Para definir um código pessoal e um código de coação pessoal:

1. Selecione um espaço na app Ajax.
2. Aceda ao menu **Definições** .
3. Abra o menu **Utilizadores**.
4. Localize a sua conta na lista e toque nela.
5. Aceda ao menu **Configurações de palavra-passe**.
6. Defina o **Código do utilizador**. Contém de 4 a 6 dígitos.
7. Toque em **Guardar**.
8. Defina o **Código de coação**. Contém de 4 a 6 dígitos.
9. Toque em **Guardar**.
10. Toque em **Voltar** para guardar as definições.

Código de utilizador não registado

Para definir um código de acesso para um utilizador sem conta:

1. Selecione o hub na app Ajax.
2. Aceda ao menu **Definições** .
3. Aceda ao menu **Códigos de acesso do teclado**.
4. Toque em **Adicionar código**. Defina o **Nome** e o **Código de acesso**. Contém de 4 a 6 dígitos.
5. Toque em **Adicionar** para guardar os dados.

Para definir um código de coação para um utilizador sem conta:

1. Selecione o menu **Códigos de acesso do teclado** nas definições do hub.
2. Selecione o utilizador não registado pretendido.
3. Toque em **Adicionar código de coação**. Defina o código. Contém de 4 a 6 dígitos.
4. Toque em **Concluído**.



Para utilizadores não registados, um administrador ou PRO com direitos de configuração do sistema pode ajustar o acesso à gestão da segurança. Primeiro, ative o Modo de grupo. Em seguida, selecione o menu **Códigos de acesso do teclado** nas

definições do hub, encontre o utilizador pretendido e defina os parâmetros adequados no menu **Gestão da segurança**.

Código URR

Apenas um PRO com direitos de configuração do sistema pode criar e configurar os códigos URR nas apps Ajax PRO. Pode encontrar mais informações sobre a configuração desta funcionalidade neste artigo.

Cartões e comandos

Superior KeyPad Plus G3 Jeweller pode funcionar com comandos Tag, cartões Pass e dispositivos de terceiros que suportam a tecnologia DESFire®.


i Antes de adicionar dispositivos de terceiros que suportem DESFire®, certifique-se de que estes têm memória livre suficiente para suportar o novo teclado. De preferência, o dispositivo de terceiros deve ser pré-formatado.

Este artigo fornece informações sobre como repor o **Tag** ou o **Pass**.

O número máximo de dispositivos Pass e Tag adicionados depende do modelo do hub. Os dispositivos Pass e Tag adicionados não afetam o limite total de dispositivos no hub.

Verifique a compatibilidade do dispositivo

Adicionar Tag ou Pass

1. Abra a app Ajax.
2. Selecione o espaço com hub ao qual pretende adicionar Tag ou Pass.
3. Aceda ao separador **Dispositivos** .



Certifique-se de que a função **Leitura de pass/tag** está ativada em pelo menos uma definição do teclado.

4. Toque em **Adicionar dispositivo**.
5. Selecione **Adicionar pass/tag**.
6. Especifique o tipo (Tag ou Pass), a cor, o nome do dispositivo e o utilizador (se necessário).
7. Toque em **Seguinte**. Depois disso, o hub passa para o modo de registo de dispositivos.
8. Aceda a qualquer teclado compatível com a **Leitura de pass/tag** ativada. Prima o botão **Desarmar** para mudar o teclado para o modo de registo do dispositivo de acesso.
9. Encoste o Pass ou o Tag com o lado largo virado para o teclado durante alguns segundos. Após a adição bem sucedida, receberá uma notificação na app Ajax.

Se a conexão falhar, tente novamente dentro de 5 segundos. Tenha em atenção que, se o número máximo de dispositivos Tag ou Pass já tiver sido adicionado ao hub, receberá uma notificação correspondente na app Ajax quando adicionar um novo dispositivo.



Tanto o Tag como o Pass podem funcionar com vários hubs ao mesmo tempo. O número máximo de hubs é 13. Se tentar adicionar um Tag ou um Pass a um hub que já tenha atingido o limite de hubs, receberá uma notificação correspondente. Para adicionar um comando/cartão a um novo hub, terá de o repor.


Se precisar de adicionar outro Tag ou Pass, toque em **Adicionar outro pass/tag** na app. Repetir os passos 6–9.

Apagar (repor) Tag ou Pass




A reinicialização elimina todas as definições e ligações dos comandos e cartões. O Tag e o Pass são eliminados apenas do hub a partir do qual a formatação foi efetuada. Noutros hubs, Tag ou Pass continuam a ser apresentados na app, mas não

podem ser utilizados para gerir os modos de segurança. Estes dispositivos devem ser removidos manualmente.

1. Abra a app Ajax.
2. Selecione e espaço.
3. Aceda ao separador **Dispositivos** .
4. Selecione um teclado compatível na lista de dispositivos.



Certifique-se de que a função **Leitura de pass/tag** está ativada nas definições do teclado.

5. Aceda às definições do teclado clicando no ícone .
6. Toque em **Repor pass/tag**.
7. Toque em **Continuar**.
8. Aceda a qualquer teclado compatível com a **Leitura de pass/tag** ativada. Prima o botão **Desarmar** para mudar o teclado para o modo de reposição do dispositivo de acesso.
9. Encoste o Pass ou o Tag com o lado largo virado para o teclado durante alguns segundos. Após a formatação bem sucedida, receberá uma notificação na app Ajax. Se a formatação falhar, tente novamente.

Se precisar repor outro Tag ou Pass, toque em **Repor outro Pass/Tag** na app. Repita o passo 9.

Controlo da segurança

Utilizando códigos, Tag ou Pass, é possível controlar **Modo noturno** e a segurança de todo o local ou de grupos separados. O utilizador ou PRO com direitos de configuração do sistema pode definir códigos de acesso. [Este capítulo](#) fornece informações sobre como adicionar Tag ou Pass ao hub.

Se for utilizado um código pessoal ou de acesso, Tag ou Pass, o nome do utilizador que alterou o modo de segurança é apresentado no historial de eventos do hub e na lista de notificações. Se for utilizado um código geral, é apresentado o nome do teclado a partir do qual o modo de segurança foi alterado.

i Superior KeyPad Plus G3 Jeweller fica bloqueado durante o tempo especificado nas definições se for introduzido um código incorreto ou se for apresentado um dispositivo de acesso não verificado três vezes consecutivas num intervalo de 1 minuto. As notificações correspondentes são enviadas aos utilizadores e à estação de controlo da empresa de segurança. Um utilizador ou PRO com direitos para configurar o sistema pode desbloquear Superior KeyPad Plus G3 Jeweller na app Ajax.

A sequência de passos para alterar o modo de segurança com o teclado depende se as opções **Armar sem código**, **Confirmação de autorização com um código de acesso** e **Gestão fácil do modo armado** estão ativadas nas definições de Superior KeyPad Plus G3 Jeweller.




Utilização de Tag ou Pass


















1. Ative o teclado aproximando a sua mão na frente dele.
2. Aproxime Tag ou Pass do leitor de Tag/Pass do teclado.
3. Introduza o código necessário se a função **Confirmação de autorização com um código de acesso** estiver ativada.
4. Prima o botão **Armar**, **Desarmar** ou **Modo noturno** no teclado.

Se a opção **Gestão fácil do modo armado** estiver ativada, não é necessário premir o botão **Armar**, **Desarmar** ou **Modo noturno** após a leitura do dispositivo de acesso.

Utilização de códigos de acesso

i Os códigos introduzidos incorretamente podem ser eliminados premindo o botão **Repor**.

Código	Exemplo	Atenção
Gestão dos modos de segurança da instalação		
Código do teclado	1234 →  /  / 	
Código de coação do teclado		

Código do utilizador	5 → → 1234 →  /  /	5 é um ID de utilizador
Código de coação do utilizador		
Código de utilizador não registado	1234 →  /  / 	
Código de coação do utilizador não registado		
Código URR	1234 →  /  / 	
Gestão dos modos de segurança de grupo		
Código do teclado	1234 → → 2 →  / 	2 é um ID de grupo
Código de coação do teclado		
Código do utilizador	5 → → 1234 → → 2 →	5 é um ID de utilizador
Código de coação do utilizador	 / 	2 é um ID de grupo
Código de utilizador não registado	1234 → → 2 →  / 	2 é um ID de grupo
Código de coação do utilizador não registado		
Código URR	1234 → → 2 →  / 	2 é um ID de grupo

[Saiba mais sobre o ID de utilizador](#)

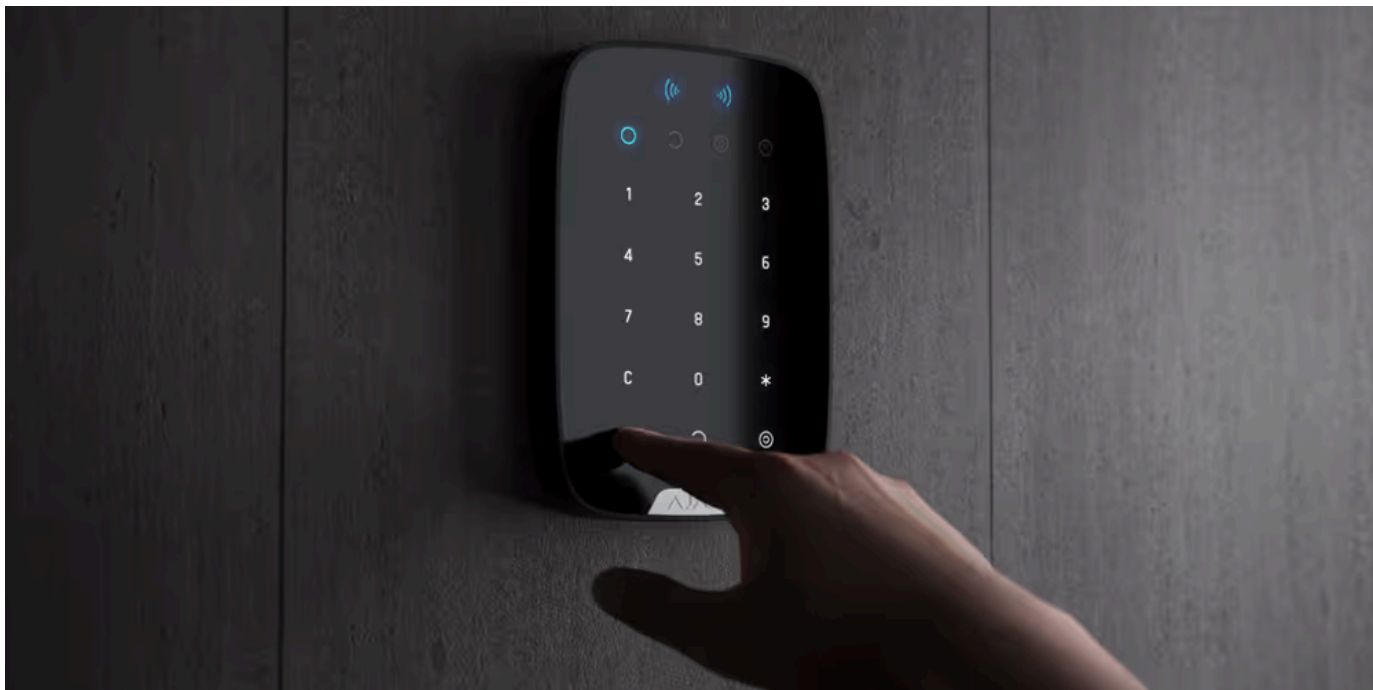
[Saiba mais sobre o ID do grupo](#)

Confirmação de autorização com um código de acesso

A Confirmação de autorização com um código de acesso é uma funcionalidade que permite configurar a autenticação de dois fatores para os utilizadores quando estes controlam os modos de segurança do sistema. Esta definição significa que os utilizadores devem primeiro utilizar um dispositivo de acesso (Pass ou Tag) e, em seguida, introduzir um código de acesso para confirmarem a sua autorização no sistema.

[Saiba mais sobre a confirmação de autorização com um código de acesso](#)

Indicação



Superior KeyPad Plus G3 Jeweller pode indicar o modo de segurança atual, as teclas premidas, as avarias e o estado através de uma indicação LED e de um som. A retroiluminação mostra o modo de segurança atual após o teclado ser ativado. As informações sobre o modo de segurança atual são relevantes mesmo que o modo de armar seja alterado por outro dispositivo: um comando, outro teclado ou uma app.

Pode ativar o teclado passando a mão sobre o painel tátil de cima para baixo. Quando ativada, a retroiluminação do teclado acende-se e é emitido um sinal sonoro (se estiver ativado).

Evento	Indicação	Atenção
Ligação do dispositivo	Todos os indicadores e a retroiluminação do teclado numérico acendem-se brevemente. Em seguida, um sinal sonoro de três tons é emitido e o LED do modo de segurança atual do sistema e a retroiluminação do teclado numérico acendem-se. A seguir, a retroiluminação do teclado numérico apaga-se suavemente e é emitido um sinal sonoro duplo	



Ligar o dispositivo que não foi adicionado ao hub	Todos os indicadores e a retroiluminação do teclado numérico acendem-se brevemente. Depois disso, o LED X pisca 6 vezes e, em seguida, pisca 3 vezes rapidamente	O teclado desliga-se após o término da indicação
Desligação do dispositivo	O LED X acende-se durante cerca de 1 segundo e, em seguida, pisca 3 vezes	O sistema envia uma notificação quando o teclado é desligado com o botão de alimentação
O dispositivo é eliminado do hub	O LED X pisca 6 vezes e, em seguida, pisca 3 vezes rapidamente	O teclado desliga-se após o término da indicação
Não existe qualquer ligação ao hub ou ao repetidor de sinal de rádio	O LED X pisca	
A tampa do dispositivo está aberta (o painel SmartBracket foi removido)	O LED X pisca brevemente uma vez	
Botão tátil premido	Sinal sonoro curto, o LED de estado de segurança atual do sistema pisca uma vez	O volume depende das definições do teclado
O sistema está armado	Sinal sonoro curto, LED Armado ou Modo noturno acende-se	
O sistema está desarmado	Dois sinais sonoros curtos, o LED Desarmado acende-se	
Foi introduzido um código incorreto ou foi feita uma tentativa de alterar o modo de segurança com um pass/tag não ligado ou desativado	Sinal sonoro longo, a retroiluminação do teclado numérico pisca 3 vezes	
O modo de segurança não pode ser ativado (falha na Verificação da integridade do sistema)	Sinal sonoro longo, o LED do estado de segurança atual pisca 3 vezes	
O sistema requer a confirmação da autorização com uma palavra-passe após a confirmação do dispositivo de acesso. Disponível se a funcionalidade Confirmação da autorização com uma palavra-passe estiver ativada	O LED do estado de segurança atual pisca durante o tempo definido para confirmação	

O teclado está bloqueado devido a uma tentativa de introdução de código incorreto ou tentativa de utilização de um pass/tag não autorizado	Sinal sonoro longo, durante o qual os LEDs de estado de segurança e a retroiluminação do teclado piscam 3 vezes	
O hub não responde	Sinal sonoro longo, o LED X acende-se	
A carga da bateria é baixa	Após a alteração do modo de segurança, o LED X acende-se. Os botões táteis ficam bloqueados durante este período. Quando tenta ligar o teclado com as pilhas descarregadas, este emite um sinal sonoro longo, o LED X acende-se e apaga-se suavemente e, de seguida, o teclado desliga-se.	Como substituir as pilhas

Avisos sonoros de avarias

Superior KeyPad Plus G3 Jeweller pode notificar os utilizadores do sistema com um sinal sonoro se algum dispositivo estiver offline ou se as pilhas estiverem fracas. Os LEDs dos teclados **X** piscarão. As notificações de avaria serão apresentadas no historial de eventos, no texto de SMS ou na notificação push.

Para ativar as notificações sonoras de avarias, utilize numa app Ajax PRO:

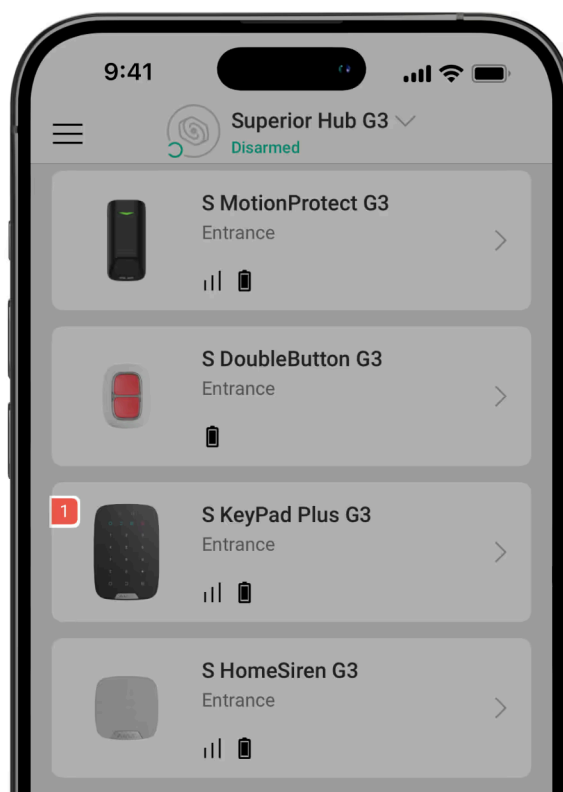
1. Aceda ao separador **Dispositivos** .
2. Selecione o hub e aceda às respetivas definições .
3. Aceda a **Serviço** → **Sons e alertas**.
4. Ative interruptores: **Se a bateria de qualquer dispositivo estiver fraca e Se qualquer dispositivo estiver offline**.
5. Toque em **Voltar** para guardar as definições.

Evento	Indicação	Atenção
Se algum dispositivo estiver offline	Dois sinais sonoros curtos, o LED X pisca duas vezes. Emite um sinal sonoro uma vez por minuto até que todos os	Os utilizadores podem atrasar a indicação sonora por 12 horas

	dispositivos no sistema estejam online.	
Se Superior KeyPad Plus G3 Jeweller estiver offline	Dois sinais sonoros curtos, o LED X pisca duas vezes. Emite um sinal sonoro uma vez por minuto até o teclado ficar online no sistema.	É impossível atrasar a indicação sonora
Se a bateria de qualquer dispositivo estiver fraca	Três sinais sonoros curtos, o LED X pisca três vezes. Emite um sinal sonoro uma vez por minuto até as pilhas serem restauradas ou o dispositivo ser removido.	Os utilizadores podem atrasar a indicação sonora por 4 horas

Os avisos sonoros de avarias aparecem quando a indicação do teclado termina. Se ocorrerem várias avarias no sistema, o teclado notificará primeiro a perda de ligação entre o dispositivo e o hub.

Avarias



Quando o dispositivo deteta uma avaria (por exemplo, não há ligação através do protocolo Jeweller), é apresentado um contador de avarias na app Ajax no canto superior esquerdo do ícone do dispositivo.

Todas as avarias podem ser vistas nos estados do dispositivo. Os campos com avarias vão ser indicados a vermelho.

Uma avaria é apresentada se:

- A temperatura do dispositivo está fora dos limites aceitáveis.
- A tampa do dispositivo está aberta (o alarme de tamper é ativado).
- Não há ligação com o hub ou com o repetidor do sinal de rádio através do Jeweller.
- A bateria do dispositivo está fraca.

Manutenção

Verifique regularmente o funcionamento do dispositivo. A frequência ideal dos controlos é de três em três meses. Limpe a carcaça do dispositivo de pó, teias de aranha e outros contaminantes à medida que vão surgindo. Utilize um pano macio e seco adequado para a manutenção do equipamento.

Não utilize substâncias que contenham álcool, acetona, gasolina e outros solventes ativos para limpar o dispositivo.

Se as pilhas do teclado estiverem fracas, o sistema envia notificações apropriadas e o indicador **X** de **Avaria** acende-se suavemente e apaga-se após cada introdução bem-sucedida do código.

Superior KeyPad Plus G3 Jeweller pode funcionar por até 2 meses após o sinal de bateria fraca. No entanto, recomendamos que substitua as pilhas imediatamente após a notificação. É aconselhável utilizar pilhas de lítio. Têm uma grande capacidade e são menos afetados por temperaturas.

[Como substituir as pilhas em Superior KeyPad Plus G3 Jeweller](#)

Características técnicas

[Todas as características técnicas](#)

Conformidade com as normas

Ligação em conformidade com os requisitos da norma EN 50131

Garantia

A garantia dos produtos da «Ajax Systems Manufacturing» Limited Liability Company é válida durante 2 anos após a compra.

Se o dispositivo não funcionar corretamente, recomendamos que contacte primeiro o serviço de assistência, uma vez que a maioria dos problemas técnicos pode ser resolvida remotamente.

Obrigações de garantia

Acordo de Utilizador

Contactar o Suporte Técnico:

- e-mail
- Telegram

Fabricado por «AS Manufacturing» LLC



Precisa de ajuda?

Nesta secção, encontrará manuais detalhados e vídeos educativos sobre todas as funcionalidades de Ajax. Se precisar de ajuda técnica, estamos disponíveis 24 horas por dia, 7 dias por semana.

[Enviar pedido](#)

Subscrever

Subscreva a nossa newsletter sobre vida segura. Sem spam.

[Subscrever](#)

Solicitar ajuda extra

✉ support@ajax.systems

📍 @AjaxSystemsSupport_Bot

💬 Enviar pedido



4.500.000

pessoas em todo o mundo protegidas por Ajax

Classificação 4.8

🔗 Sugerir uma funcionalidade



Produtos

Proteção contra intrusão

Videovigilância

Segurança contra Incêndio

Conforto e automatização

Todos os produtos

Serviços

Integrações de sistema

Produtos Ajax Ready

Protocolo Fibra com fios

Protocolos de rádio Ajax

Software

Ajax Security System

Ajax PRO: Tool for Engineers

Ajax Desktop

Ajax PRO Desktop

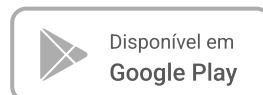
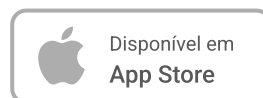
Ajax TV

Ajax Translator PRO

Ajax Cloud Signaling

Ajax Media Player

Cenários



Soluções

Histórias dos clientes

Soluções por tipo de instalação

Sistema comercial de deteção e alarme de incêndios

Solução sem fios de Grade 3

Solução de videovigilância

Integração com fechaduras inteligentes Yale

Assistência

Guias e Artigos

Conformidade com as normas

Ferramentas

Compatibilidade dos dispositivos Ajax

[Atualizações e modernizações](#)

[Porquê Ajax](#)

[Como funciona Ajax](#)

[Compatibilidade com software da CRA](#)

[Disponibilidade dos Serviços Ajax](#)

[Calculadora de armazenamento de vídeo](#)

[Calculadora de dispositivos de vídeo](#)

[Calculadora da duração da bateria](#)

[Calculadora do alcance da comunicação via rádio](#)

[Configuradora de interruptores e tomadas](#)

[Calculadora de fonte de alimentação Fibra](#)

[Todas as ferramentas Web](#)

Soluções de monitorização e integrações

[Monitorização de alarmes de intrusão](#)

[Videovigilância e verificação visual de alarmes](#)

[Verificação de alarmes por áudio](#)

Empresa

[Blog](#)

[Sobre nós](#)

[Página de imprensa](#)

[Eventos](#)

[Carreira](#)

[Ajax Next](#)

[Avaliações e feedback](#)

Para parceiros

[Para parceiros](#)

[Ajax Academy](#)

[Partner Portal](#)

 [España](#) [Política de Privacidade](#) [Comunicar uma vulnerabilidade](#) [Artigo técnico RGPD](#) [Declaração NDAA](#)

[Política de cookies](#) [Política Anti-Spam](#) [Ajax Services T&C](#) [Acordo de Utilizador Final](#) [Garantia](#)

© 2026 AJAX SYSTEMS CH. Todos os direitos reservados