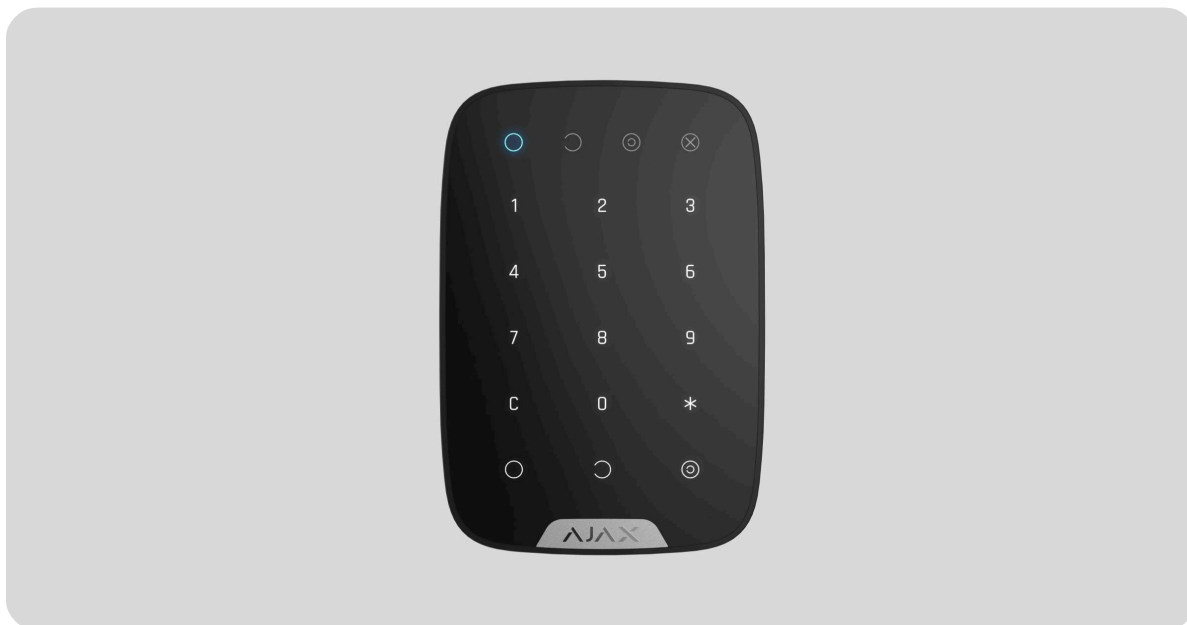


Manual do utilizador do KeyPad

Atualizado Setembro 1, 2025



O **KeyPad** é um teclado interior sem fios sensível ao toque que gere o sistema Ajax. Concebido para utilização em interior. Com este dispositivo, o utilizador pode armar e desarmar o sistema e ver o seu estado de segurança. O KeyPad está protegido contra tentativas de adivinhação do código e pode emitir um alarme silencioso quando o código é introduzido sob coação.

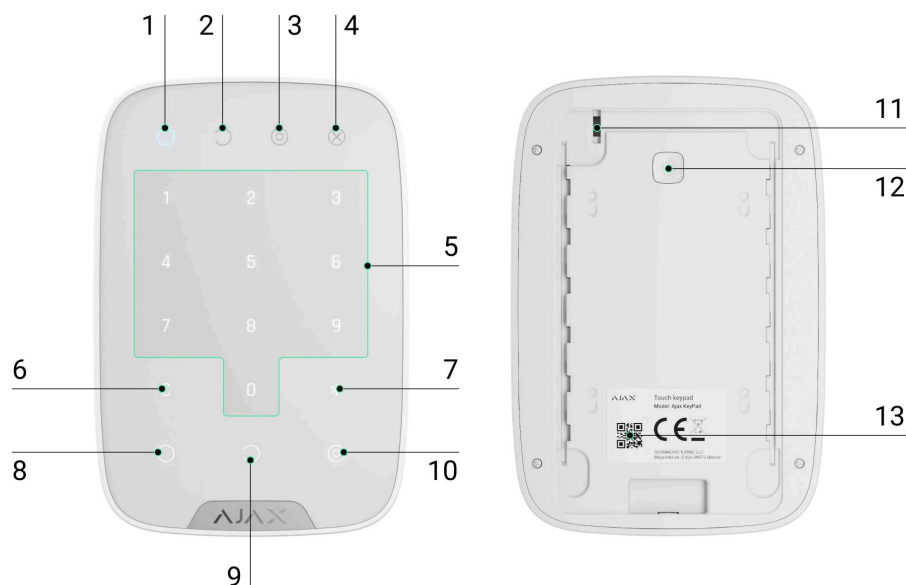
Ligando-se ao sistema Ajax através de um protocolo de rádio seguro **Jeweller**, o KeyPad comunica com o **hub** a uma distância de até 1700 m em linha reta.



O KeyPad funciona apenas com hubs Ajax e não suporta a ligação através dos módulos de integração **ocBridge Plus** ou **uartBridge**.

O dispositivo é configurado através das **aplicações Ajax** para iOS, Android, macOS e Windows.

Elementos funcionais



1. Indicador de modo **Armado**
2. Indicador de modo **Desarmado**
3. Indicador do **Modo noturno**
4. Indicador de **Avaria**
5. O bloco de botões numéricos
6. Botão **Limpar**
7. Botão de **Função**
8. Botão para **Armar**
9. Botão para **Desarmar**
10. Botão do **Modo Noturno**
11. Botão de tamper anti-sabotagem
12. Botão de ligar/desligar
13. Código QR

Para retirar o painel SmartBracket, faça-o deslizar para baixo (a parte perfurada é necessária para acionar o tamper em caso de tentativa de arrancar o dispositivo da superfície).

Princípio de funcionamento

O KeyPad é um teclado tátil para gerir o sistema Ajax. Controla os modos de segurança de todo o objeto ou grupos individuais e permite ativar o **Modo Noturno**. O teclado suporta a função de “alarme silencioso” – o utilizador informa a empresa de segurança de que foi forçado a desarmar o sistema de segurança e não é exposto pelos sons da sirene ou pelas aplicações Ajax.

Pode controlar os modos de segurança com o KeyPad utilizando códigos. Antes de introduzir o código, é necessário ativar (“acordar”) o teclado tocando-lhe. Quando está ativado, a retroiluminação dos botões é ativada e o teclado emite um sinal sonoro.

O KeyPad suporta os seguintes tipos de códigos:




- **Código do teclado** — código geral configurado para o teclado. Quando utilizado, todos os eventos são enviados para apps Ajax em nome do teclado.
- **Código do utilizador** — código pessoal configurado para os utilizadores conectados ao hub. Quando utilizado, todos os eventos são entregues a apps Ajax em nome do utilizador.
- **Código de acesso do teclado** — 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 RRU** é um código de acesso às unidades de resposta rápida (RRU) 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, de acesso e RRU depende do modelo do hub.

O brilho da luz de fundo e o volume do teclado são ajustados nas suas configurações. Com as baterias descarregadas, a luz de fundo acende no nível mínimo, independentemente das configurações.

Se não tocar no teclado durante 4 segundos, o KeyPad reduz o brilho da luz de fundo e, 8 segundos depois, entra no modo de poupança de energia e desliga o ecrã. Quando o teclado entra no modo de poupança de energia, repõe os comandos introduzidos!

O teclado suporta códigos de 4 a 6 dígitos. A introdução do código deve ser confirmada premindo um dos botões:  (armar),  (desarmar) e  (**Modo Noturno**). Quaisquer caracteres digitados por engano são reiniciados com o botão **C** (**Reiniciar**).

O KeyPad também suporta o controlo dos modos de segurança sem introduzir um código, se a função «Armar sem código» estiver ativada nas definições. Esta função está desativada por defeito.

Botão de Função

O KeyPad possui um botão **Função** que opera em três modos:

- **Desligado** — o botão está desativado. Não acontece nada depois de clicar.
- **Alarme** — após premir o botão Função, o sistema envia um alarme para a central de monitoramento da empresa de segurança, para os utilizadores e ativa as sirenes conectadas ao sistema.
- **Silenciar alarmes de detetores de incêndio interligados** — após pressionar o botão Função, o sistema desativa as sirenes dos detectores de incêndio Ajax. A opção só funciona se a opção Alarmes FireProtect interligados estiver activada (Hub → Definições → Serviço → Definições dos detectores de incêndio).

Código de coação

O código de coação permite-lhe simular a desativação do alarme. Ao contrário do botão de pânico, se este código for introduzido, o utilizador não será comprometido pelo som da sirene e o teclado e a aplicação Ajax informarão sobre o desarmamento bem sucedido do sistema. Ao mesmo tempo, a empresa de segurança recebe um alarme.

Estão disponíveis os seguintes tipos de códigos de coação:

- **Código do teclado** — código geral de emergência. Quando utilizados, os eventos são enviados para aplicações Ajax em nome do teclado.
- **Código de emergência do utilizador** — código de emergência pessoal, definido para cada utilizador conectado ao hub. Quando utilizados, os eventos são entregues a aplicações Ajax em nome do utilizador.
- **Código de acesso do teclado** — código de emergência definido 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.

Saiba mais

Bloqueio automático de acesso não autorizado

Se for introduzido um código errado três vezes no espaço de 1 minuto, o teclado será bloqueado durante o tempo especificado nas definições. Durante este tempo, o hub ignorará todos os códigos e informará os utilizadores do sistema de segurança e o CMS sobre uma tentativa de adivinhar o código.

O teclado desbloqueia-se automaticamente após o fim do tempo de bloqueio definido nas definições. No entanto, o utilizador ou PRO com direitos de administrador pode desbloquear o teclado através da aplicação Ajax.

Armar em duas fases

O KeyPad participa no armar em duas fases. Quando esta função está activada, o sistema só será armado depois de ser rearmado com o SpaceControl ou depois de um detetor de segunda fase ser restaurado (por exemplo, fechando a porta da frente na qual o DoorProtect está instalado).

Saiba mais

Protocolo de transferência de dados do Jeweller

O teclado utiliza o protocolo de rádio Jeweller para transmitir eventos e alarmes. Este é um protocolo de transferência de dados sem fios bidirecional que proporciona uma comunicação rápida e fiável entre o hub e os dispositivos ligados.

Jeweller suporta encriptação de bloco com uma chave flutuante e autenticação de dispositivos em cada sessão de comunicação para evitar sabotagem e falsificação de dispositivos. O protocolo envolve a sondagem regular dos dispositivos pelo hub em intervalos de 12 a 300 segundos (definidos na aplicação Ajax) para monitorizar a comunicação com todos os dispositivos e apresentar os respectivos estados nas aplicações Ajax.

Mais informações sobre a tecnologia Jeweller

Envio de eventos para a central de monitorização

O sistema Ajax pode transmitir alarmes para a aplicação de monitorização PRO Desktop, bem como para a estação central de monitorização (CMS) através de SurGard (Contact ID), SIA (DC-09), ADEMCO 685 e outros protocolos proprietários. Consulte a lista de CMSs aos quais pode conectar o sistema Ajax aqui.

O KeyPad pode transmitir os seguintes eventos:

- Código sob coação introduzido.

- O botão de pânico é premido (se o botão de **função** funcionar no modo de botão de pânico).
- O teclado está bloqueado devido a uma tentativa de adivinhar um código.
- Alarme de tamper / restabelecimento.
- Perda/restauração da ligação do hub.
- O teclado está permanentemente desativado/ativado.
- Tentativa sem êxito de armar o sistema de segurança (com o controlo de integridade ativado).

Quando um alarme é recebido, o operador da estação de monitorização da empresa de segurança sabe o que aconteceu e para onde enviar a equipa de resposta rápida. A capacidade de endereçamento de cada dispositivo Ajax permite-lhe enviar não só eventos, mas também o tipo de dispositivo, o grupo de segurança, o nome que lhe foi atribuído e a divisão para o PRO Desktop ou para o CMS. A lista de parâmetros transmitidos pode variar consoante o tipo de CRA e o protocolo de comunicação selecionado.



A ID do dispositivo e o número do circuito (zona) podem ser encontrados nos seus estados na aplicação Ajax.

Indicação



Ao tocar no KeyPad, este acorda, realçando o teclado e indicando o modo de segurança: Armado, Desarmado ou Modo Noturno. O modo de



segurança é sempre atual, independentemente do dispositivo de controlo que foi utilizado para o alterar (o comando ou a aplicação).

De mascaramento	Indicação
O indicador X de avaria pisca	O indicador avisa da falta de comunicação com o hub ou da abertura da tampa do teclado. É possível verificar o motivo da avaria na aplicação <u>Ajax Security System</u>
Botão do teclado premido	Um breve sinal sonoro, o LED do estado de ativação atual do sistema pisca uma vez
O sistema está armado	Sinal sonoro curto, Modo Armado / Modo Noturno O indicador LED acende
O sistema está desarmado	Dois sinais sonoros curtos, o indicador LED do modo Desarmado acende
Código de acesso incorreto	Sinal sonoro longo, a retroiluminação do teclado pisca 3 vezes
É detectada uma avaria ao armar (por exemplo, o detetor é perdido)	Um sinal sonoro longo, o LED do estado de ativação atual do sistema pisca 3 vezes
O hub não responde ao comando — sem ligação	Sinal sonoro prolongado, o indicador Avaria acende
O teclado é bloqueado após 3 tentativas infrutíferas de introdução do código de acesso	Sinal sonoro longo, os indicadores do modo de segurança piscam simultaneamente
Bateria fraca	<p>Após armar/desarmar o sistema, o indicador Avaria pisca suavemente. O teclado está bloqueado enquanto o indicador estiver a piscar.</p> <p>Ao ativar o teclado com as pilhas fracas, ele emitirá um sinal sonoro prolongado, o indicador Avaria acenderá suavemente e, em seguida, desligar-se-á.</p>

Avisos sonoros de avarias

Se algum dispositivo estiver offline ou se a bateria estiver fraca, o KeyPad pode notificar os utilizadores do sistema com um som audível. Os LEDs dos teclados ficarão intermitentes. As notificações de avaria serão apresentadas no historial de eventos, no texto SMS ou na notificação push.

Para ativar as notificações sonoras de avarias, utilize as [apps](#) Ajax PRO e PRO Desktop:

1. Clique em **Dispositivos** , selecione o hub e abra as suas configurações :
Clique em **Serviço** → **Sons e Alertas**
2. Ative as alternâncias: **Se a bateria de qualquer dispositivo estiver fraca e Se qualquer dispositivo estiver offline.**
3. Clique **Voltar** duas vezes para guardar as definições.



As notificações sonoras das configurações de mau funcionamento estão disponíveis para todos os hubs (exceto o modelo Hub) com a versão de firmware OS Malevich 2.15 ou superior.

As notificações sonoras de avarias são suportadas pelo KeyPad com a versão de firmware 5.57.1.1 ou superior.

De mascaramento	Indicação	Nota
Se algum dispositivo estiver offline.	Dois sinais sonoros curtos, o indicador de Avaria X pisca duas vezes. Emite um sinal sonoro uma vez por minuto até que todos os dispositivos no sistema estejam online.	Os utilizadores podem atrasar a indicação sonora durante 12 horas.
Se o KeyPad estiver offline.	Dois sinais sonoros curtos, o indicador de Avaria X pisca duas vezes.	É impossível atrasar a indicação sonora.

	Emite um sinal sonoro uma vez por minuto até o teclado do sistema estar online.	
Se a bateria de qualquer dispositivo estiver fraca.	Três sinais sonoros curtos, o indicador de Avaria X pisca três vezes. Emite um sinal sonoro uma vez por minuto até a bateria ser restaurada ou o dispositivo ser removido.	Os utilizadores podem atrasar a indicação sonora durante 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.

Conexão



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 contactar o [Suporte Técnico da Ajax](#) para verificar as bandas de frequência de rádio na sua região.

Antes de ligar o dispositivo

1. Ligue o hub e verifique a sua ligação à Internet (o logótipo brilha a branco ou verde).
2. Instale a [app Ajax](#). Crie a conta, adicione o hub à aplicação e crie pelo menos uma divisão.
3. Certifique-se de que o hub não está armado e que não é atualizado, verificando o seu estado na aplicação Ajax.



Apenas utilizadores com direitos de administrador podem adicionar um dispositivo à aplicação.

Como ligar o KeyPad ao hub

1. Selecione a opção **Adicionar Dispositivo** na app Ajax.
2. Dê um nome ao dispositivo, leia/escreva manualmente o **código QR** (localizado no corpo e na embalagem) e selecione a sala de localização.
3. Clique em **Adicionar** — a contagem decrescente começará.
4. Ligue o KeyPad mantendo premido o botão de alimentação durante 3 segundos — este piscará uma vez com a retroiluminação do teclado.

Para que a deteção e o emparelhamento ocorram, o KeyPad deve estar localizado dentro da cobertura da rede sem fios do hub (no mesmo objeto protegido).

Um pedido de ligação ao hub é transmitido durante um curto período de tempo no momento em que o aparelho é ligado.

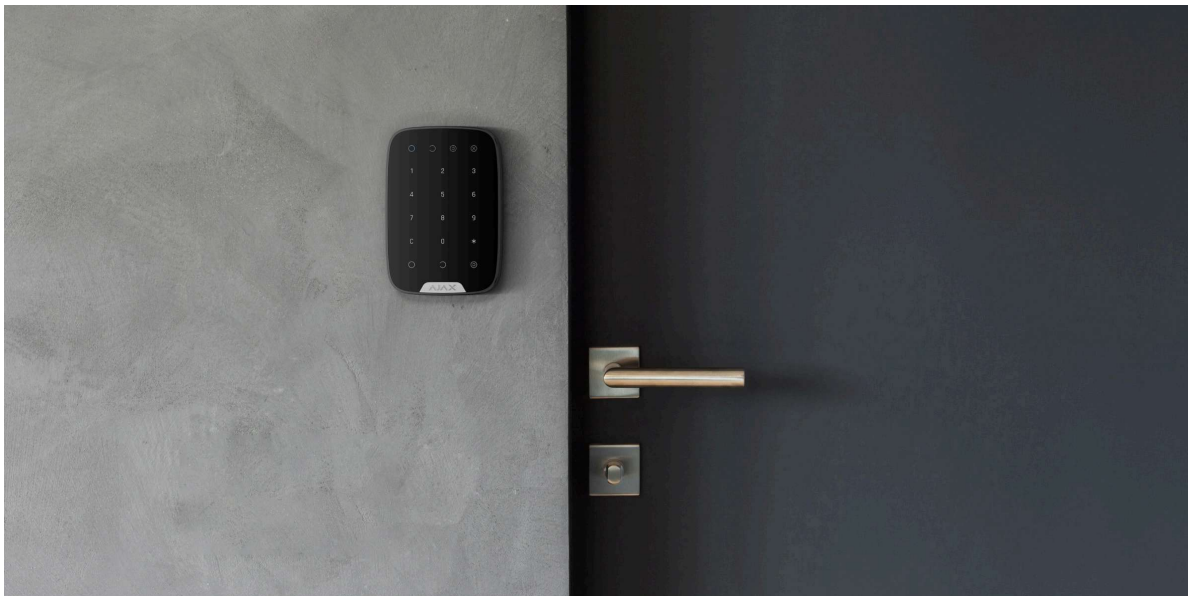
Se o KeyPad não conseguir ligar-se ao hub, desligue-o durante 5 segundos e tente novamente.

O dispositivo ligado aparecerá na lista de dispositivos da aplicação. A atualização do estado dos dispositivos na lista depende do intervalo de ping do detetor nas definições do hub (o valor predefinido é 36 segundos).



Não existem códigos pré-definidos para o KeyPad. Antes de utilizar o KeyPad, defina todos os códigos necessários: código do teclado (código geral), códigos de utilizador pessoal e códigos de coação (geral e pessoal).

Seleção do local



A localização do dispositivo depende da sua distância do hub e dos obstáculos que dificultam a transmissão do sinal de rádio: paredes, chão, objectos grandes dentro da sala.



O dispositivo foi desenvolvido apenas para utilização em interiores.

Não instalar o KeyPad:

1. Perto do equipamento de transmissão de rádio, incluindo o que funciona em redes móveis 2G/3G/4G, routers Wi-Fi, transceptores, estações de rádio, bem como um hub Ajax (utiliza uma rede GSM).
2. Perto de cabos eléctricos.
3. Perto de objectos metálicos e espelhos que possam causar atenuação ou sombreamento do sinal de rádio.
4. Fora das instalações (no exterior).
5. No interior de instalações com temperatura e humidade acima dos limites permitidos.
6. Mais perto de 1 m do hub.



Verificar a intensidade do sinal Jeweller no local de instalação

Durante o teste, o nível do sinal é exibido na aplicação e no teclado com indicadores de modo de segurança ○ (modo armado), ○ (modo desarmado), ○ (modo noturno) e indicador de mau funcionamento X.

Se o nível do sinal for baixo (uma barra), não podemos garantir o funcionamento estável do dispositivo. Tome as medidas possíveis para melhorar a qualidade do sinal. Pelo menos, desloque o aparelho: mesmo uma deslocação de 20 cm pode melhorar significativamente a qualidade da receção do sinal.

Se, após a deslocação, o dispositivo continuar a ter uma intensidade de sinal baixa ou instável, utilize um repetidor do sinal de rádio.

O KeyPad foi concebido para funcionar quando fixado numa superfície vertical. Ao utilizar o KeyPad nas mãos, não podemos garantir o funcionamento correto do teclado com sensor.

Estados

1. Dispositivos


2. KeyPad

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><u>Saiba mais</u></p>

Temperatura	<p>Temperatura do detetor. Medida no processador e muda gradualmente.</p> <p>Erro aceitável entre o valor na app e a temperatura ambiente – 2°C.</p> <p>O valor é atualizado assim que o dispositivo identifica uma variação de temperatura de, pelo menos, 2°C.</p> <p>É possível configurar um cenário por temperatura para controlar dispositivos de automatização.</p> <p><u>Saiba mais</u></p>
Intensidade de sinal Jeweller	Força do sinal entre o hub e o KeyPad.
Conexão	Estado da ligação entre o hub e o KeyPad.
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><u>Saiba mais</u></p>
Carga da bateria	<p>Nível da bateria do dispositivo . Dois estados disponíveis:</p> <ul style="list-style-type: none"> • OK. • Bateria descarregada. <p><u>Como a carga da bateria é apresentada nas apps Ajax</u></p>
Tampa	O modo de tamper do dispositivo, que reage ao desprendimento ou a danos no corpo.
ReX	Exibe o estado de utilização de um <u>repetidor de sinal de rádio</u> .


Desativação permanente	Mostra o estado do dispositivo: ativo, completamente desativado pelo utilizador ou apenas as notificações sobre o acionamento do botão de tamper do dispositivo estão desativadas.
Desativação Única	Mostra o estado da desativação do dispositivo até ao primeiro desarmamento: ativo, completamente desativado pelo utilizador ou apenas as notificações sobre a ativação da sabotagem do dispositivo estão desativadas.
Firmware	Versão do firmware do teclado.
ID do dispositivo	Identificador do dispositivo.


Definições


1. Dispositivos 

2. KeyPad

3. Definições 

Definição	Significado
Nome	Nome do dispositivo, pode ser editado.
Sala	Seleção da divisão virtual à qual o dispositivo está atribuído.
Gestão de grupos	<p>Seleção do grupo de segurança controlado pelo dispositivo. Pode selecionar todos os grupos ou apenas um.</p> <p>O campo é apresentado quando o <u>Modo de grupo</u> está ativado.</p> <div>  <p>Se a funcionalidade <u>Grupo seguido</u> estiver configurada para grupos, o seu estado de</p> </div>

	<div>segurança pode mudar automaticamente em função das suas definições e dos estados dos iniciadores.</div>
Access Settings	<p>Selecting the way of verification for arming/disarming:</p> <ul style="list-style-type: none"> • Keypad codes only. • User codes only. • Keypad and user codes. <div>  <p>To activate the Access Codes set up for people who are not registered in the system, select the options on the keypad: Keypad codes only or Keypad and user codes.</p> </div>
Definições de acesso	<p>Seleção do modo de verificação para armar/desarmar:</p> <ul style="list-style-type: none"> • Apenas códigos de teclado. • Apenas códigos de utilizador. • Códigos de teclado e de utilizador. <p>Para ativar os Códigos de Acesso configurados para pessoas que não estão registadas no sistema, selecione as opções no teclado: Apenas códigos do teclado ou Teclado e código do utilizador.</p>
Código do teclado	Definição de um código para armar/desarmar.

Código de coação	<p>Definir <u>um código de emergência para alarme silencioso</u>.</p>
Botão de função	<p>Seleção da função do botão</p> <ul style="list-style-type: none"> ● Desativado — o botão Função está desativado e não executa nenhum comando quando premido. ● Pânico — ao premir o botão Função, o sistema envia um alarme para a central de monitorização da empresa de segurança e para todos os utilizadores. ● Silenciar alarme dos detetores de incêndio interligados — quando premido, silencia o alarme dos <u>detetores de incêndio Ajax</u>. Esta funcionalidade só funciona se a opção <u>Alarmes de detetores de incêndio interligados</u> estiver ativada. <p><u>Saiba mais</u></p>
Proteção contra pressão accidental	<div>  <p>Disponível com <u>OS Malevich 2.31</u> ou posterior.</p> </div> <p>Quando ativado, o botão de Função deve ser premido duas vezes para enviar um alarme de pânico.</p> <p>Esta definição está disponível se o Botão de função estiver definido para Pânico.</p>
Armar sem código	<p>Se estiver ativo, o sistema pode ser armado premindo o botão Armar sem um código.</p>
Acesso não autorizado Bloqueio automático	<p>Se estiver ativo, o teclado é bloqueado durante o tempo predefinido após a introdução de um código incorreto três vezes seguidas no espaço de 1 minuto.</p>

	Durante este tempo, o sistema não pode ser desarmado através do KeyPad.
Tempo auto-bloquear, min	Período de bloqueio após tentativas erradas de introdução de um código.
Brilho	Brilho da retroiluminação do teclado.
Botões Volume	Volume do sinal sonoro.
Alerta com uma sirene se o botão de pânico for premido	<p>A configuração é exibida se o modo Alarme for selecionado para o botão Função.</p> <p>Se estiver ativo, o botão Função ao ser premido aciona as sirenes instaladas no objeto.</p>
Teste de Intensidade de Sinal de Jeweller.	Passa o dispositivo para o modo de teste da intensidade do sinal.
Teste de atenuação do sinal	Alterna o teclado para o modo de teste de atenuação do sinal (disponível em dispositivos com firmware versão 3.50 e posterior).
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 executa comandos do sistema nem participa em cenários de automatização; além disso, o sistema ignora alarmes e outras notificações do dispositivo. • Apenas tampa — o sistema ignora as notificações de ativação do tamper do dispositivo. <p>Saiba mais</p>
Desativação Única	Mostra o estado da definição de desativação única do teclado:

	<ul style="list-style-type: none"> • Não — o teclado funciona no modo normal. • Apenas tampa — as notificações sobre o acionamento de uma violação no teclado são desativadas até ao primeiro desarme. • Inteiramente — o teclado 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. <p><u>Saiba mais</u></p>
Guia do Utilizador	Abre o manual do utilizador do KeyPad.
Eliminar dispositivo	Desliga o dispositivo do hub e elimina as suas definições.

Configuração de códigos

O sistema Ajax permite-lhe definir um código de teclado, bem como códigos pessoais para os utilizadores adicionados ao hub.

Com a atualização **OS Malevich 2.13.1**, também adicionamos a capacidade de criar códigos de acesso para pessoas que não estão conectadas ao hub. Isto é conveniente, por exemplo, para dar a uma empresa de limpeza acesso à gestão da segurança. Veja abaixo como configurar e utilizar cada tipo de código.


Para definir o código do teclado

1. Aceda às definições do teclado.
2. Selecione **Código do teclado**.
3. Definir o código de teclado pretendido.

Para definir o código de coação do teclado

1. Aceda às definições do teclado.
2. Selecione **Código de Coação**.
3. Defina o código de coação do teclado que pretende.


Para definir um código pessoal para um utilizador registado:

1. Aceda às definições do perfil: Hub → **Definições**  → **Utilizadores** → **Definições do utilizador**. Neste menu, também pode encontrar o ID do utilizador.
2. Clique em **Configurações de código de acesso**.
3. Defina o **Código do Utilizador** e o **Utilizador Código de Coação**



Cada utilizador define um código pessoal individualmente!

Para definir um código de acesso para uma pessoa não registada no sistema

1. Aceda às definições do hub (**Hub** → **Definições** ).
2. Selecione **Códigos de acesso do Keypad**.
3. Configure **Nome** e **Código de Acesso**.

Se pretender configurar um código de coação, alterar as definições de acesso a grupos, Modo Noturno, ID do código, desativar temporariamente ou eliminar este código, selecione-o na lista e efectue as alterações.



Utilizador PRO ou um utilizador com direitos de administrador pode definir um código de acesso ou alterar as suas definições. Esta função é suportada por hubs com OS Malevich 2.13.1 e superior. Os códigos de acesso não são suportados pelo painel de controlo do Hub.

Para definir o código RRU

Apenas um PRO com direitos de configuração do sistema pode criar e configurar os códigos URR nas apps Ajax PRO. Para mais informações sobre a configuração desta funcionalidade, consulte [este artigo](#).



Os códigos RRU são suportados pelos hubs (exceto o modelo Hub) com o sistema operativo Malevich 2.17 e superior.

Controlo da segurança através de códigos

É possível controlar a segurança de toda a instalação ou de grupos separados através de códigos gerais, pessoais ou RRU, bem como através de códigos de acesso (configurados pelo PRO ou por um utilizador com direitos de administrador).




Se for utilizado um código de utilizador pessoal, o nome do utilizador que armou/desarmou o sistema é apresentado nas notificações e no historial de eventos do hub. Se for utilizado o código RRU — é apresentado o título do código RRU. Se for utilizado um código geral, o nome do utilizador que alterou o modo de segurança não é apresentado.



Os códigos de acesso do Keypad são suportados por hubs (exceto o modelo Hub) com OS Malevich 2.13.1 e superior. O painel de controlo do hub não suporta esta função.

Os códigos RRU são suportados pelos hubs (exceto o modelo Hub) com o sistema operativo Malevich 2.17 e superior.


Gestão da segurança de toda a instalação através de um código geral

Introduza o **código geral** e prima a tecla **armar**  / **desarmar**  / **ativar modo noturno** .

Por exemplo: 1234 → 

Gestão da segurança do grupo com um código geral

Introduza o **código geral**, prima a tecla *****, introduza o **ID do grupo** e prima a tecla **armar**  / **desarmar**  / **ativar o modo noturno** tecla .

Por exemplo: 1234 → * → 2 → 

O que é a ID de grupo




Se um grupo estiver atribuído ao KeyPad (campo **Permissão de armar/desarmar** nas definições do teclado), não é necessário introduzir o ID do grupo. Para gerir o modo de armar deste grupo, basta introduzir um código de utilizador geral ou pessoal.


Por favor, observe que, se um grupo estiver atribuído ao KeyPad, não será possível gerir o **Modo Noturno** utilizando um código geral.

Neste caso, o **Modo Noturno** só pode ser gerido utilizando um código de utilizador pessoal (se o utilizador tiver os direitos apropriados).

Direitos no sistema Ajax

Gestão da segurança de toda a instalação através de um código pessoal

Introduza o **ID do utilizador** *****, prima , introduza o **código pessoal do utilizador** e prima **armar**  / **desarmar**  / **ativação do modo noturno** tecla .

Por exemplo: 2 → * → 1234 → 

O que é o ID de utilizador

Gestão da segurança do grupo através de um código pessoal

Introduza o **ID do utilizador** *, prima , introduza o **código pessoal do utilizador** *, prima , introduza o **ID do grupo** e prima **armar** ○ / **desarmar** ○ / **ativar o Modo Noturno** ☹.

Por exemplo: 2 → * → 1234 → * → 5 → ○

O que é a ID de grupo

O que é o ID de utilizador

Se um grupo estiver atribuído ao KeyPad (campo **Permissão de armar/desarmar** nas definições do teclado), não é necessário introduzir o ID do grupo. Para gerir o modo de armar deste grupo, basta introduzir um código de utilizador pessoal.

Controlo de segurança de todo o objeto através de um código de acesso

Introduza o **código de acesso** e prima a tecla **armar** ○ / **desarmar** ○ / **ativação do modo noturno** ☹.

Por exemplo: 1234 → ○

Gestão da segurança do grupo através de um código de acesso

Introduza o **código de acesso**, prima a tecla *, introduza o **ID do grupo** e prima a tecla **armar** ○ / **desarmar** ○ / **ativação do modo noturno** ☹.

Por exemplo: 1234 → * → 2 → ○

O que é a ID de grupo

Utilização do código de coação

O **Código de Coação** permite que se acione um alarme silencioso e simule a desativação do alarme. Um alarme silencioso significa que a aplicação Ajax e as sirenes não irão soar e expô-lo. No entanto, uma empresa de segurança e outros utilizadores serão alertados instantaneamente. Pode utilizar códigos de coação **personais** e **gerais**. Também pode configurar um código de acesso de coação para pessoas não registadas no sistema.


O que é um código de coação e como utilizá-lo




Os cenários e as sirenes reagem ao desarme sob coação da mesma forma que ao desarme normal.


Para utilizar um código de coação geral:

Introduza o **código de emergência geral** e prima o botão **desarmar** .

Por exemplo: 4321 → .

To Para utilizar um código de emergência pessoal de um utilizador registado:

Introduza **ID do utilizador**, prima *****, introduza o **código de emergência pessoal** e prima o botão **desarmar** .

Por exemplo: 2 → ***** → 4422 → .

Para utilizar um código de emergência de uma pessoa não registada no sistema:

Introduza o **código de emergência** definido em **Códigos de acesso do teclado** e prima o botão **desarmar** .




Por exemplo: 4567 → .

Utilização do código URR

O código URR é ativado após o disparo do alarme durante o tempo configurado nas definições do hub, e é válido por um período especificado. Isto garante que este código só será utilizado em caso de risco, ao contrário dos códigos de teclado ou de utilizador.




Como configurar o código URR


Controlo de segurança do objeto através do código URR:

Introduza o **Código RRU** e prima o botão **armar**  / **desarmar**  / **ativação do Modo Noturno** .

Por exemplo: 1234 → 

Controlo de segurança do grupo através do código URR:

Introduza o **Código RRU**, prima *****, digite o **ID do Grupo**, e prima o botão **armar**  / **desarmar**  / **ativação do modo noturno** .

Por exemplo: 1234 → * → 2 → 

Como funciona a função de silenciamento do alarme de incêndio

Utilizando o KeyPad, pode silenciar o alarme dos detetores de incêndio interligados, premindo o botão Função (se a configuração correspondente estiver ativada). A reação do sistema ao premir um botão depende do estado do sistema:

- **Os alarmes dos detetores de incêndio interligados já se propagaram** — ao premir pela primeira vez o botão Função, 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 Função, a sirene dos detetores de incêndio Ajax acionados é

silenciada.

Saiba mais sobre alarmes de detetores de incêndio interligados



Com a atualização do [OS Malevich 2.12](#), os utilizadores podem silenciar alarmes de incêndio nos seus grupos sem afetar os detetores nos grupos aos quais não têm acesso.

[Saiba mais](#)

Teste de funcionalidade

Um sistema de segurança Ajax permite efetuar testes para verificar a funcionalidade dos dispositivos ligados.

Os testes não se iniciam imediatamente, mas num período de 36 segundos, quando se utilizam as definições padrão. O início do tempo de teste depende das configurações do período de varredura do detetor (o parágrafo sobre configurações **Jeweller** nas configurações do hub).

Teste de intensidade do sinal do Jeweller

Teste de atenuação do sinal

Instalação



Antes de instalar o detetor, certifique-se de que selecionou o local ideal e que este está em conformidade com as diretrizes contidas neste manual.



O KeyPad deve ser fixado à superfície vertical.

1. Prenda o painel SmartBracket à superfície utilizando os parafusos fornecidos, utilizando pelo menos dois pontos de fixação (um deles

acima do tamper) Depois de selecionar outras ferragens de fixação, certifique-se de que estas não danificam ou deformam o painel.



O dispositivo foi desenvolvido apenas para utilização em interiores. A fita irá secar com o tempo, o que pode resultar na queda do KeyPad e danos ao dispositivo.

2. Coloque o KeyPad no painel de fixação e aperte o parafuso de montagem na parte inferior do corpo.

Assim que o KeyPad estiver fixado no SmartBracket, ele piscará com o LED **X** (Falha) — isso será um sinal de que a sabotagem foi acionada.

Se o indicador de avaria não piscar **X** após a instalação no SmartBracket, verifique o estado da sabotagem na aplicação Ajax e, em seguida, verifique se o painel está bem fixo.

Se o KeyPad for arrancado da superfície ou removido do painel de fixação, receberá uma notificação.

Manutenção do KeyPad e substituição da bateria

Verifique regularmente o funcionamento do KeyPad.

A bateria instalada no KeyPad garante até 2 anos de funcionamento autónomo (com a frequência de consulta pelo hub de 3 minutos). Se a bateria do KeyPad estiver fraca, o sistema de segurança enviará os avisos relevantes e o indicador de avaria acender-se-á suavemente e apagar-se-á após cada introdução de código bem sucedida.

Qual é a autonomia das baterias dos dispositivos Ajax e o que pode afetar a sua autonomia

Substituição da bateria

Características técnicas

Todas as especificações técnicas do KeyPad Jeweller

Conformidade com as normas

Garantia

A garantia dos produtos da sociedade de responsabilidade limitada “Ajax Systems Manufacturing” é válida durante 2 anos após a compra.

Se o dispositivo não funcionar corretamente, contacte primeiro o Apoio Técnico Ajax. Na maioria dos casos, os problemas técnicos podem ser resolvidos remotamente.

Obrigações de garantia

Acordo de Utilizador

Contactar o Suporte Técnico Ajax

- email
- Telegram