Manual do Usuário

Placa Controladora C2-260

Data: Outubro de 2023

Versão do Documento: 1.1

Português

Obrigado por escolher nosso produto. Por favor, leia atentamente as instruções antes de operá-lo. Siga estas instruções para garantir o correto funcionamento do produto. As imagens mostradas neste manual são apenas ilustrativas.

Para obter mais informações, visite o site da nossa empresa em www.zkteco.com.

Copyright © 2022 ZKTECO CO., LTD. Todos os direitos reservado.

Marca registrada

ZKTeco é uma marca registrada da ZKTeco. Outras marcas mencionadas neste manual são propriedades de seus respectivos proprietários.

Responsabilidade

Este manual contém informações sobre a operação e manutenção dos produtos ZKTeco. Os direitos de propriedade intelectual de todos os documentos, desenhos, etc., em relação aos produtos fornecidos pela ZKTeco são de propriedade da ZKTeco. O conteúdo deste documento não deve ser usado ou compartilhado pelo receptor com terceiros sem a permissão expressa por escrito da ZKTeco.

O conteúdo deste manual deve ser lido na íntegra antes de iniciar a utilização e manutenção do produto adquirido. Se algum dos conteúdos do manual parecer pouco claro ou incompleto, entre em contato com a ZKTeco antes de iniciar a utilização e/ou manutenção do referido produto.

É um pré-requisito essencial para a operação e/ou manutenção corretas/adequadas, que a equipe que irá utilizar e/ou dar manutenção, esteja totalmente familiarizado com o projeto e que esta equipe tenha recebido um treinamento completo da utilização e/ou manutenção da máquina / unidade / produto. É ainda essencial para a utilização segura da máquina / unidade / produto que a equipe tenha lido, compreendido e seguido as instruções de segurança contidas no manual.

Em caso de qualquer conflito entre os termos e condições deste manual e as especificações de fichas-técnicas, desenhos, folhas de instruções ou quaisquer outros documentos acordados entre as partes relacionados ao produto, as condições de tais documentos devem prevalecer em relação ao manual.

A responsabilidade da ZKTeco em relação ao presente manual e ao produto está detalhada nos termos de sua respectiva Garantia.

A ZKTeco reserva-se o direito de adicionar, apagar, alterar ou modificar as informações contidas no manual de tempos em tempos, independente de aviso prévio, por meio de circulares, cartas, notas e/ou novas edições do manual, visando a melhor utilização e/ou segurança do produto. Os mais recentes procedimentos de utilização e documentos relevantes estão disponíveis em http://www.zkteco.com.br sendo de responsabilidade do usuário verificar eventuais atualizações e informes, especialmente se o produto indicar problemas no funcionamento ou se restarem dúvidas sobre sua instalação, manejo, armazenamento, operação e/ou manutenção.

Se houver algum problema relacionado ao produto, entre em contato conosco.

ZKTeco Filial Brasil

Endereço **Vespasiano:** Rodovia MG-010, KM 26 - Loteamento 12 - Bairro Angicos, Vespasiano - MG | CEP: 33.206-240

Telefone (31) 3055-3530

Para questões comerciais, por favor entre em contato conosco pelo e-mail: comercial.brasil@zkteco.com
Para saber mais sobre nossas filiais globais, visite www.zkteco.com

Sobre a Empresa

A ZKTeco é um dos maiores fabricantes do mundo de leitores RFID e biométricos (impressão digital, facial, veia do dedo). A oferta de produtos inclui leitores e painéis de controle de acesso, câmeras de reconhecimento facial de alcance próximo e remoto, controladores de acesso a elevadores/andares, torniquetes, controladores de portões de reconhecimento de placas de veículos (LPR) e produtos de consumo, incluindo fechaduras de porta com bateria operada com leitor de impressão digital e facial. Nossas soluções de segurança são multilíngues e localizadas em mais de 18 idiomas diferentes. Na moderna instalação de fabricação da ZKTeco, certificada pela ISO9001 e com 700.000 pés quadrados, controlamos a fabricação, o design do produto, a montagem de componentes e a logística/ envio, tudo sob um mesmo teto.

Os fundadores da ZKTeco estabeleceram a determinação de pesquisa e desenvolvimento independentes de procedimentos de verificação biométrica e a produção em série de SDK de verificação biométrica, que inicialmente foram amplamente aplicados em segurança de PC e campos de autenticação de identidade. Com o contínuo aprimoramento do desenvolvimento e muitas aplicações de mercado, a equipe gradualmente construiu um ecossistema de autenticação de identidade e um ecossistema de segurança inteligente, que são baseados em técnicas de verificação biométrica. Com anos de experiência na industrialização de verificações biométricas, a ZKTeco foi oficialmente estabelecida em 2007 e agora é uma das principais empresas do mundo na indústria de verificação biométrica, possuindo várias patentes e sendo selecionada como Empresa Nacional de Alta Tecnologia por 6 anos consecutivos. Seus produtos são protegidos por direitos de propriedade intelectual.

Sobre o Manual

Este manual apresenta as operações da **Placa Controladora C2-260.**

Todas as imagens exibidas são apenas para fins ilustrativos. As imagens neste manual podem não ser exatamente consistentes com os produtos reais.

Convenções do Documento

As convenções utilizadas neste manual estão listadas abaixo:

Convenções de Interface Gráfica do Usuário:

Para o software	
Convenção	**Descrição**
Bold	Utilizado para identificar nomes de interfaces de software, por exemplo, **OK, Confirmar, Cancelar.**
>	Os menus de vários níveis são separados por estes parêntesis. Por exemplo, Ficheiro > Criar > Pasta.
Para o dispositivo	
Convenção	**Descrição**
< >	Nomes de botões ou teclas para dispositivos. Por exemplo, pressione <OK>.
[ ]	Os nomes de janelas, itens de menu, tabelas de dados e nomes de campos estão entre colchetes. Por exemplo, abra a janela [Novo usuário].
/	Os menus de vários níveis são separados por barras inclinadas. Por exemplo, [Arquivo/Criar/Pasta].

Símbolos

Convenção	Descrição
	Isso representa uma nota à qual é preciso dar mais atenção.
	As informações gerais que ajudam a realizar as operações mais rapidamente.
	As informações que são importantes.
	Cuidados a tomar para evitar perigos ou erros.
	A declaração ou o evento que alerta sobre algo ou que serve como exemplo de advertência.

Índice

1 INSTRUÇÕES DE SEGURANÇA 6
1.1 Instruções de Segurança Importantes 6
1.2 Instruções de Instalação 7
2 INTRODUÇÃO AO SISTEMA 9
2.1 Parâmetros Funcionais do Sistema 9
2.2 Parâmetros Técnicos do Produto 9
2.3 Indicadores do Painel de Controle 9
3 INSTALAÇÃO E CONEXÃO 11
3.1 Procedimento de Instalação 11
3.2 Instalação dos Fios de Painel de Controle de Acesso 12
3.3 Instalação do Sistema de Painel de Controle 13
3.4 Terminais de Conexão do Painel de Controle 14
3.5 Conexão com Sensores de Porta, Interruptores de Saída, Dispositivos de Entrada Auxiliar e Comunicação de Extensão RS485 15
3.6 Conexão com Leitores RS485/Wiegand 18
3.7 Conexão de Saída de Relé 20
4 COMUNICAÇÃO DE EQUIPAMENTOS 22
4.1 Fiação e Conexões de Rede de Controle de Acesso 22
4.2 Comunicação TCP/IP 23
4.3 ZKPanelWeb 23
5 ZKBIOACCESS 28
5.1 Login 28
5.2 Ativar o Sistema 28
5.3 Modificar Senha 28
5.4 Dispositivo 29
5.4.1 Adicionando um Dispositivo 30
5.4.2 Placa de E/S 34
5.4.3 Operação do Dispositivo 35
5.5 Adicionar um Usuário e um Cartão 42
5.6 Configurações de Controle de Acesso 47
5.7 Monitoramento em Tempo Real 47
5.8 Relatórios 51
APÊNDICE 1 53
Demonstração Operacional de Conexão da C2-260, WR485 e Leitor Wiegand 53
APÊNDICE 2 58
Declaração sobre o Direito à Privacidade 58
Operação Ecologicamente Correta 59
Garantia 60

1 Instruções de Segurança

1.1 Instruções de Segurança Importantes

1. Leia e siga cuidadosamente as instruções antes da operação. Por favor, mantenha as instruções para referência futura.
2. Acessórios: Por favor, utilize os acessórios recomendados pelo fabricante ou fornecidos com o produto. Outros acessórios não são recomendados, incluindo sistemas de alarme e sistemas de monitoramento principais. O sistema principal de alarme e monitoramento deve estar em conformidade com os padrões locais aplicáveis de prevenção contra incêndios e segurança.
3. Cuidados na instalação: Não coloque este equipamento em uma mesa, tripé, suporte ou base instáveis, para que o equipamento não caia e seja danificado ou ocorram quaisquer outros resultados indesejáveis que possam causar lesões pessoais graves. Portanto, é essencial instalar o equipamento conforme as instruções do fabricante.
4. Todos os dispositivos periféricos devem ser aterrados.
5. Nenhum fio de conexão externa pode ficar exposto. Todas as conexões e extremidades ociosas dos fios devem ser envolvidas com fitas isolantes para evitar qualquer dano ao equipamento por contato acidental com os fios expostos.
6. Reparo: Não tente fazer reparos não autorizados no equipamento. Desmontar ou desacoplar é arriscado e pode causar choque elétrico. Todos os reparos devem ser feitos por um técnico qualificado.
7. Se ocorrer algum dos seguintes casos, desconecte primeiro a fonte de alimentação do equipamento e avise imediatamente o técnico.
   - *O cabo de alimentação ou conector está danificado.*
   - *Qualquer líquido ou material derramado no equipamento.*
   - *O equipamento está molhado ou exposto a condições climáticas adversas (chuva, neve, etc.).*
   - *Se o equipamento não funcionar corretamente, mesmo se operado conforme as instruções, ajuste apenas os componentes de controle especificados nas instruções de operação. Ajustes incorretos em outros componentes de controle podem danificar o equipamento e até mesmo impedir seu funcionamento permanente.*
   - *O equipamento cair ou sua performance mudar drasticamente.*
8. Substituição de componentes: Se for necessário substituir um componente, apenas o técnico autorizado pode substituir os acessórios especificados pelo fabricante.
9. Inspeção de segurança: Após o reparo do equipamento, o técnico deve realizar uma inspeção de segurança para garantir o funcionamento adequado do equipamento.

10. Fonte de alimentação: Opere o equipamento apenas com o tipo de fonte de alimentação indicado na etiqueta. Entre em contato com o técnico em caso de qualquer dúvida sobre o tipo de fonte de alimentação.

O desrespeito a qualquer uma das seguintes precauções pode resultar em lesões pessoais ou falha do equipamento. Não seremos responsáveis pelos danos ou lesões causados por isso.

- Antes da instalação, desligue o circuito externo (que fornece energia ao sistema), incluindo fechaduras.
- Antes de conectar o equipamento à fonte de alimentação, verifique se a tensão de saída está dentro da faixa especificada.
- Nunca conecte a energia antes de concluir a instalação.

1.2 Instruções de Instalação

1. Os conduítes de fios sob o relé devem ser compatíveis com conduítes metálicos; outros fios podem utilizar conduítes de PVC para evitar falhas causadas por danos de roedores. O painel de controle possui funções adequadas de proteção contra eletricidade estática, raios e vazamentos; certifique-se de que seu chassi e o fio de aterramento AC estejam corretamente conectados e que o fio de aterramento AC esteja fisicamente aterrado.
2. É recomendado não conectar/desconectar terminais de conexão frequentemente quando o sistema estiver ligado. Certifique-se de desconectar os terminais de conexão antes de iniciar qualquer trabalho de solda relevante.
3. Não remova ou substitua qualquer chip do painel de controle sem permissão, pois uma operação não autorizada pode causar danos ao painel de controle.
4. É recomendado não conectar quaisquer outros dispositivos auxiliares sem permissão. Todas as operações não rotineiras devem ser comunicadas antecipadamente aos nossos engenheiros.
5. Um painel de controle não deve compartilhar a mesma tomada de energia com qualquer outro dispositivo de alto consumo de corrente.
6. É preferível instalar leitores de cartão e botões a uma altura de 1,4 a 1,5 metros do chão, ou de acordo com a prática usual dos clientes para ajuste adequado.
7. É aconselhável instalar os painéis de controle em locais de fácil manutenção, como uma sala elétrica fraca.
8. É altamente recomendado que a parte exposta de qualquer terminal de conexão não seja superior a 4 mm, e ferramentas de fixação especializadas podem ser utilizadas para evitar curto-circuito ou falha de comunicação resultante do contato acidental com fios excessivamente expostos.
9. Para salvar registros de eventos de controle de acesso, exporte os dados periodicamente dos painéis de controle.
10. Prepare medidas de contingência de acordo com os cenários de aplicação para falhas de energia inesperadas, como selecionar uma fonte de alimentação com UPS (sistema de alimentação ininterrupta).

11. Se um leitor RS485 for conectado externamente e compartilhar a fonte de alimentação com o dispositivo (o painel de controle não suporta verificação de impressão digital de leitores RS485), é recomendado que a conexão entre a porta do leitor RS485 e o leitor não ultrapasse 100 metros. Caso contrário, é recomendado que o leitor utilize uma fonte de alimentação separada.
12. Para proteger o sistema de controle de acesso contra a força eletromotriz autoinduzida gerada por uma fechadura eletrônica no momento da ligação/desligamento, é necessário conectar um diodo em paralelo (utilize o FR107 fornecido com o sistema) com a fechadura eletrônica para liberar a força eletromotriz autoinduzida durante a conexão no local para aplicação do sistema de controle de acesso.
13. É recomendado que uma fechadura eletrônica e um painel de controle utilizem fontes de alimentação separadas.
14. É recomendado utilizar a fonte de alimentação fornecida com o sistema como fonte de alimentação do painel de controle.
15. Em locais com interferência magnética significativa, é recomendado o uso de tubos de aço galvanizado ou cabos blindados, e é necessário um aterramento adequado.

2 Introdução ao Sistema

O sistema de gerenciamento de controle de acesso é um novo sistema de gerenciamento de segurança modernizado, que é uma medida eficaz de gerenciamento de segurança e proteção. Ele é principalmente usado para gerenciar as entradas e saídas de lugares altamente seguros, como bancos, hotéis, salas de equipamentos, escritórios, comunidades inteligentes e fábricas.

2.1 Parâmetros Funcionais do Sistema

- CPU de 32 bits de alta velocidade de 1,0 GHz e 64 MB de RAM.
- Sistema operacional EMBEDDED LINUX.
- Duas portas unidirecionais/bidirecionais.
- Capacidade de usuário: 30.000.
- Um máximo de 30.000 titulares de cartão.
- 200.000 registros de eventos offline.
- Utiliza tecnologias de comunicação Ethernet para comunicações confiáveis.
- Painel de controle com watchdog (hardware) integrado para evitar falhas.
- Proteção contra sobrecorrente, sobretensão e inversão de tensão para a entrada da fonte de alimentação do painel de controle.
- Proteção contra sobrecorrente para a fonte de alimentação dos leitores de cartão.
- Proteção instantânea contra sobretensão para todas as portas de entrada/saída.
- Proteção instantânea contra sobretensão para as portas de comunicação.

2.2 Parâmetros Técnicos do Produto

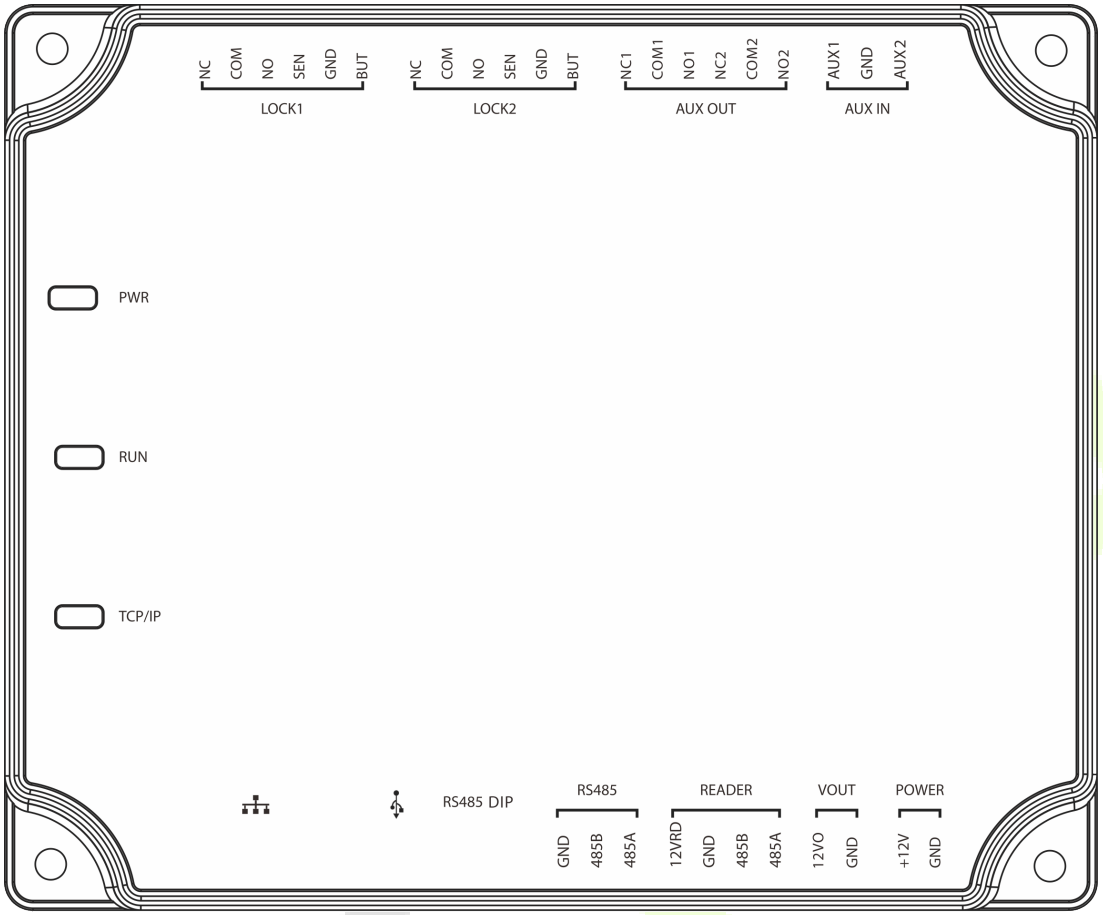
- Fonte de alimentação de trabalho: Tensão nominal de 12V (±20%) DC, corrente nominal é ≥ 3A.
- Ambiente de trabalho: Temperatura de -10°C a 50°C; Umidade de 20% a 80%.
- Saída do relé de trava eletrônica: Tensão máxima de comutação de 36V(DC); Corrente máxima de comutação de 5A.
- Saída de relé auxiliar: Tensão máxima de comutação de 36V(DC); Corrente máxima de comutação de 2A.
- Os terminais de conexão removíveis são feitos de materiais de flange não magnético de aço-liga.
- Dimensões do painel de controle: 116,5 mm * 96,5 mm * 31,3 mm.

2.3 Indicadores do Painel de Controle

Quando a C2-260 é ligada, normalmente o indicador de ENERGIA (vermelho) fica aceso constantemente, o indicador de EXECUÇÃO (verde) piscará lentamente (indicando que o sistema está normal), e os demais indicadores estarão desligados.

Indicador de COMUNICAÇÃO (amarelo): Ele piscará quando o sistema estiver se comunicando com outros dispositivos (por exemplo, PC). Quando o indicador estiver piscando continuamente, isso indica transmissão de dados. Quando o indicador estiver piscando lentamente, isso indica o status de monitoramento em tempo real.

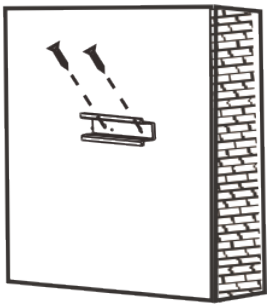
Diagrama de indicadores:

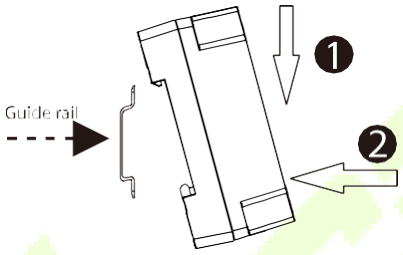


3 Instalação e Conexão

3.1 Procedimento de Instalação

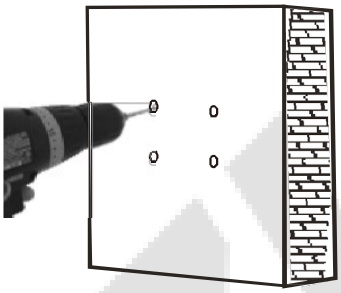
- A seguir, descreve-se o processo de instalação do trilho.

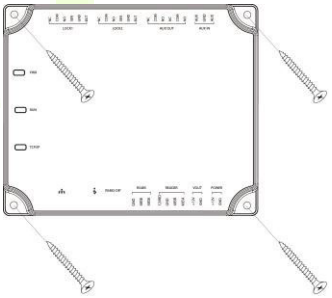




1) Fixe o trilho guia na parede. ⋯▶ 2) Fixe o dispositivo ao trilho guia.

- A seguir, descreve-se o processo de instalação na parede.





1) Faça furos na parede. ⋯▶ 2) Faça furos na parede.

3.2 Instalação dos fios do Painel de Controle de Acesso

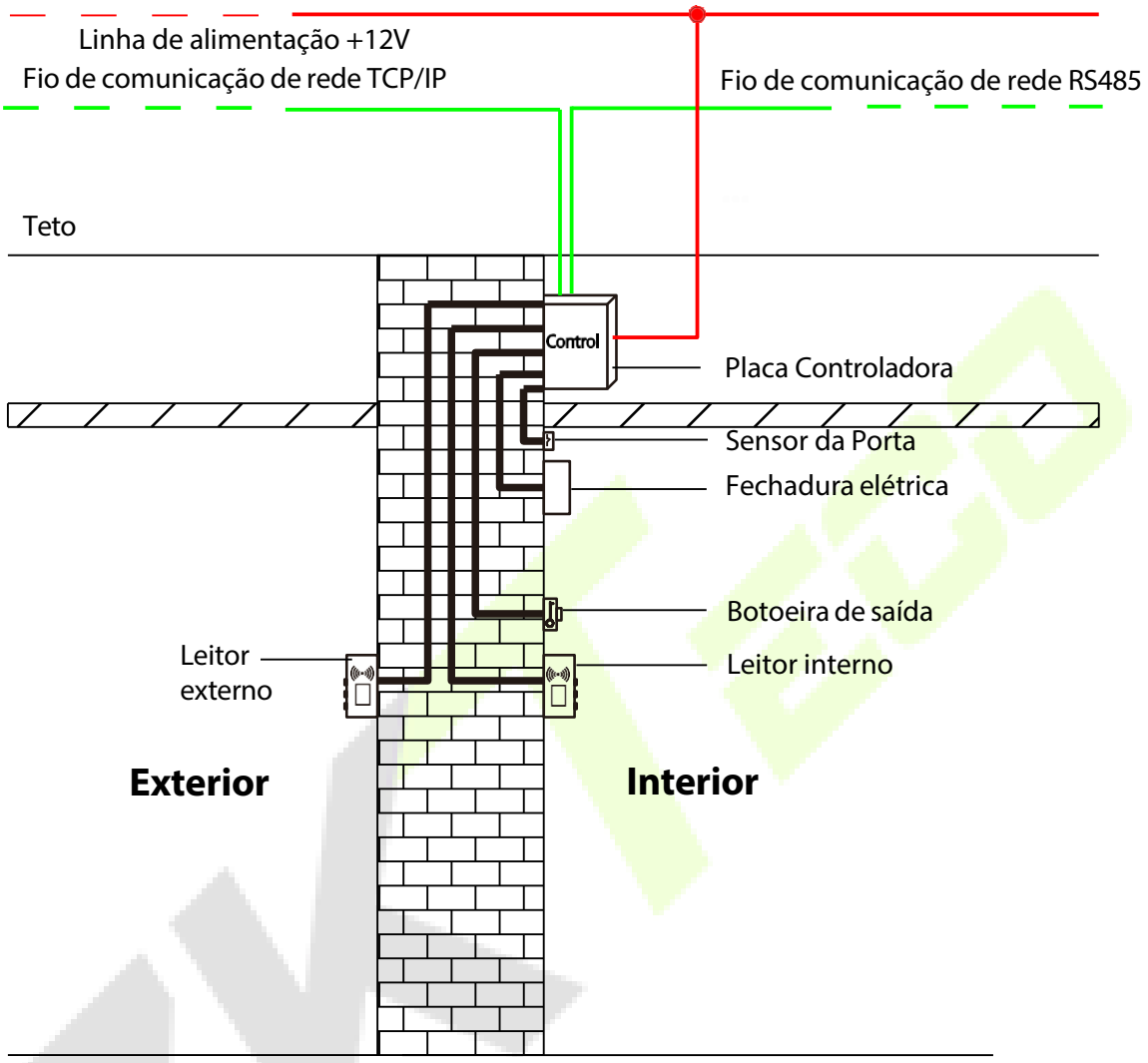


Diagrama de instalação dos fios do Painel de Controle de Acesso

Observações:

- Certifique-se de que a alimentação esteja desconectada antes de conectar os fios; caso contrário, pode causar danos graves ao equipamento.
- Os fios de controle de acesso devem ser separados de acordo com corrente pesada e leve; os fios do painel de controle, os fios da fechadura eletrônica e os fios do botão de saída devem passar por suas respectivas tubulações de proteção.

3.3 Instalação do Sistema de Painel de Controle

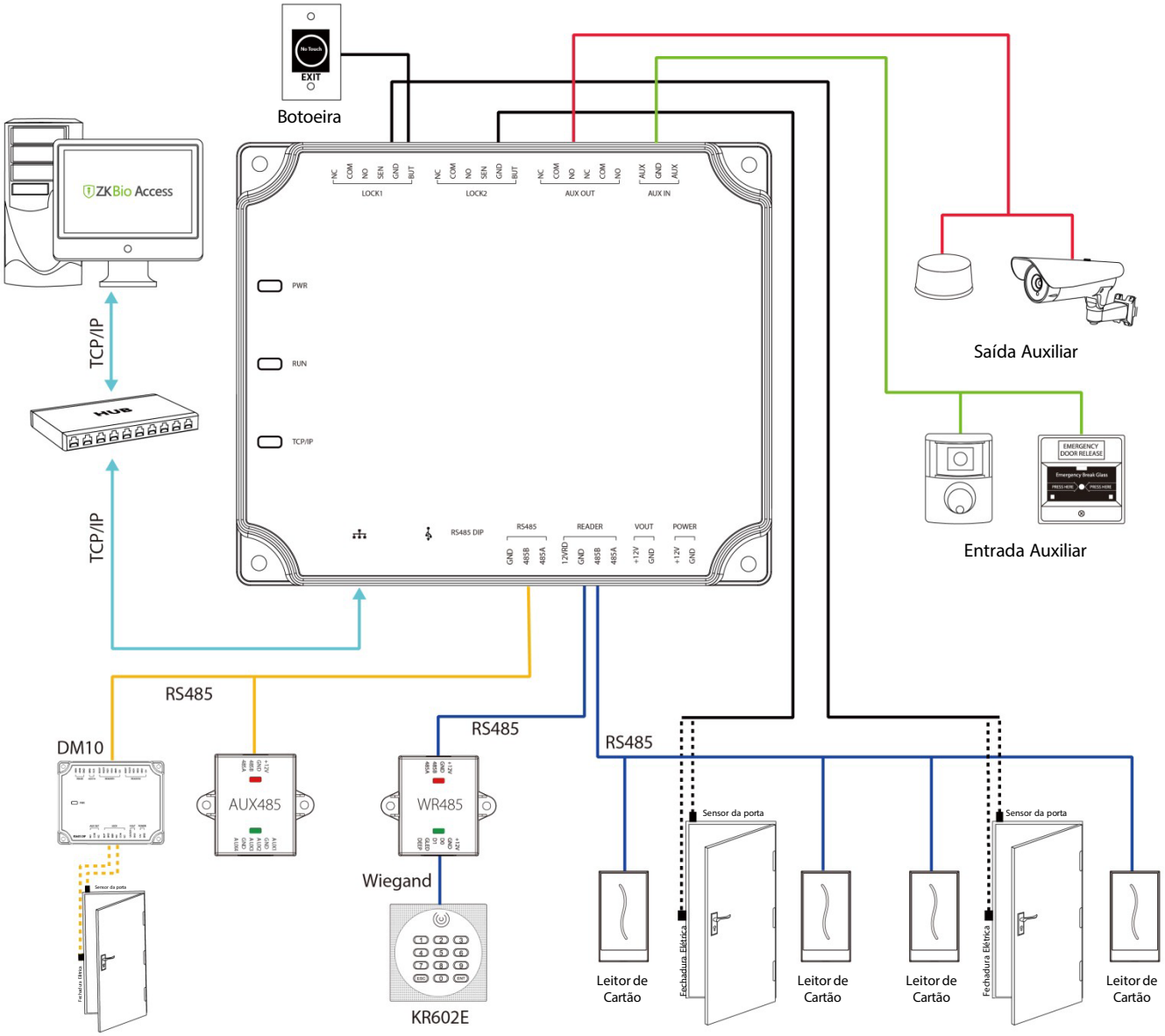


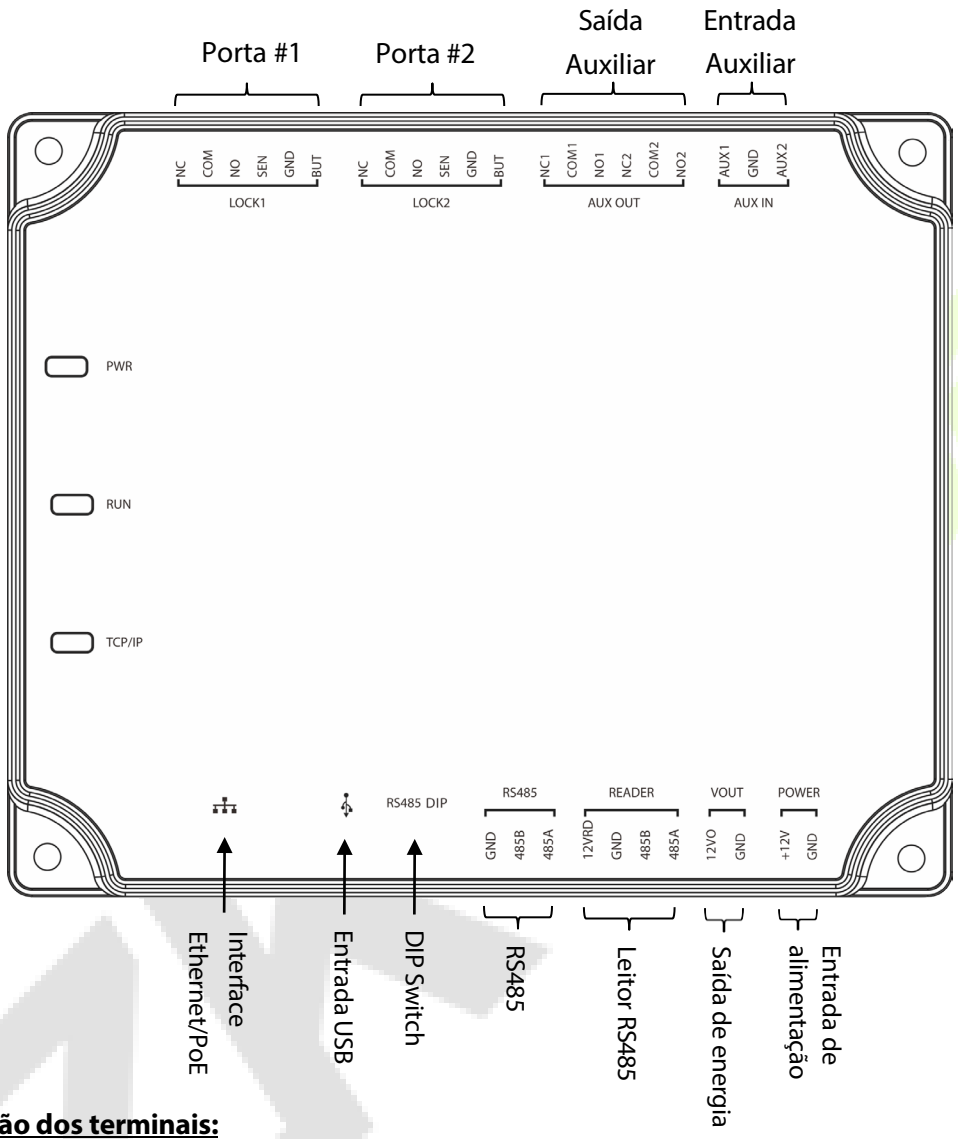
Diagrama Esquemático da Instalação do Sistema

O sistema de gerenciamento de controle de acesso consiste em duas partes: Estação de Trabalho de Gerenciamento (PC) e Painel de Controle. A estação de trabalho de gerenciamento e o painel de controle se comunicam por meio de redes TCP/IP e RS485. Os cabos de comunicação devem ser mantidos afastados de cabos de alta voltagem, tanto quanto possível, e não devem ser roteados em paralelo ou agrupados com cabos de alimentação.

Uma estação de trabalho de gerenciamento é um PC conectado à rede. Executando o software de gerenciamento de controle de acesso instalado no PC, o pessoal de gerenciamento de controle de acesso pode realizar remotamente várias funções de gerenciamento, como adicionar/excluir um usuário, visualizar registros de eventos, abrir/fechar portas e monitorar o status de cada porta em tempo real.

3.4 Terminais de Conexão do Painel de Controle

Diagrama de conexão dos terminais do C2-260



- **<u>Descrição dos terminais:</u>**

1. A entrada auxiliar pode ser conectada a detectores de corpo infravermelho, alarmes de incêndio ou detectores de fumaça.
2. A saída auxiliar pode ser conectada a alarmes, câmeras ou campainhas, etc.
3. PC RS485 indica que o cabo RS485 está conectado ao DM10/AUX485 por meio desta porta. A porta do leitor RS485 pode ser conectada externamente a um leitor RS485.
4. Restaurar configuração de fábrica: A chave DIP nº 4 está desligada por padrão. Ao movê-la para cima e para baixo três vezes dentro de 5 segundos e finalmente retorná-la para a posição ON, as configurações de fábrica serão restauradas após o painel de controle de acesso ser reiniciado, e o endereço IP será restaurado para o padrão (192.168.1.201).
5. Os terminais acima são configurados por meio do software de controle de acesso relevante. Consulte o respectivo manual do software para obter mais detalhes.

Portas do Painel de Controle C2-260:

Número	Porta Funcional	C2-260 (Duas Portas Bidirecionais)
1	Botoeira de Saída	2
2	Relé de controle de fechadura	2
3	Sensor de porta	2
4	Entrada Auxiliar	2
5	Saída Auxiliar	2
6	Leitor RS485	4
7	Comunicação de Extensão RS485	✓
8	TCP/IP	✓

3.5 Conexão com Sensores de Porta, Interruptores de Saída, Dispositivos de Entrada Auxiliar e Comunicação de Extensão RS485

1. Sensor de Porta

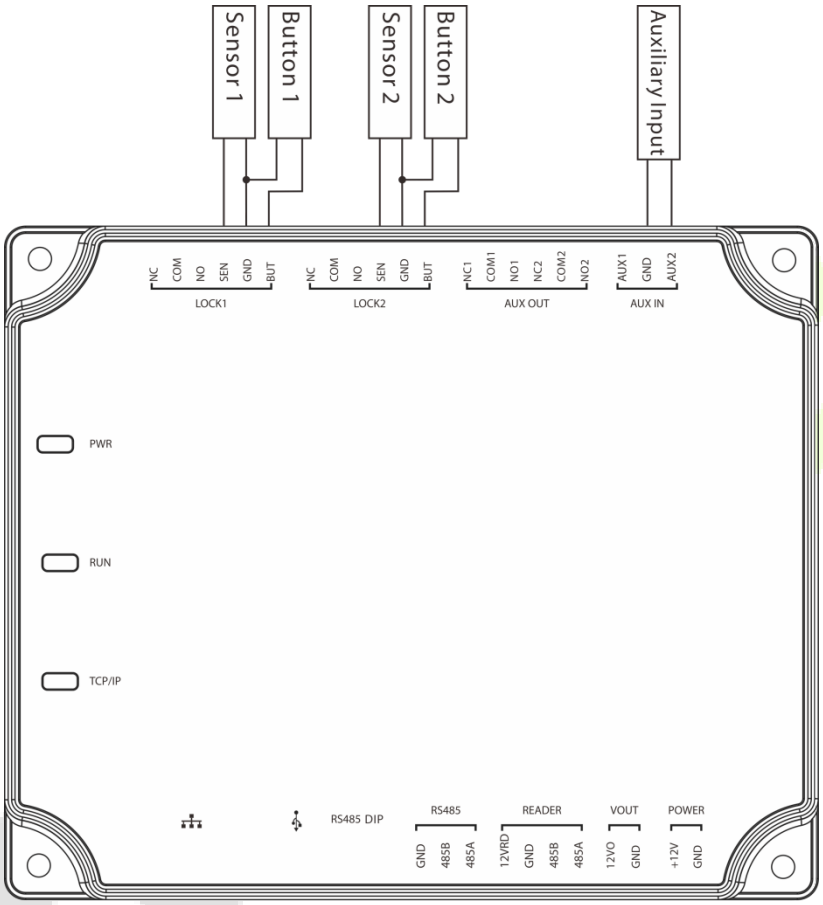
Um Sensor de Porta é usado para detectar o status de abertura/fechamento de uma porta. Com um interruptor de sensor de porta, um painel de controle de acesso pode detectar a abertura não autorizada de uma porta e acionar a saída de alarme. Além disso, se uma porta não for fechada dentro de um período especificado após ser aberta, o painel de controle da porta também emitirá um alarme. É recomendado selecionar fios de dois condutores com uma bitola acima de 0,22 mm^2. Um sensor de porta pode ser omitido se não for necessário monitorar o status de abertura/fechamento de uma porta, acionar o alarme quando a porta não for fechada por um longo período, monitorar se houver acesso não autorizado e usar a função de intertravamento.

2. Interruptor de Saída

Um interruptor de saída é um interruptor instalado dentro de um ambiente para abrir uma porta. Quando ele é acionado, a porta é aberta. Uma botoeira é fixada a uma altura de aproximadamente 1,4 m do chão. Certifique-se de que ele esteja localizado na posição correta, sem inclinação, e que a conexão esteja correta e segura. (Corte a ponta exposta de qualquer fio não utilizado e envolva-o com fita isolante.) Certifique-se de evitar interferência eletromagnética (como interruptores de luz e computadores). É recomendado utilizar fios de dois condutores com uma bitola acima de 0,3 mm^2 como fio de conexão entre o interruptor de saída e o painel de controle.

3. Entrada Auxiliar

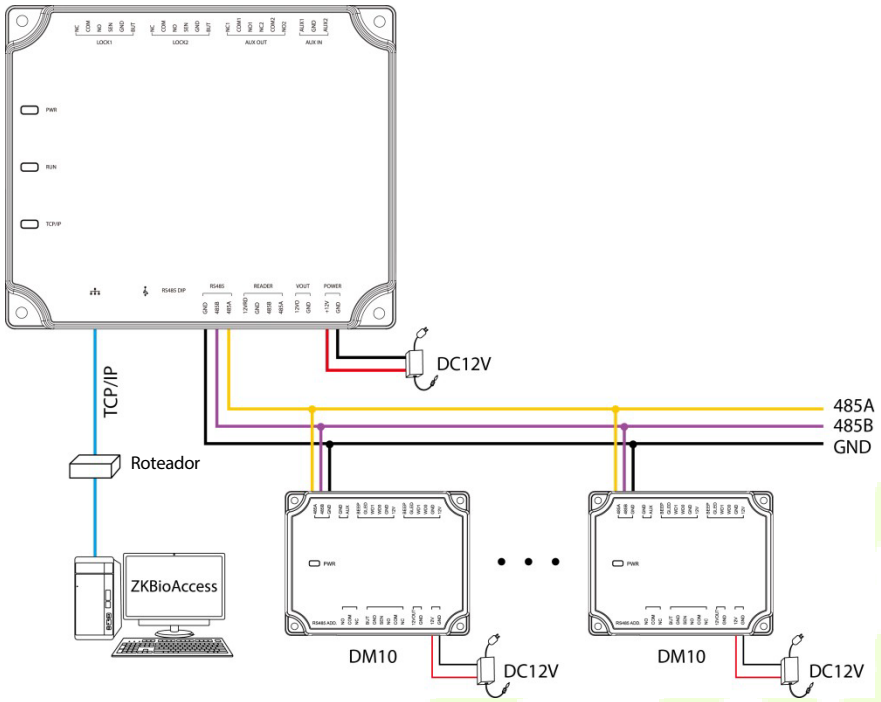
O painel de controle fornece uma interface de entrada auxiliar que pode ser conectada a detectores de corpo infravermelho, detectores de fumaça, detectores de gás, alarmes magnéticos de janela, interruptores de saída sem fio, etc. As entradas auxiliares são configuradas por meio do software de controle de acesso relevante. Consulte o respectivo manual do software para obter mais detalhes.



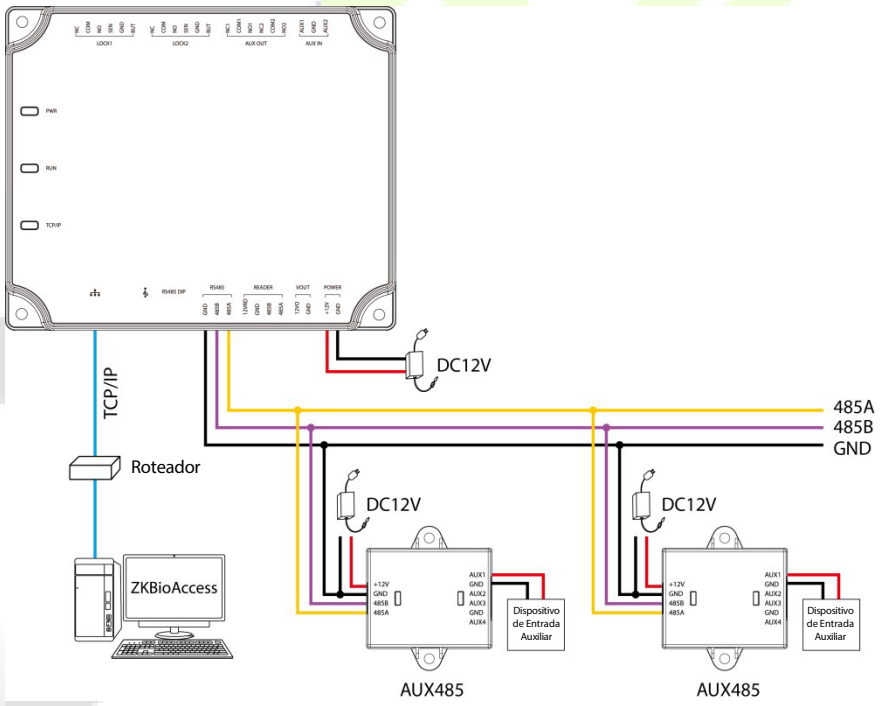
Conexões entre Painel de Controle e Sensores de Porta, Interruptores de Saída e Dispositivos de Entrada Auxiliares.

4. Comunicação de extensão RS485

O painel de controle suporta módulos extensivos como o **DM10** e o **AUX485** através da comunicação RS485. Um C2-260 pode se conectar a no máximo oito DM10 ou a no máximo dois AUX485. Como mostrado na figura a seguir.



Conecte-se ao DM10 através do RS485.



Conecte-se ao AUX485 através do RS485.

Observação:

1. Um C2-260 pode se conectar a no máximo oito módulos DM10 ou dois módulos AUX485.
2. Cada módulo AUX485 pode se conectar a no máximo quatro dispositivos auxiliares.
3. Cada módulo DM10/AUX485 requer uma fonte de alimentação separada.

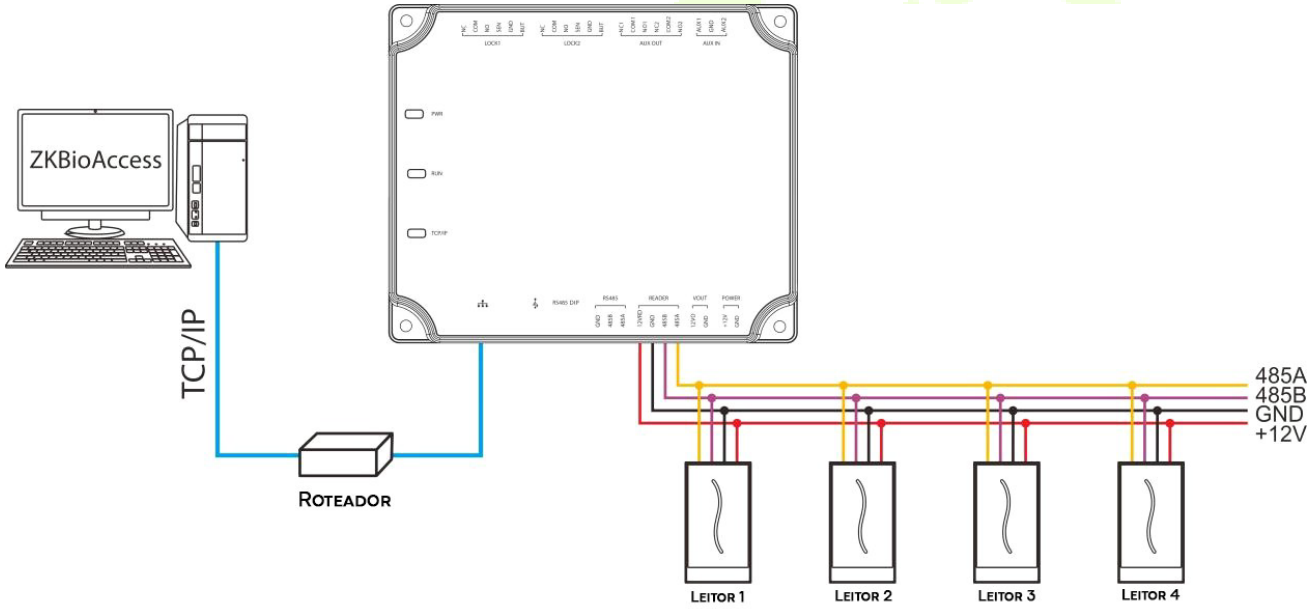
3.6 Conexão com Leitores RS485/Wiegand

O painel de controle suporta leitores de cartão RS485. Além disso, ele também suporta leitores Wiegand através do WR485.

- **Conexão com Leitores RS485**

O painel de controle suporta quatro leitores, que podem ser conectados no modo de duas portas bidirecionais. Conexão do leitor RS485: Defina o endereço RS485 (número do dispositivo) do leitor através de chaves DIP ou outros meios.

Endereço RS485 / Placa Controladora	1	2	3	4
C2-260	Porta 1 (Entrada)	Porta 1 (Saída)	Porta 2 (Entrada)	Porta 2 (Saída)



A conexão entre o Painel de Controle e os Leitores de Cartão RS485

Uma única interface de leitor RS485 pode fornecer no máximo 750 mA (12V) de corrente. Portanto, o consumo total de corrente deve ser inferior a esse valor máximo quando os leitores compartilham a energia com o painel. Para cálculos, por favor, utilize a corrente máxima do leitor, sendo que a corrente de inicialização geralmente é mais do que o dobro da corrente de trabalho padrão.

Usando o leitor de cartão KR502M-RS como exemplo, a corrente em standby é inferior a 80 mA; a corrente máxima é inferior a 90 mA. Ao iniciar o dispositivo, a corrente instantânea pode chegar a 180 mA. Para um leitor RS485, considerando que a corrente de inicialização é alta, apenas quatro leitores podem ser conectados à fonte de alimentação através da interface RS485 do leitor. Portanto, o painel de controle pode conectar no máximo 2 leitores.

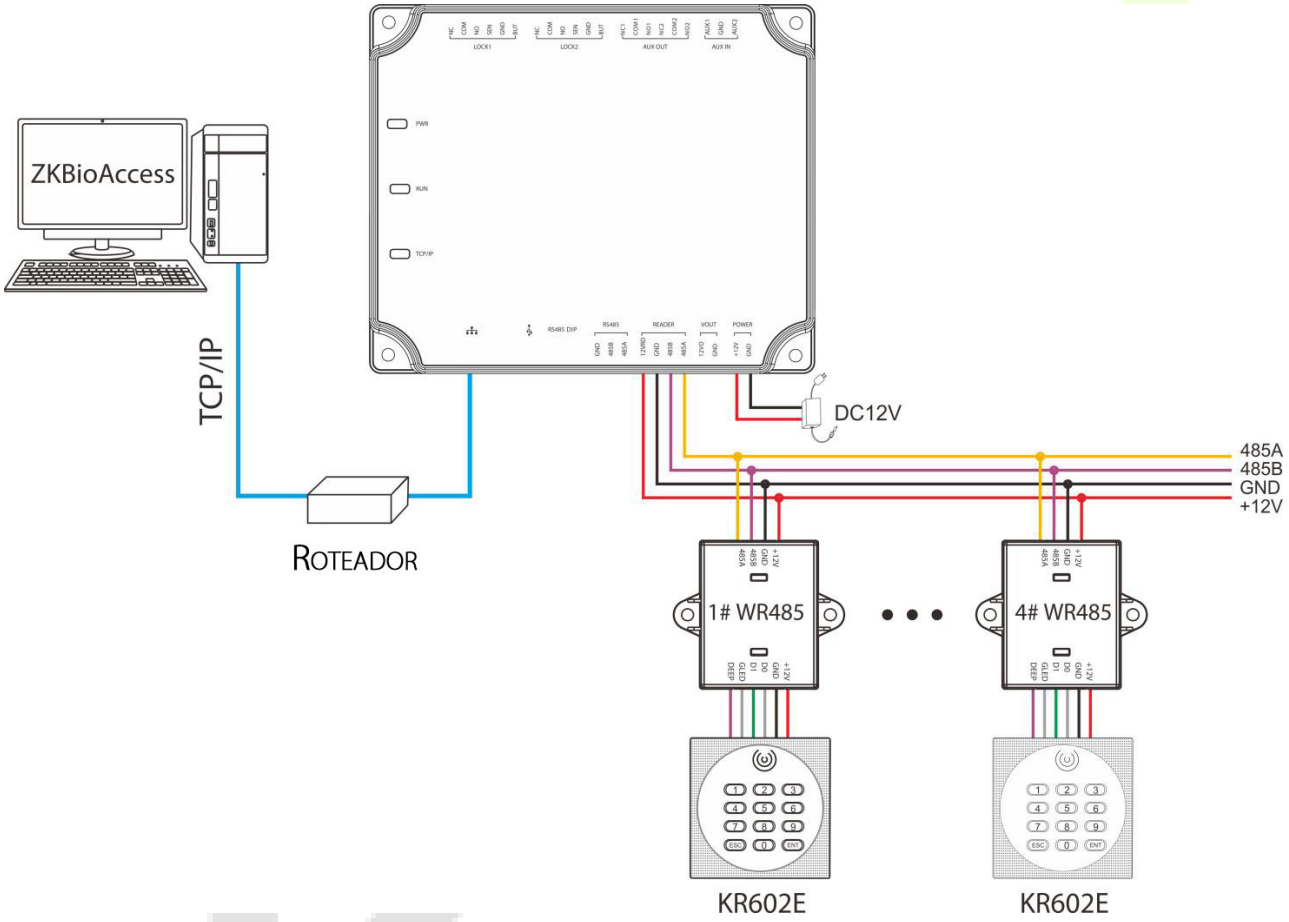
Se o leitor RS485 for conectado externamente e compartilhar a fonte de alimentação com o dispositivo,

é recomendado que a conexão entre a porta do leitor RS485 e o leitor não ultrapasse 100m. Caso contrário, é recomendado usar uma fonte de alimentação separada para o leitor.

Para os dispositivos que consomem mais energia, sugerimos o uso de fontes de alimentação diferentes para garantir um funcionamento estável.

- **Conexão com Leitores Wiegand**

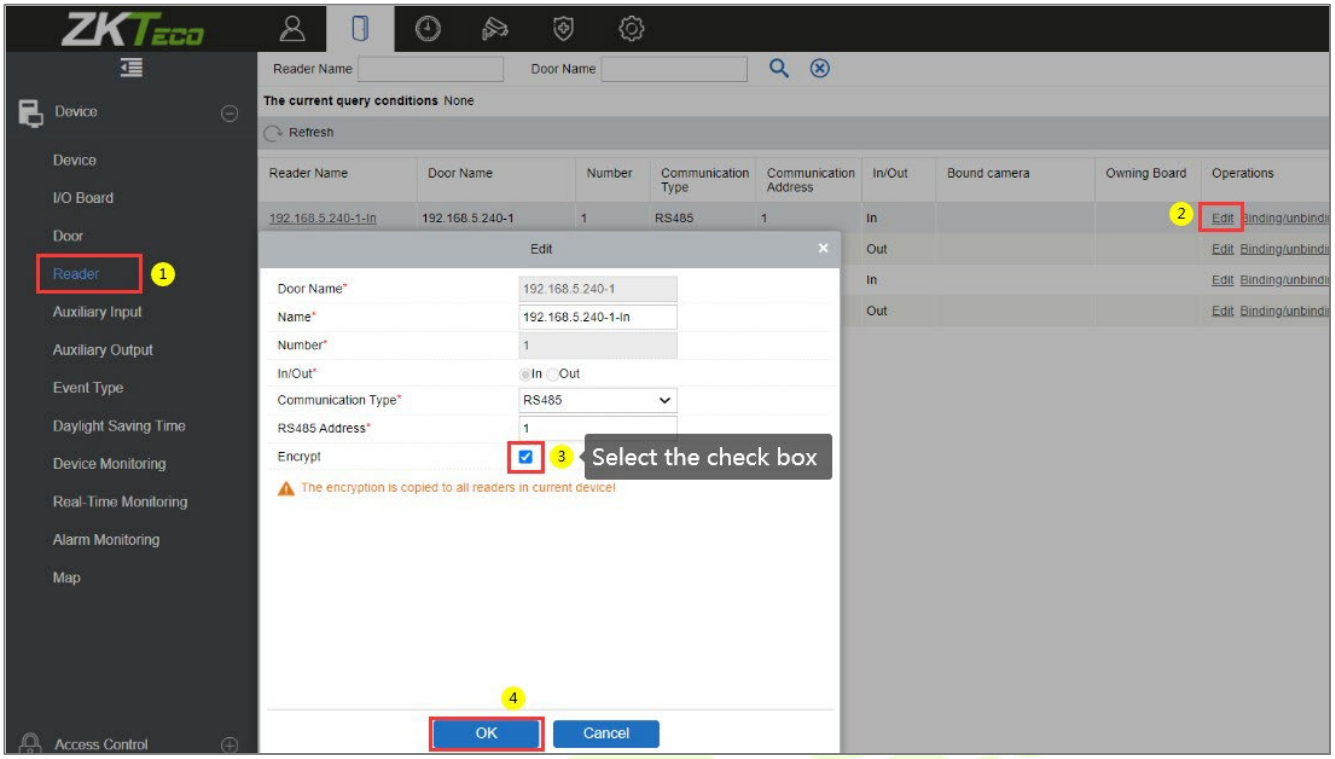
O controladora suporta a conexão de leitores Wiegand através do módulo WR485. A fiação é mostrada na figura abaixo.



Conexão entre a placa controladora e Leitores Wiegand via módulo WR485

Observação:

- Um C2-260 pode se conectar a no máximo quatro módulos WR485.
- Como o WR485 é um modo de criptografia, após adicionar o painel de controle C2-260 ao software ZKBioAccess, você precisa configurar a opção "Encrypt" para o leitor Wiegand. Isso permitirá que o leitor Wiegand seja usado normalmente. Conforme mostrado na figura a seguir.
- Para obter mais detalhes e configurações dos parâmetros, consulte o Apêndice 1.



3.7 Conexão de Saída de Relé

O C2-260 possui três relés (dois utilizados como fechaduras de controle por padrão e o outro utilizado como saída auxiliar).

Os relés para saídas auxiliares podem ser conectados a monitores, alarmes, campainhas, etc. As saídas auxiliares são configuradas através do software de controle de acesso relevante. Consulte o manual do software correspondente para obter mais detalhes.

1. O modo de conexão padrão da fechadura da porta é "modo seco" (dry mode). Em geral, a fechadura eletrônica utiliza uma fonte de alimentação externa separada. O modo de fiação do relé da fechadura da porta não pode ser alterado, exceto o relé de saída auxiliar. O diagrama abaixo utiliza o exemplo de conexão de uma fechadura da porta para demonstrar a conexão do relé de saída.
2. Um painel de controle de acesso fornece várias saídas para fechaduras eletrônicas. Os terminais COM e NA (Normalmente Aberto) são usados para fechaduras que são destravadas quando a energia é conectada e trancadas quando a energia é desconectada. Os terminais COM e NF (Normalmente Fechado) são usados para fechaduras que são trancadas quando a energia é conectada e destravadas quando a energia é desconectada.
3. Nosso painel de controle de acesso é alimentado por PoE padrão ou por uma fonte de alimentação de controle de acesso. Você pode escolher uma das fontes de alimentação conforme necessário. Ambas as fontes de alimentação fornecem 12V/3A apenas para o consumo de energia do painel de controle, leitores Wiegand e consumo de energia de saída do leitor RS485.
4. Para proteger o sistema de controle de acesso contra a força eletromotriz autoinduzida gerada por uma fechadura eletrônica no instante de ligar/desligar, é necessário conectar um diodo em paralelo (utilize o FR107 fornecido com o sistema) com a fechadura eletrônica para liberar a força eletromotriz autoinduzida durante a conexão no local para aplicação do sistema de controle de acesso.

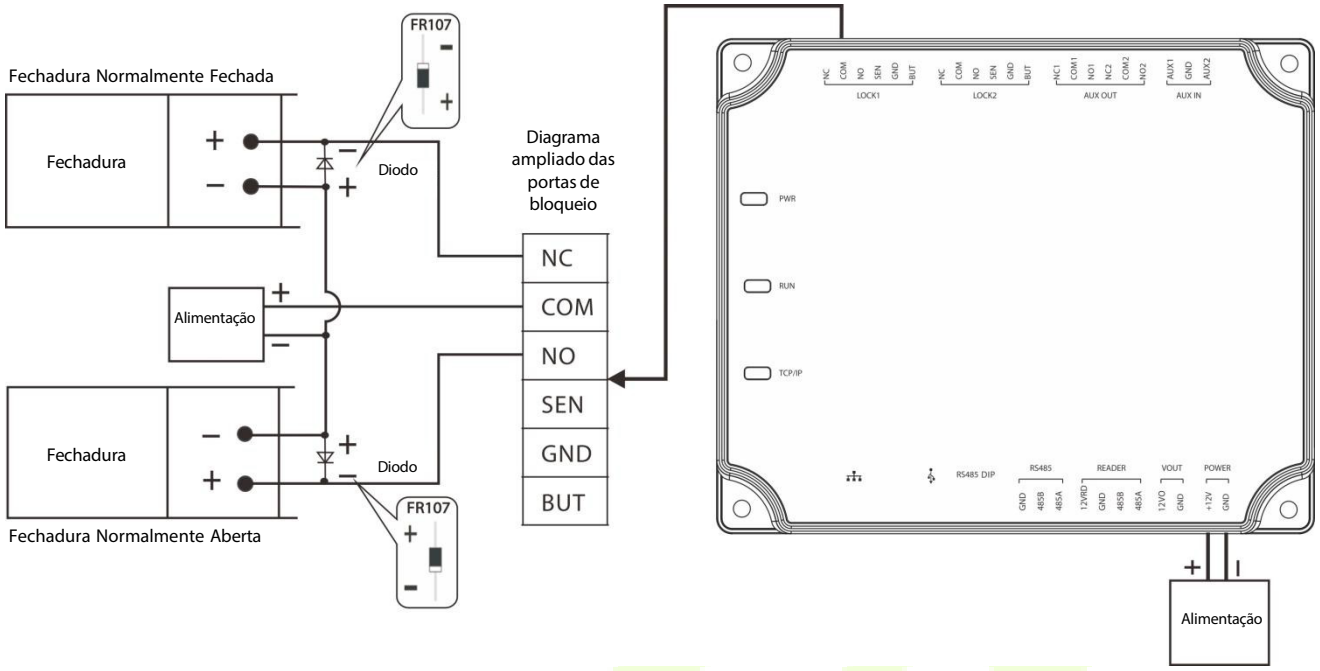


Diagrama de fiação da conexão da fechadura

4 Comunicação de Equipamentos

O software de PC em segundo plano pode se comunicar com o sistema de acordo com dois protocolos (TCP/IP e RS485) para a troca de dados e gerenciamento remoto.

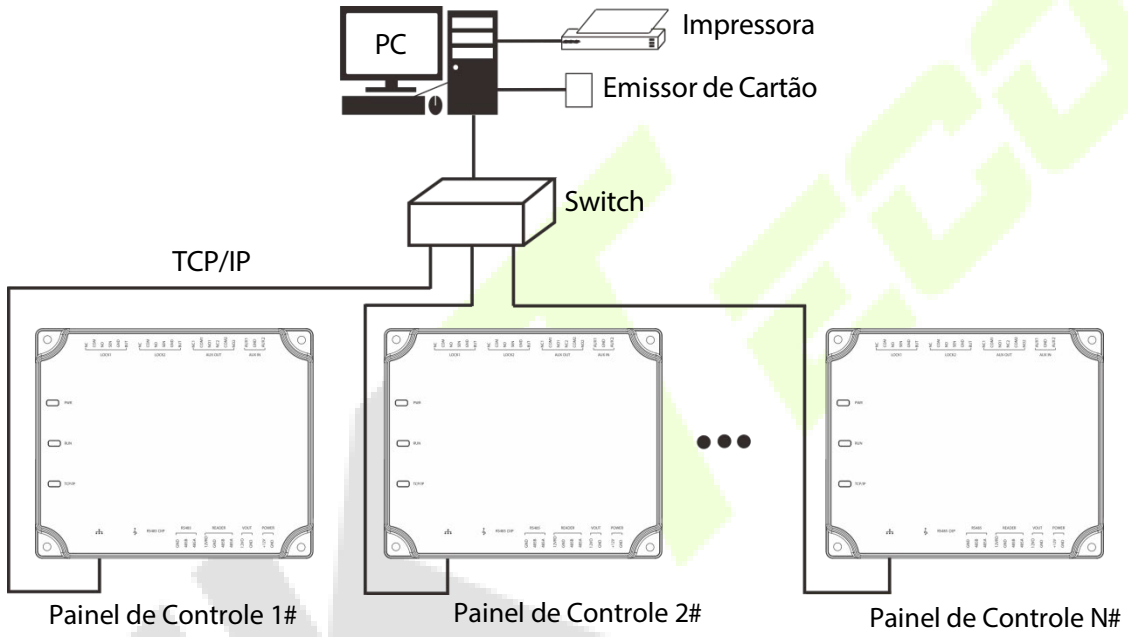
4.1 Fiação e Conexões de Rede de Controle de Acesso

1. A fonte de alimentação é de 12V DC convertida a partir de 220V ou PoE.
2. Como uma fechadura eletrônica possui uma corrente alta, ela gera um sinal de interferência forte durante o funcionamento. Para reduzir esse efeito, são recomendados cabos de 4 núcleos (RVVP 4×0.75mm2, dois para a alimentação e dois para um sensor de porta).
3. A interface "RS485" utiliza cabos blindados de comunicação de 4 núcleos (RVVSP 4*0.5mm).
4. Outros cabos de controle (como interruptores de saída) são todos feitos de cabos de 2 núcleos (RVVSP 2×0.5mm2).
5. Observações para a fiação:
   - Os cabos de sinal (como cabos de rede) não podem ser executados em paralelo nem compartilhar uma tubulação com fios elétricos de alta potência (como fios de fechadura eletrônica e cabos de alimentação). Se a fiação em paralelo for inevitável por motivos ambientais, a distância deve ser superior a 50cm.
   - Tente evitar o uso de qualquer condutor com um conector durante a distribuição. Quando um conector for indispensável, ele deve ser prensado ou soldado. Nenhuma força mecânica pode ser aplicada à junção ou ramificação dos condutores.
   - Em um prédio, as linhas de distribuição devem ser instaladas horizontal ou verticalmente. Elas devem ser protegidas em tubos de revestimento (como tubos de água de plástico ou ferro, a serem selecionados de acordo com os requisitos técnicos da distribuição interna). Mangueiras metálicas são aplicáveis para fiação no teto, mas devem ser seguras e de boa aparência.
   - Medidas de blindagem e conexão de blindagem: Se a interferência eletromagnética no ambiente de fiação for considerável na pesquisa antes da construção, é necessário considerar a proteção de blindagem dos cabos de dados ao projetar um esquema de construção. Em geral, a proteção de blindagem é necessária se houver uma fonte de interferência radioativa grande ou se a fiação tiver que ser paralela a uma fonte de alimentação de corrente alta no local de construção. Geralmente, as medidas de blindagem incluem manter uma distância máxima de qualquer fonte de interferência e usar calhas de fiação de metal ou tubos de água galvanizados para garantir um aterramento confiável da conexão entre as camadas de blindagem dos cabos de dados e as calhas ou tubos de metal. Observação: uma caixa de blindagem só pode ter efeito de blindagem quando está aterrada de forma confiável.
   - Método de Conexão do Fio de Aterramento: São necessários fios de aterramento confiáveis de grande diâmetro, em conformidade com as normas nacionais aplicáveis, no local de fiação e devem ser conectados em forma de árvore para evitar circuito de corrente contínua. Esses fios de aterramento devem ser mantidos longe de campos de raios. Nenhum para-raios pode servir como um fio de aterramento e garantir que não haja corrente de raio através de nenhum fio de

aterramento quando houver um raio. Calhas e tubos de metal devem ser conectados de forma contínua e confiável e ligados aos fios de aterramento por meio de cabos de grande diâmetro. A impedância dessa seção de fio não pode exceder 2 ohms. Além disso, a camada de blindagem deve ser conectada de forma confiável e aterrada em uma extremidade para garantir uma direção de corrente uniforme. O fio de aterramento da camada de blindagem deve ser conectado por meio de um fio de grande diâmetro (não inferior a 2,5mm2).

4.2 Comunicação TCP/IP

O cabo de rede Ethernet 10/100Base-T Crossover, um tipo de cabo de rede cruzado, é principalmente usado para interconectar hubs e switches em cascata ou para conectar dois pontos de extremidade Ethernet diretamente (sem um hub). Ambos 10Base-T e 100Base-T são suportados.



Sistema de Rede de Comunicação TCP/IP

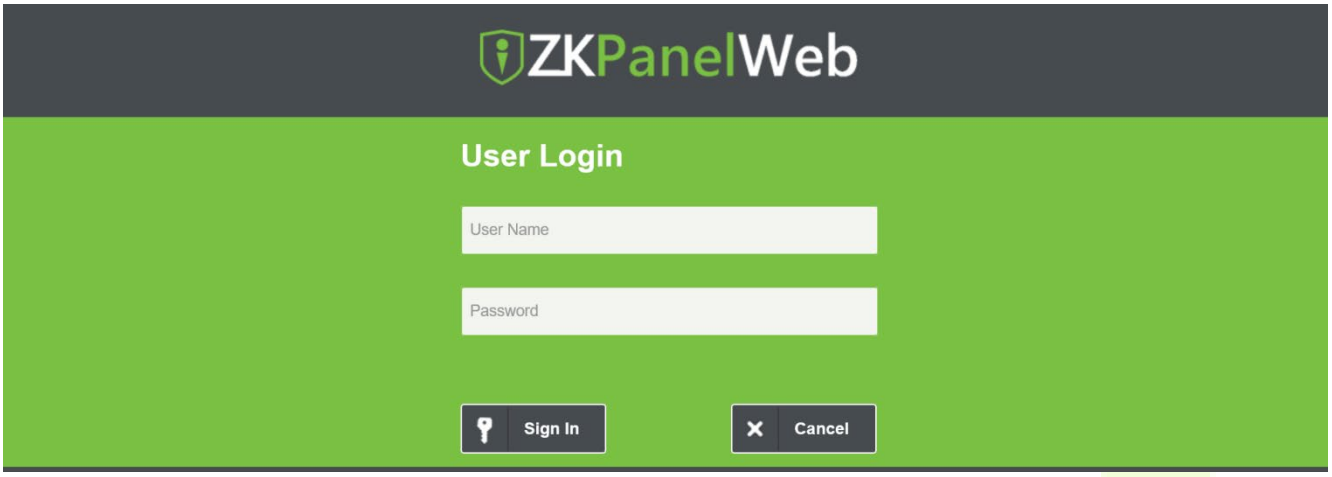
No software de acesso: clique em **Dispositivo > Procurar Dispositivo** para buscar controladoras de acesso na rede e adicionar diretamente a partir do resultado da busca.

4.3 ZKPanelWeb

Essa função incorporada foi adicionada recentemente para auxiliar o usuário a gerenciar os controladores de forma mais conveniente. Os usuários podem usar a função de Servidor Web para realizar operações, como configuração de rede, configuração de comunicação por push, sincronização de horário e gerenciamento de contas de usuário.

- **Acesse o Web Server**

Crie uma string de conexão válida usando TCP/IP. Insira o endereço IP da controladora (padrão de fábrica é 192.168.1.201) na barra de endereço; digite o nome de usuário e senha (ambos são admin) e clique em [**Entrar**] para acessar o ZKPanelWeb.

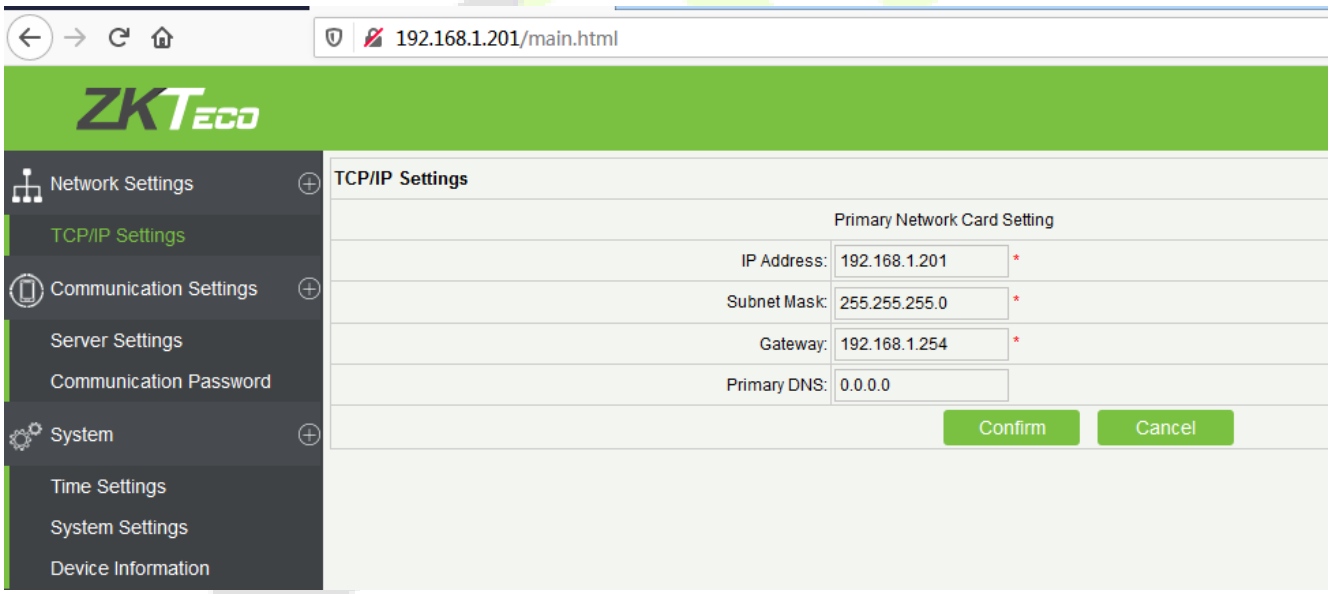


Observação:

1. Os endereços IP do servidor (PC) e do controlador devem estar no mesmo segmento de rede.
2. O endereço IP do controlador pode ser encontrado pesquisando dispositivos com o software BioSecurity ([**Accesso**] > [**Dispositivo de Acesso**] > [**Dispositivo**] > [**Buscar Dispositivo**]).

- **Configurações TCP/IP**

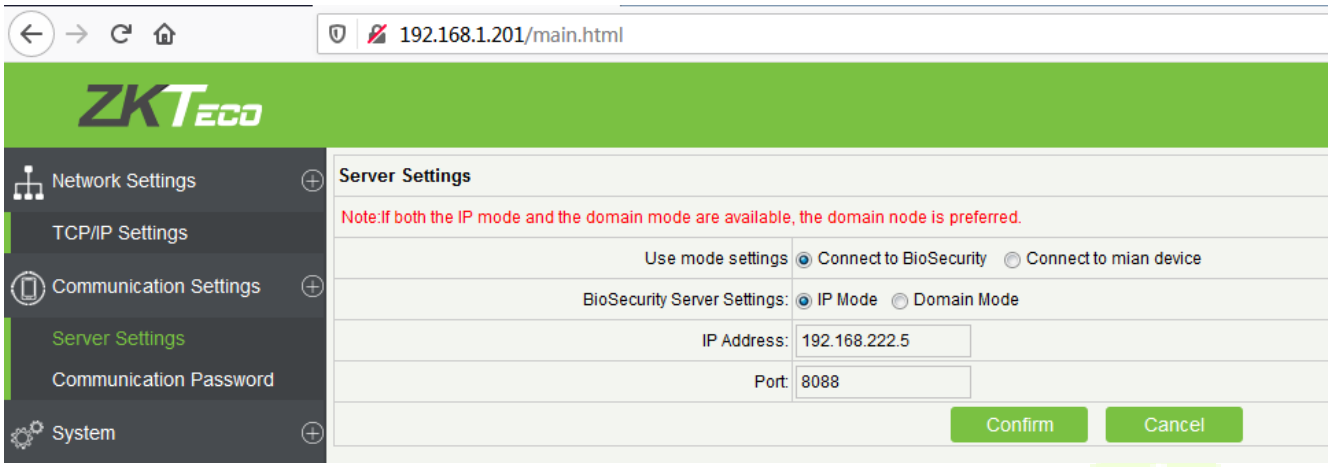
Clique em **[Configurações TCP/IP]** para modificar o endereço IP e o endereço do gateway.



- **Configurações de Comunicação**

Configure os parâmetros de comunicação no ZKPanelWeb e conecte o controlador ao servidor (PC); o controlador enviará automaticamente informações para o servidor.

1) Configurações do Servidor

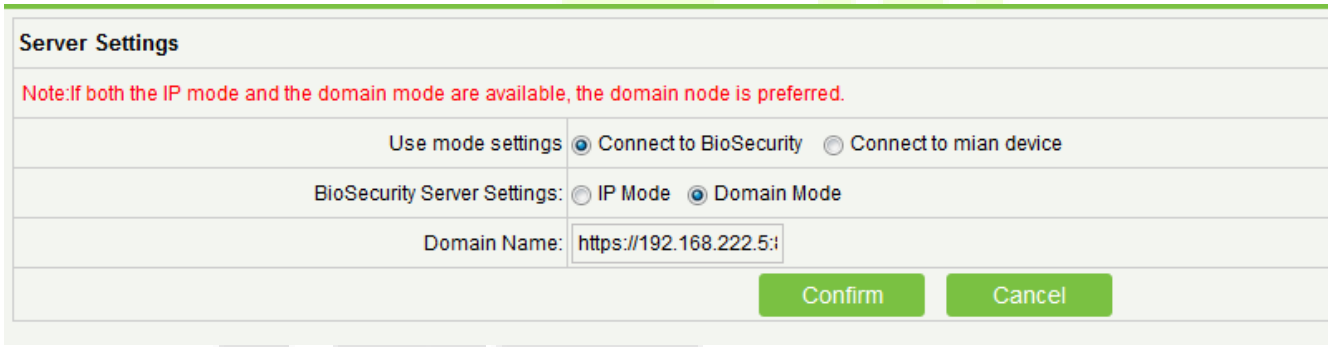


Configurações do modo: O modo padrão é Conectar ao BioSecurity.

Configurações do Servidor BioSecurity: Para definir os parâmetros do Modo IP e Modo de Domínio.

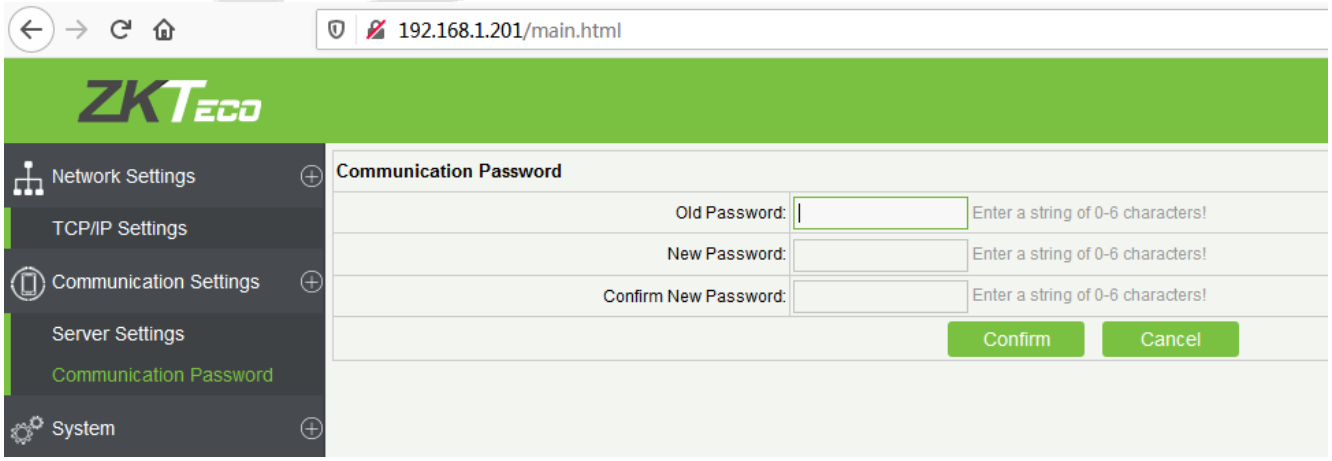
Modo IP: O IP do servidor padrão é 0.0.0.0, e você pode modificá-lo de acordo com a situação prática.

Porta: A porta padrão é 8088, e você pode modificá-la de acordo com a situação prática.



Modo de Domínio: O valor padrão é nulo, e você pode definir o seu valor. Se o usuário deseja fazer login no software BioSecurity através do HTTPS, então defina o nome de domínio aqui. O formato é: https://192.168.222.5:8088.

2) Senha de Comunicação

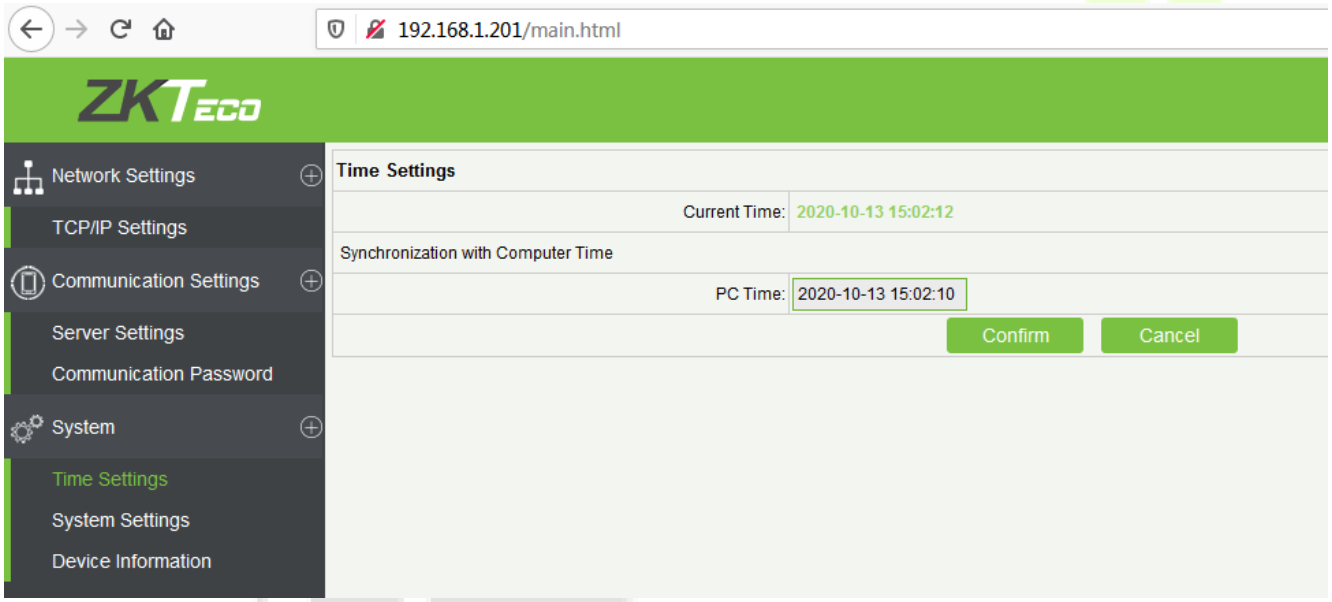


Senha de Comunicação: Indica que a comunicação em rede é criptografada. O valor padrão é nulo, e você pode definir o seu valor.
Se você configurar a senha de comunicação aqui, a mesma senha de comunicação deve ser configurada no servidor antes que a conexão possa ser estabelecida.

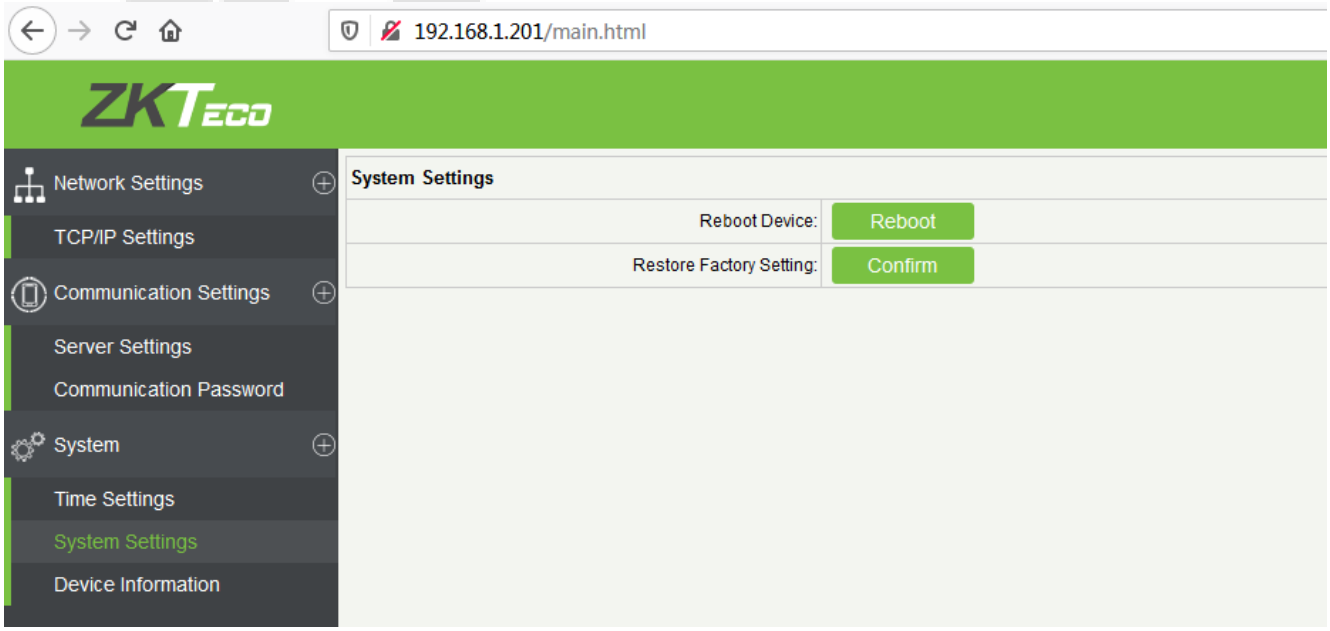
- **Sistema**

O usuário pode sincronizar o horário com o computador, configurar o sistema e visualizar informações do dispositivo aqui.

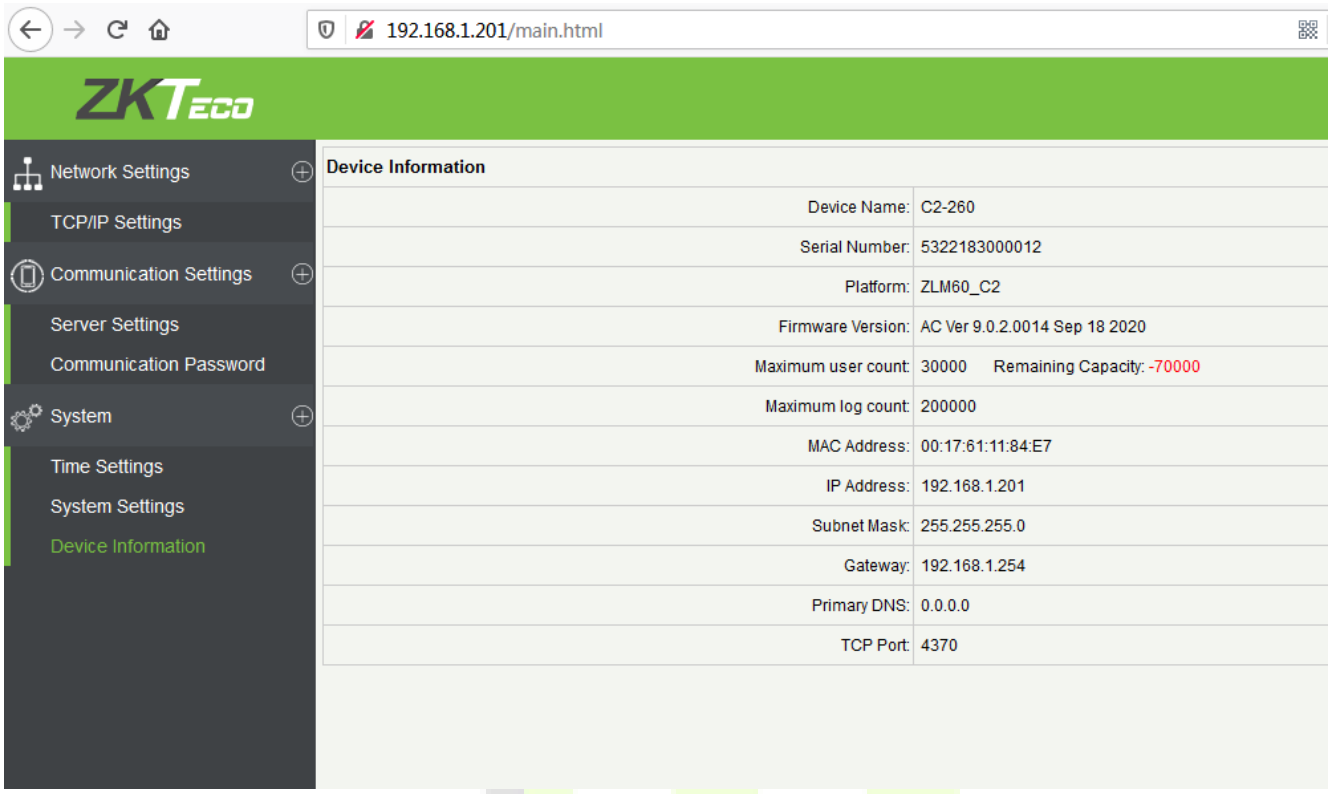
1) Configurações de Horário



2) Configurações do Sistema



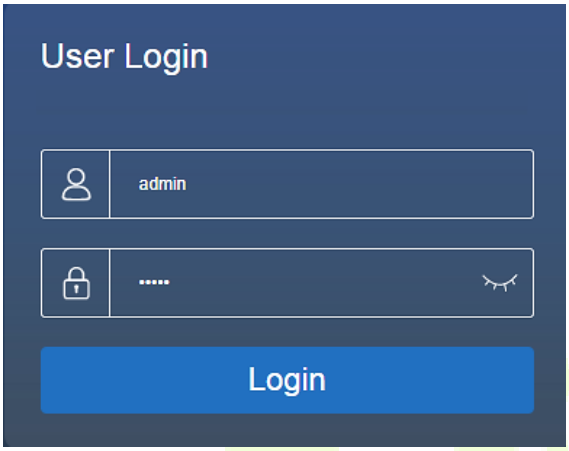
3) Informações do Dispositivo



5 ZKBioAccess

As seguintes seções explicam as funções do software ZKBioAccess após a instalação dos Controladores de Acesso.

5.1 Login



Após instalar o software, clique duas vezes no ícone do ZKBio Access para abrir o software. Você também pode abrir o navegador recomendado e inserir o endereço IP e a porta do servidor na barra de endereços. O endereço IP padrão é http://127.0.0.1:8098.

Se o software não estiver instalado no seu servidor, você pode inserir o endereço IP e a porta do servidor na barra de endereços.

Observação: O nome de usuário do superusuário é **admin**, e a senha é **admin**.

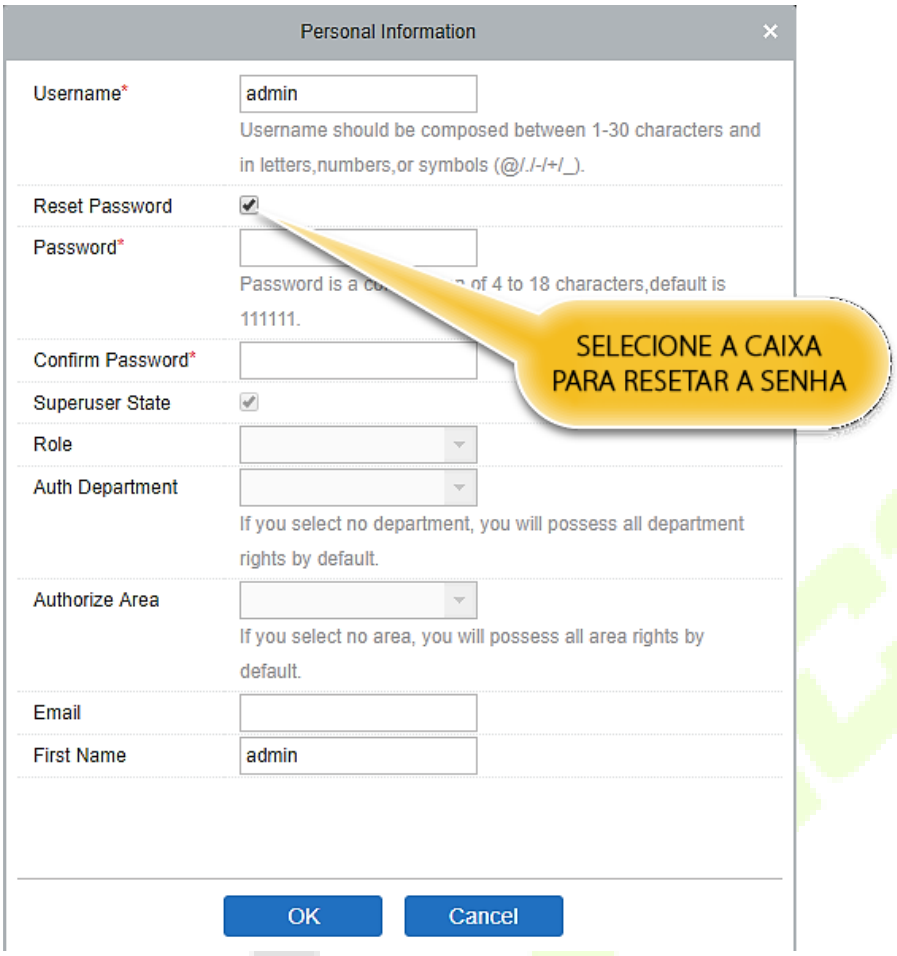
Em seguida, clique em **Login**. Após fazer login pela primeira vez, você precisará redefinir sua senha.

5.2 Ativar o Sistema

Por favor, consulte o documento de ativação de licença correspondente.

5.3 Modificar Senha

Você pode modificar a senha de login na seção de **Informações Pessoais**.



Selecione a caixa **Redefinir Senha** para modificar a senha.

Observação: Tanto o Superusuário quanto o novo usuário são criados pelo Superusuário (a senha padrão para os novos usuários é 111111). O nome de usuário não é sensível a maiúsculas e minúsculas, mas a senha é sensível a maiúsculas e minúsculas.

5.4 Dispositivo

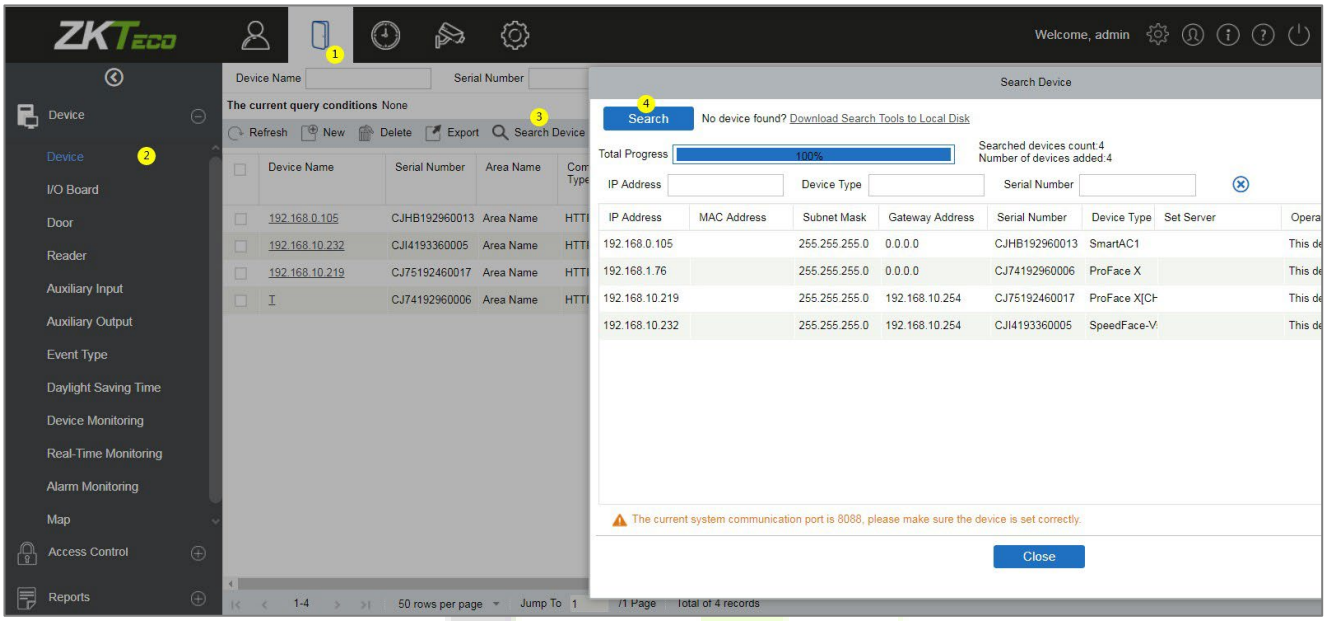
As Configurações do Dispositivo permitem adicionar um dispositivo de acesso e, em seguida, definir os parâmetros de comunicação dos dispositivos conectados, incluindo configurações do sistema e configurações do dispositivo. Quando a comunicação é bem-sucedida, você pode visualizar aqui as informações dos dispositivos conectados e realizar monitoramento remoto, upload e download, entre outras funções.

5.4.1 Adicionando um Dispositivo

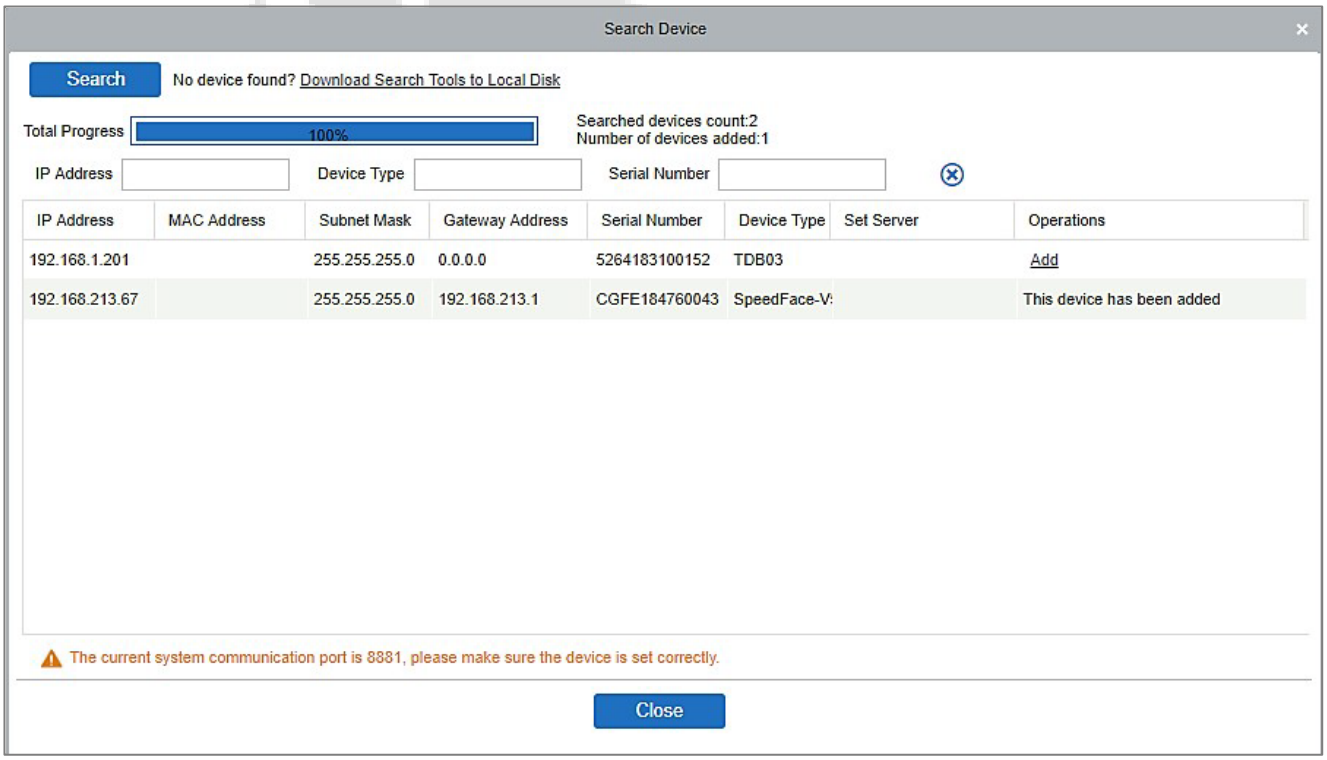
Existem duas maneiras de adicionar dispositivos de acesso.

Adicionar dispositivo pesquisando controladores de acesso.

Pesquise os controladores de acesso na Ethernet.



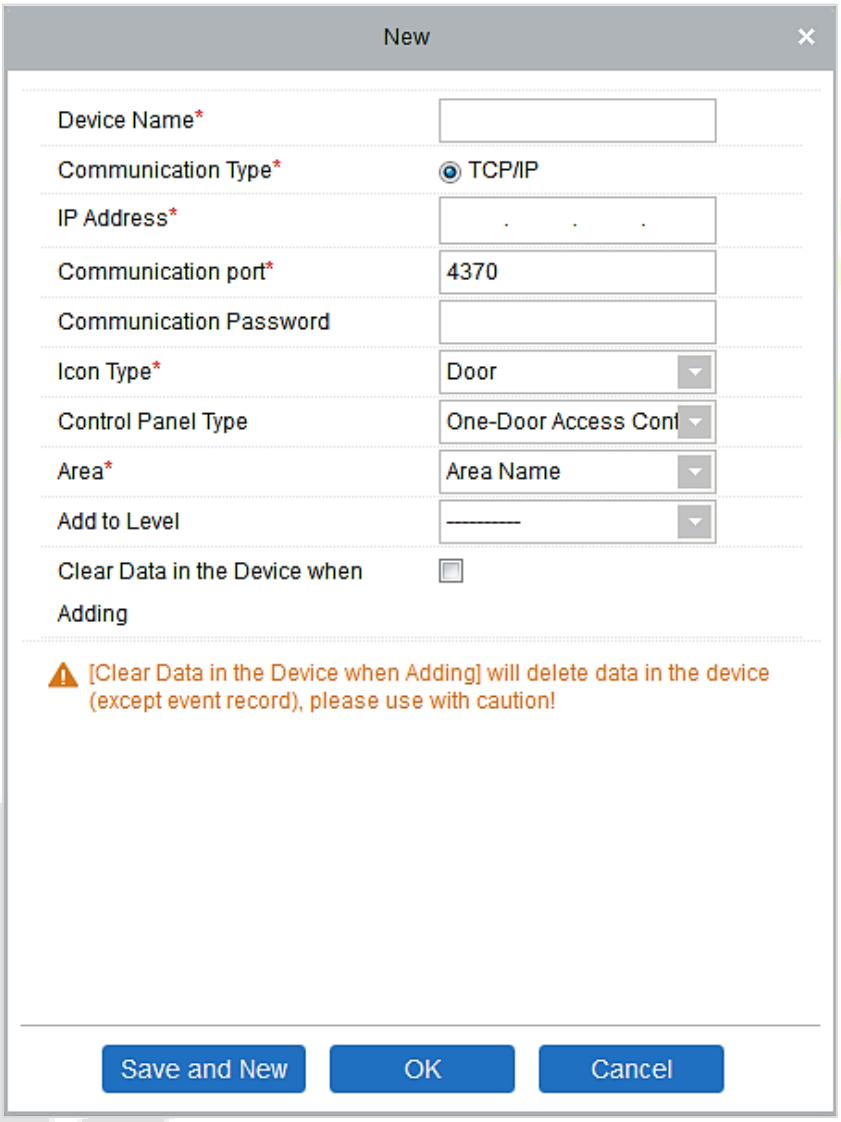
1. Clique em **Acesso > Dispositivo > Pesquisar Dispositivo** para abrir a interface de pesquisa.
2. Clique em **Pesquisar**, e será exibida a mensagem "Pesquisando..."
3. Após a conclusão da pesquisa, a lista e o número total de controladores de acesso serão exibidos.



Observação: O modo de transmissão UDP será utilizado para buscar os dispositivos de acesso. Este modo não pode realizar uma função de cruzamento de roteador. O endereço IP pode fornecer um segmento de rede cruzada, mas deve estar na mesma sub-rede, e o Gateway e o Endereço IP devem ser configurados no mesmo segmento de rede.

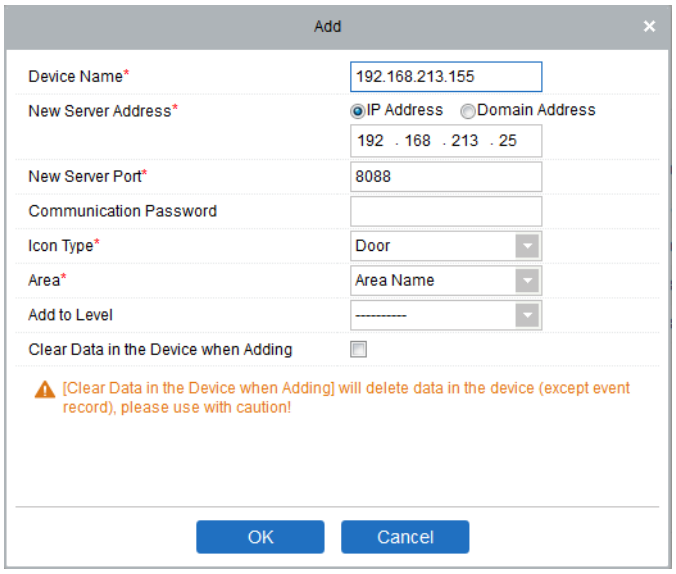
1. Clique em **Adicionar** na lista de pesquisa.

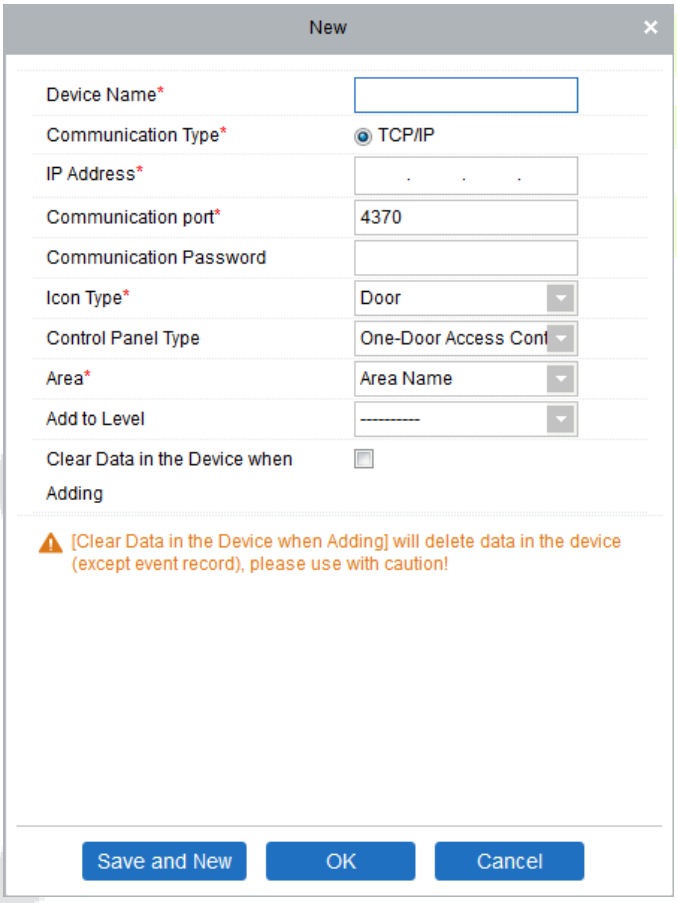
Se o dispositivo for um dispositivo pull, você pode inserir um nome de dispositivo e clicar em **OK** para concluir a adição do dispositivo.



Limpar Dados no Dispositivo ao Adicionar: Se esta opção for selecionada, após adicionar um dispositivo, o sistema irá limpar todos os dados no dispositivo (exceto os logs de eventos).

Se o dispositivo for um dispositivo com firmware push, as seguintes janelas serão exibidas após clicar em **Adicionar**. Se o endereço IP em Novo Endereço do Servidor for selecionado, então configure o endereço IP e o número da porta. Se a opção Endereço de Domínio em Novo Endereço do Servidor for selecionada, então defina o endereço de domínio, número da porta e DNS. O dispositivo será adicionado automaticamente ao software.





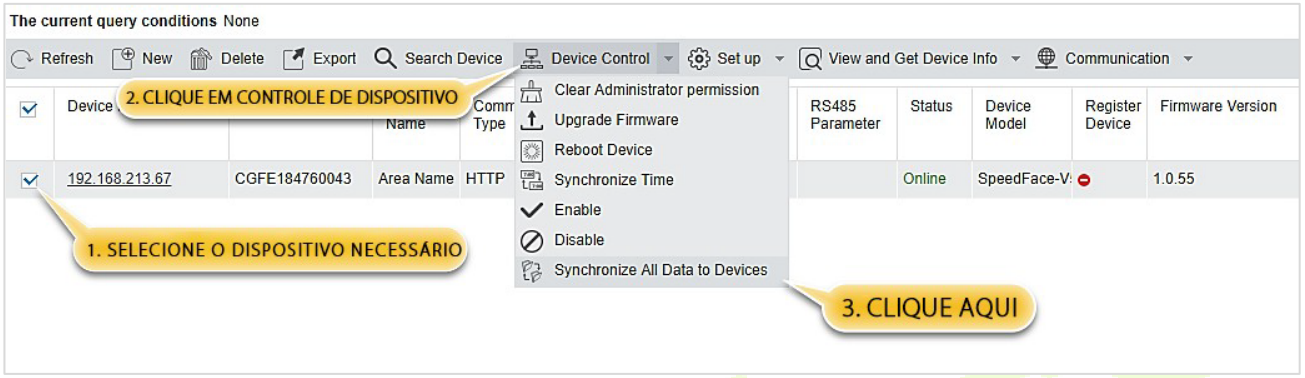
Novo Endereço do Servidor: Para adicionar um dispositivo por endereço IP ou endereço de domínio, os dispositivos podem ser adicionados ao software inserindo o endereço de domínio.

Nova Porta do Servidor: Define o ponto de acesso do sistema.

DNS: Define um endereço DNS do servidor.

Limpar Dados no Dispositivo ao Adicionar: Se esta opção for selecionada, após adicionar um dispositivo, o sistema irá limpar todos os dados no dispositivo (exceto os logs de eventos). Se você estiver adicionando o dispositivo apenas para demonstração ou teste, não é necessário selecionar esta opção.

Observação: Ao usar qualquer um dos três métodos de adição de dispositivo mencionados acima, se houver dados residuais no dispositivo original, por favor, sincronize os dados originais com ele após adicionar um novo dispositivo ao software, clicando em **Dispositivo > Sincronizar Todos os Dados nos Dispositivos**. Caso contrário, esses dados originais podem entrar em conflito com o uso normal.

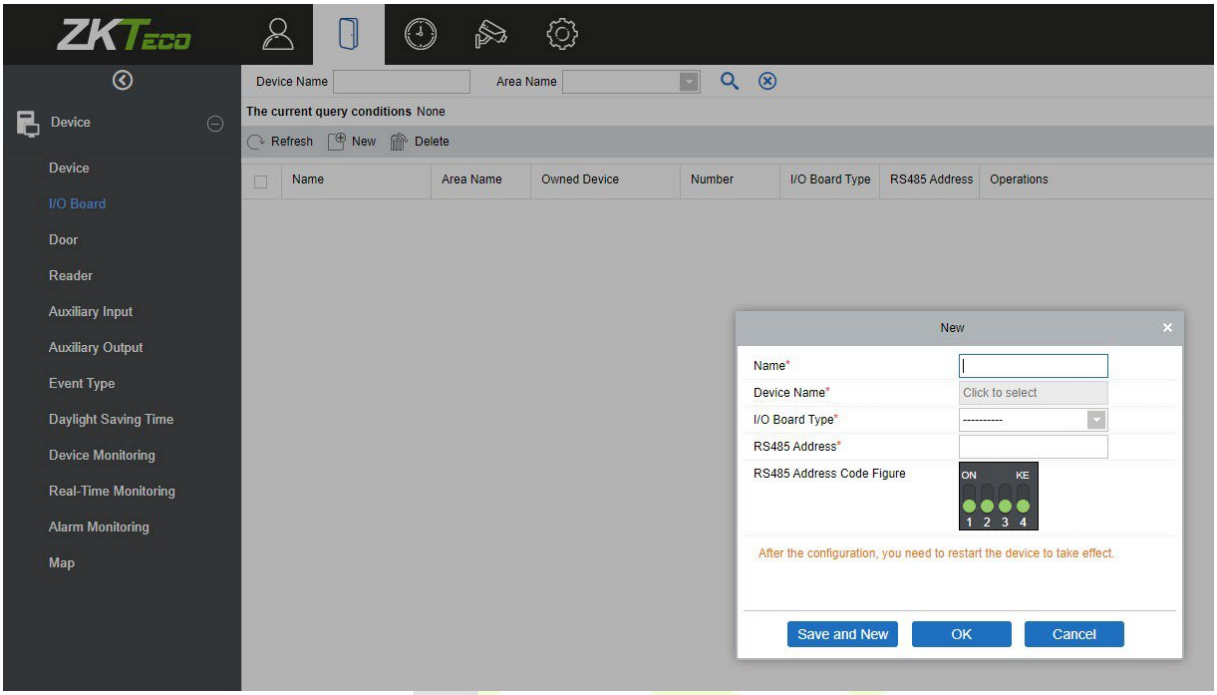


2. O endereço IP padrão do dispositivo de acesso pode entrar em conflito com o IP de um dispositivo na rede local. Você pode modificar o endereço IP: clique em **Modificar Endereço IP** e uma caixa de diálogo será exibida na interface. Insira o novo endereço IP e outros parâmetros (Observação: configure o gateway e o endereço IP no mesmo segmento de rede).

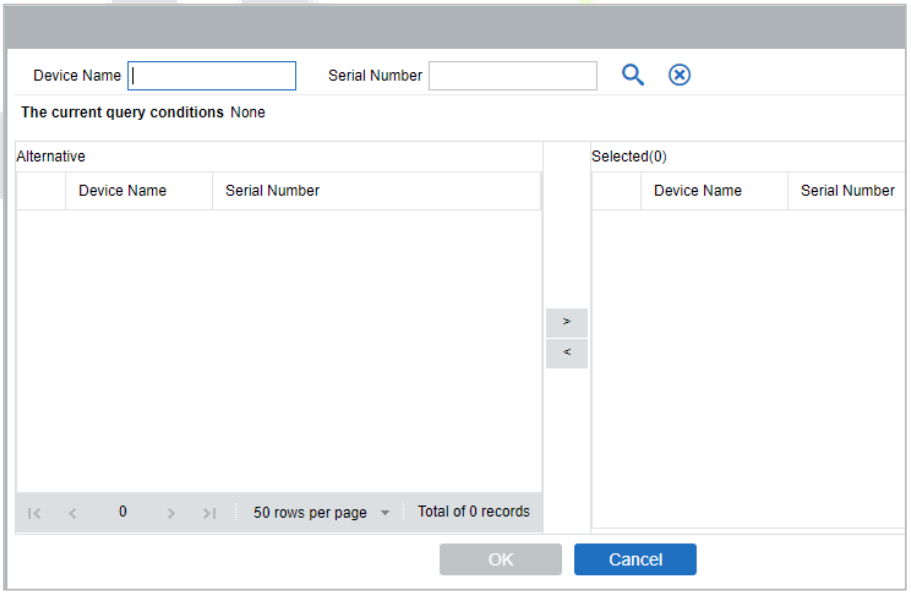
Observação: Alguns dispositivos de PUSH suportam SSL. Para utilizar essa função, selecione a porta HTTPS durante a instalação do software e certifique-se de que o firmware do dispositivo suporte SSL.

5.4.2 Placa de E/S

No módulo de dispositivo, clique em **Dispositivo** > **Placa de E/S** > **Novo** para adicionar o dispositivo de Placa de E/S ao software.



Digite o nome da Placa de E/S. Selecione o Dispositivo clicando no campo Nome do Dispositivo. A lista de dispositivos aparece, conforme mostrado abaixo:

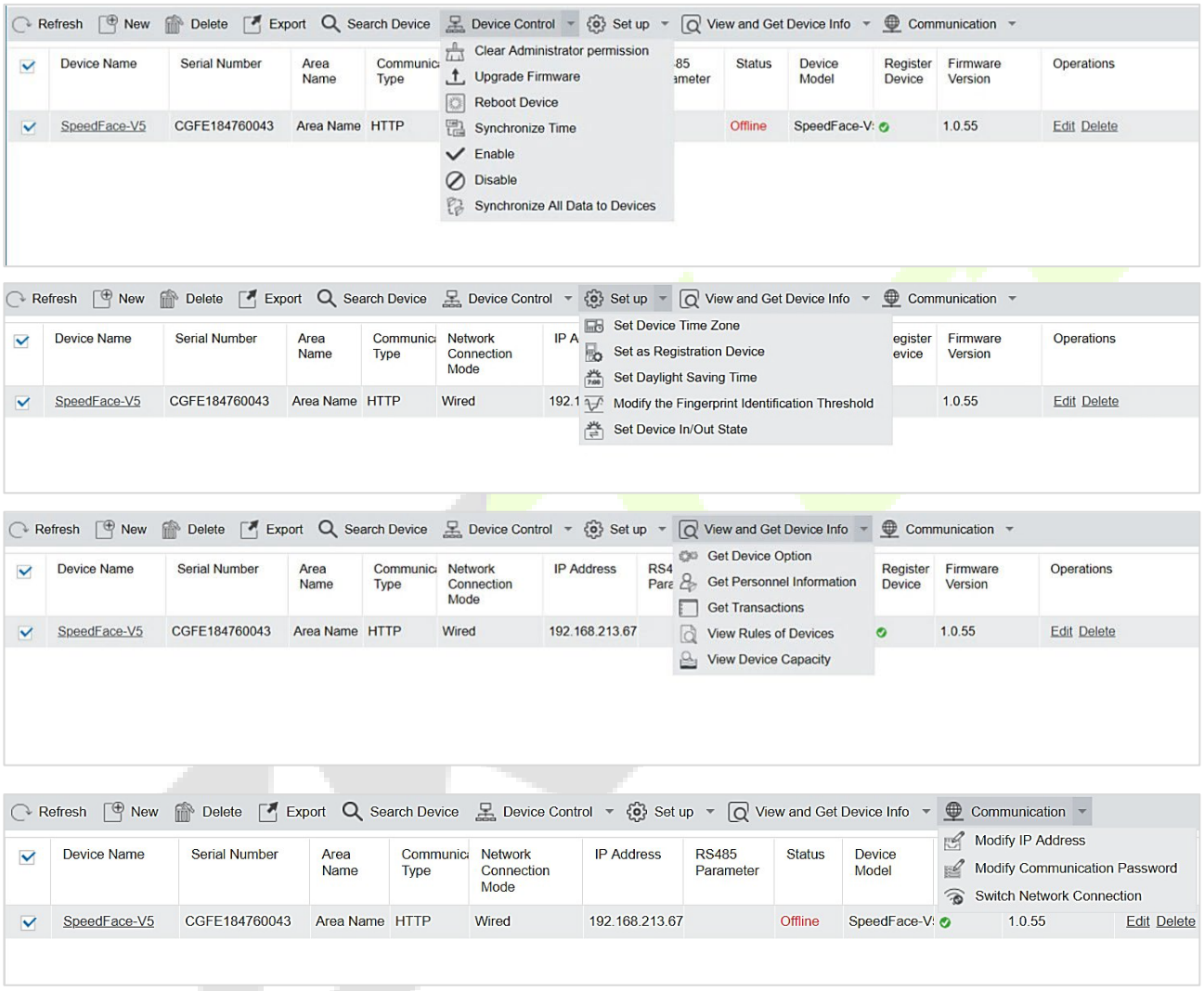


Selecione o dispositivo e clique em **OK**. Selecione o Tipo de Placa de E/S. Defina o Endereço do Código RS485 alterando o botão correspondente. Clique em **OK** para salvar os detalhes. Você pode visualizar todas as entradas auxiliares na interface de Entrada Auxiliar.

Observação: Por favor, selecione este método ao adicionar DM10 e AUX485.

5.4.3 Operação do Dispositivo

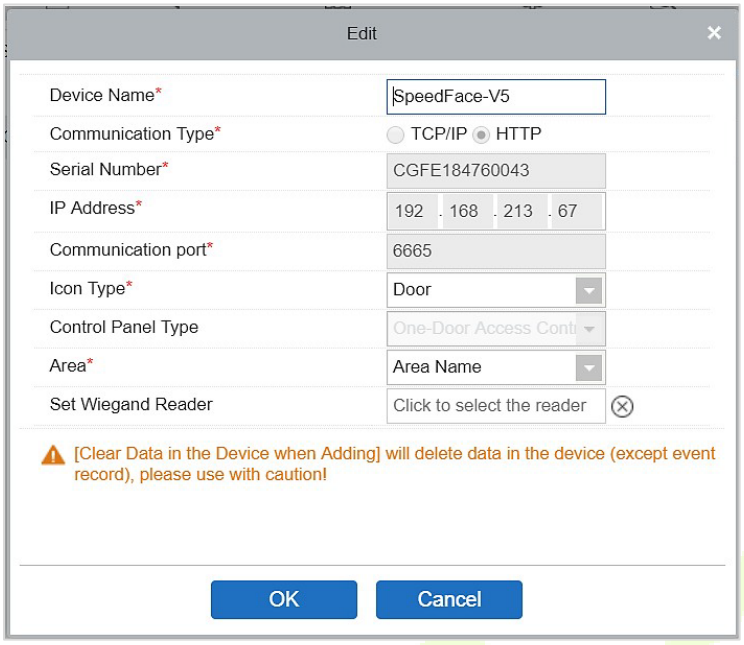
Para a comunicação entre o sistema e o dispositivo, o upload de dados, o download de configuração e a configuração de parâmetros do dispositivo e do sistema devem ser definidos. Os usuários podem editar os controladores de acesso dentro dos níveis apropriados no sistema atual; os usuários só podem adicionar ou excluir dispositivos na Gerência de Dispositivos, se necessário.



- **Editar ou Excluir um Dispositivo**

Editar: Clique no Nome do Dispositivo ou clique em Editar para acessar a interface de edição.

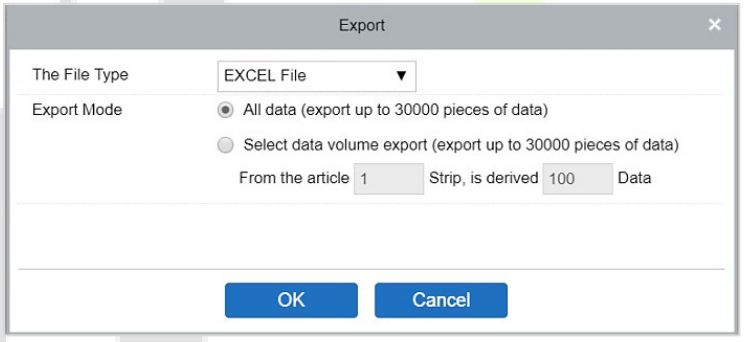
Excluir: Selecione o dispositivo, clique em Excluir e clique em OK para excluir o dispositivo.

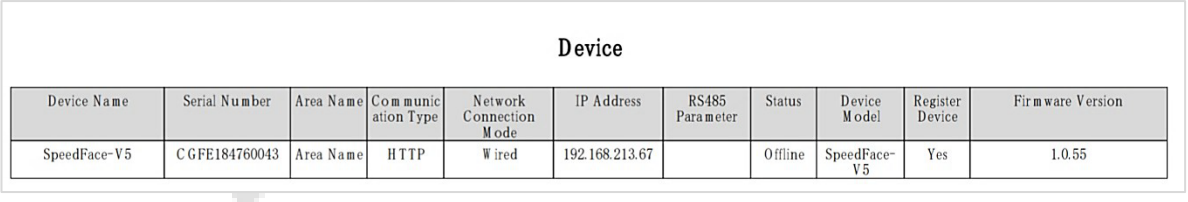


Para obter mais detalhes e configurações dos parâmetros acima, consulte Dispositivo. Alguns detalhes não podem ser editados. O nome do dispositivo deve ser único e não pode ser idêntico a outro dispositivo. O tipo de painel de controle não pode ser modificado. Se o tipo estiver incorreto, os usuários precisam excluir o dispositivo e adicioná-lo novamente manualmente.

- **Exportar**

As informações do dispositivo podem ser exportadas nos formatos de arquivo EXCEL, PDF e CSV.



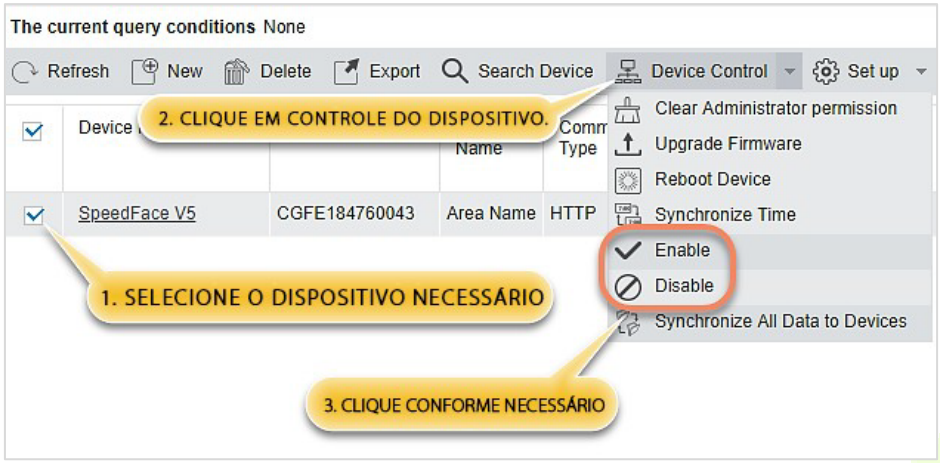


Device

Device Name	Serial Number	Area Name	Communication Type	Network Connection Mode	IP Address	RS485 Parameter	Status	Device Model	Register Device	Firmware Version
SpeedFace-V5	CGFE184760043	Area Name	HTTP	Wired	192.168.213.67		Offline	SpeedFace-V5	Yes	1.0.55

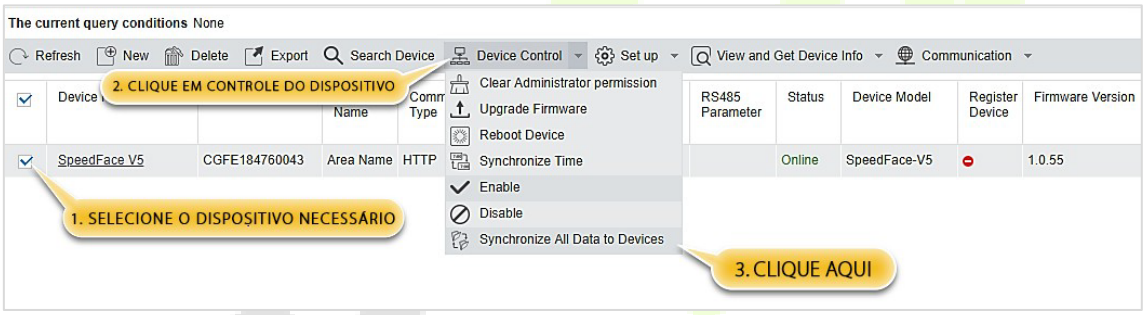
- **Desabilitar/Habilitar**

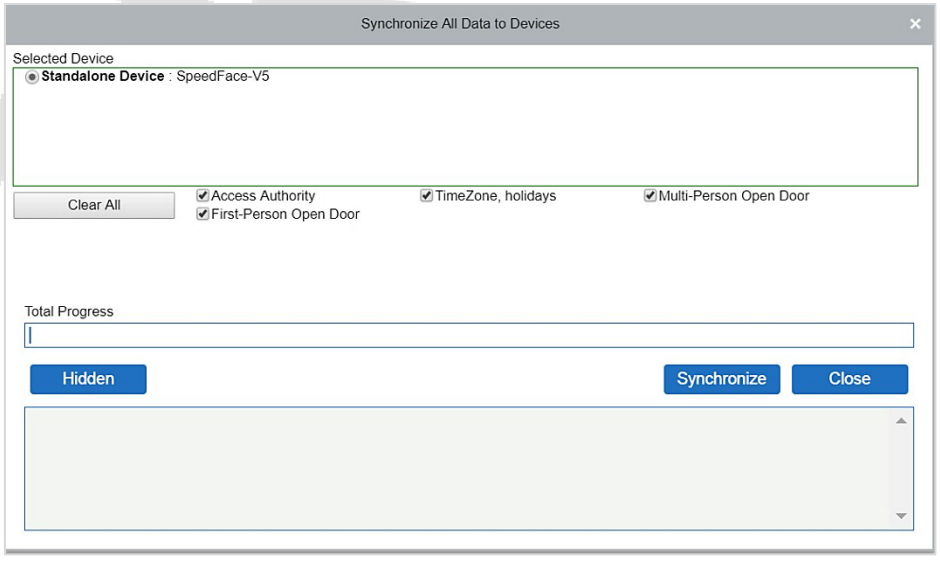
Selecione um dispositivo, clique em **Desabilitar/Habilitar** para parar/começar a usar o dispositivo. Quando a comunicação entre o dispositivo e o sistema for interrompida, ou quando o dispositivo falhar, o dispositivo poderá aparecer automaticamente em status desabilitado. Após ajustar a rede local ou o dispositivo, clique em Habilitar para reconectar o dispositivo e restaurar a comunicação do dispositivo.



- **<u>Sincronizar todos os dados nos dispositivos.</u>**

Para sincronizar os dados do sistema com o dispositivo, selecione o dispositivo e clique em **Sincronizar Todos os Dados nos Dispositivos** e clique em **OK** para concluir a sincronização.

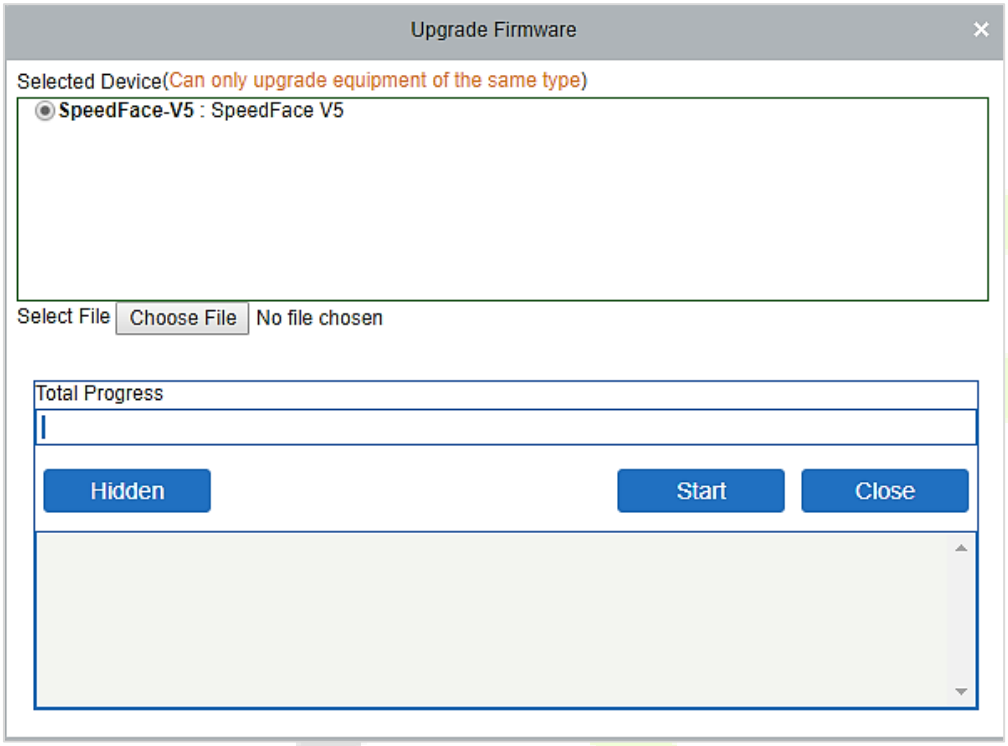




Observação: Sincronizar Todos os Dados nos Dispositivos irá primeiro excluir todos os dados no dispositivo (exceto as transações) e, em seguida, baixar todas as configurações novamente. Por favor, mantenha a conexão com a internet estável e evite situações de desligamento. Se o dispositivo estiver funcionando normalmente, use essa função com cautela. Execute-a apenas em situações excepcionais para evitar impacto no uso regular do dispositivo.

- **Atualizar o Firmware**

Selecione o dispositivo necessário que precisa ser atualizado, clique em **Atualizar firmware** para entrar na interface de edição, em seguida, clique em **Escolher arquivo** para selecionar o arquivo de atualização de firmware (nomeado emfw.cfg) fornecido pelo software de Acesso, e clique em **OK** para iniciar a atualização.



Observação: O usuário não deve atualizar o firmware sem autorização. Entre em contato com o distribuidor antes de atualizar o firmware ou faça a atualização seguindo as instruções do distribuidor. A atualização não autorizada pode afetar as operações normais.

- **Reiniciar Dispositivo**

Isso reiniciará o dispositivo selecionado.

- **Sincronizar Hora**

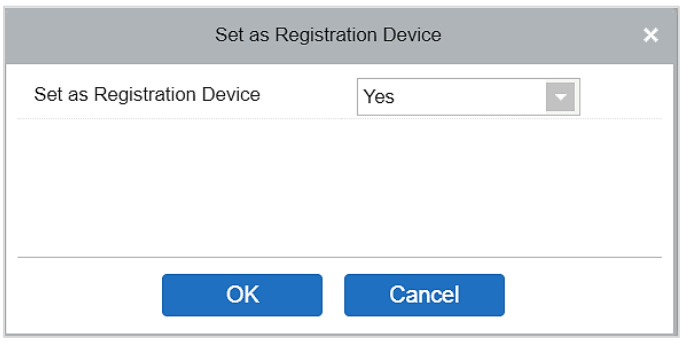
Isso irá sincronizar a hora do dispositivo com a hora atual do servidor.

- **Configurar Fuso Horário do Dispositivo**

Se o dispositivo suportar as configurações de fuso horário e não estiver no mesmo fuso horário do servidor, você precisará configurar o fuso horário do dispositivo. Após configurar o fuso horário, o dispositivo sincronizará automaticamente o horário de acordo com o fuso horário e a hora do servidor.

- **Definir como Dispositivo de Registro**

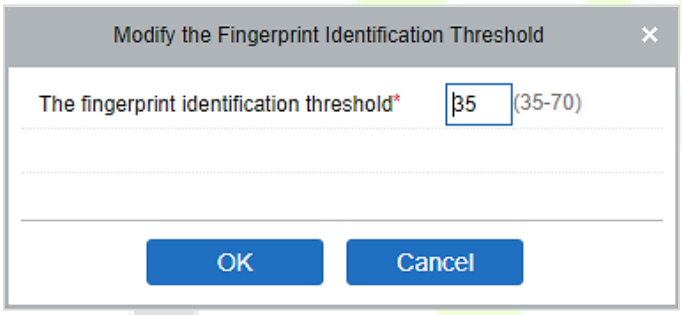
Defina o dispositivo de registro somente quando os dados do dispositivo independente, como pessoal, podem ser enviados automaticamente.



- **Configurar Horário de Verão**

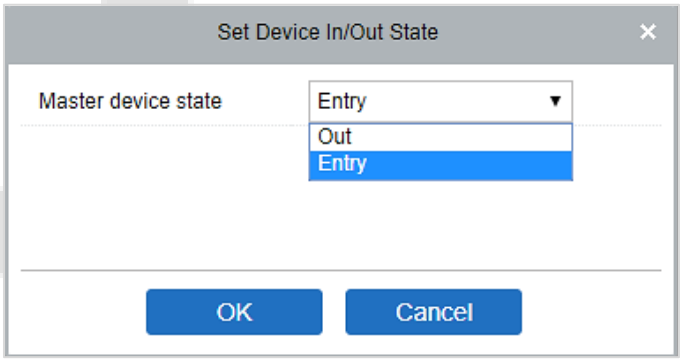
De acordo com os requisitos das diferentes regiões, configure as regras do Horário de Verão.

- **Modificar o limiar de identificação de impressão digital (Certifique-se de que o controlador de acesso suporta a função de impressão digital).**



- **Definir Estado de Entrada/Saída do Dispositivo**

Isso definirá a condição do dispositivo principal como Entrada ou Saída.

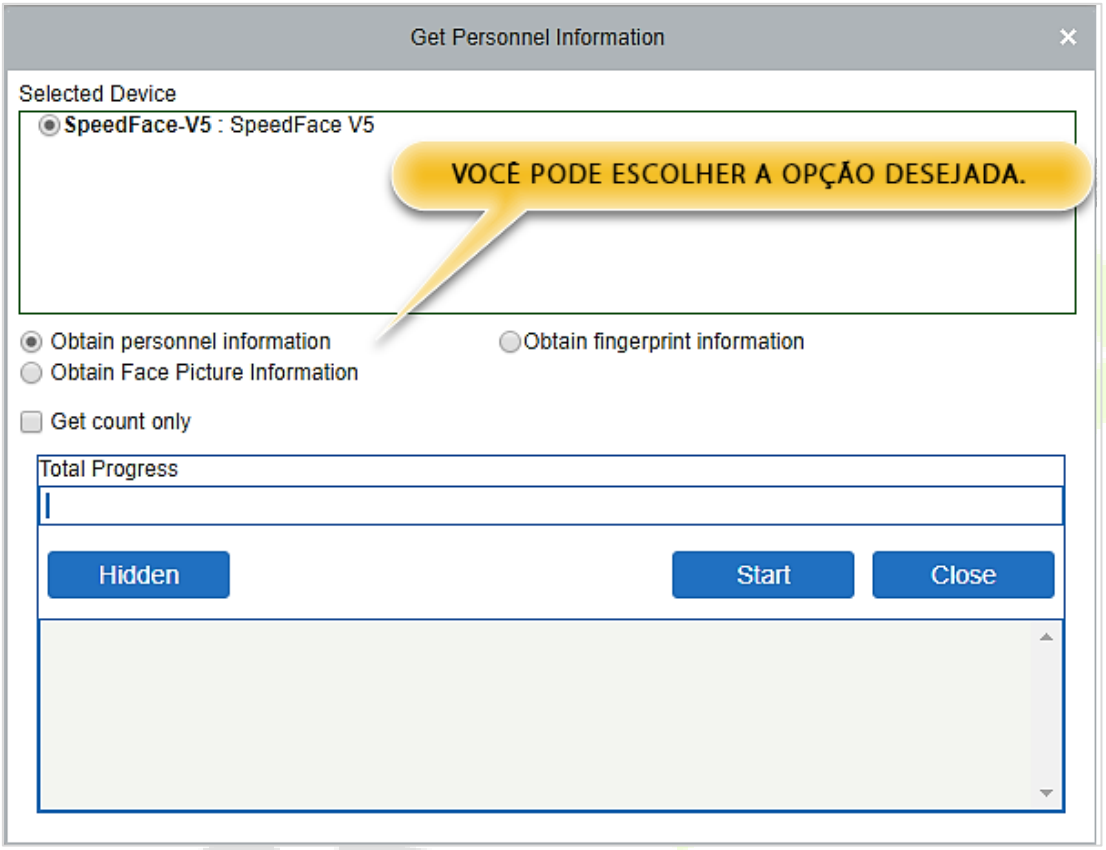


- **Obter Opções do Dispositivo**

Ele obtém os parâmetros comuns do dispositivo. Por exemplo, ele obtém a versão do firmware após o dispositivo ser atualizado.

- **Obter Informações do Pessoal**

Ele exibe o número atual de pessoal, impressões digitais, veias dos dedos e modelos faciais no dispositivo. O valor final será exibido na lista de dispositivos.



- **Obter Transações**

Ele recupera as transações do dispositivo para o sistema. Duas opções são fornecidas para essa operação: Obter Novas Transações e Obter Todas as Transações.

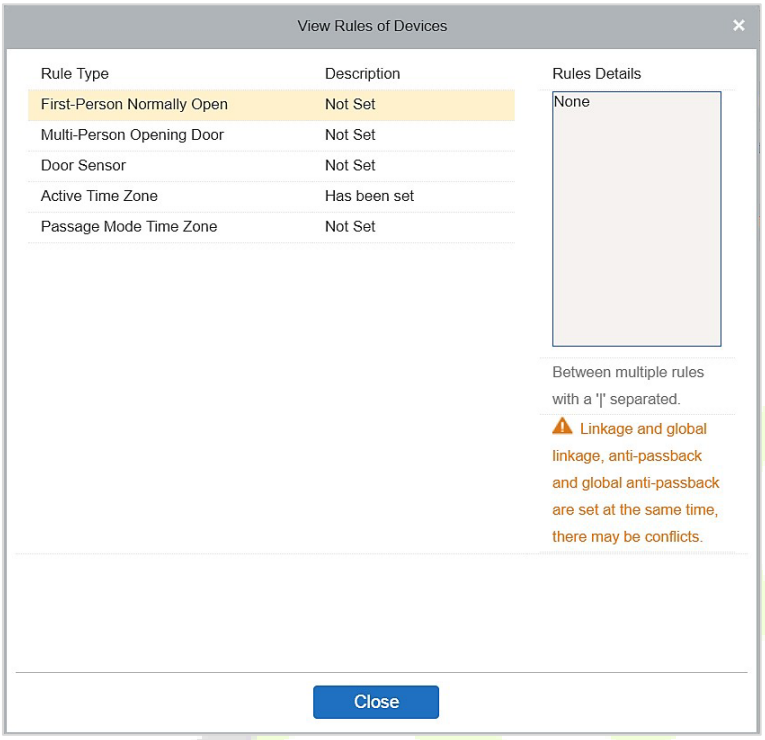
Obter Novas Transações: O sistema apenas obtém novas transações desde a última transação coletada e registrada. Transações repetidas não serão reescritas.

Obter Todas as Transações: O sistema obterá novamente todas as transações. Entradas repetidas não serão exibidas duas vezes. Quando o status da rede é saudável e a comunicação entre o sistema e o dispositivo está normal, o sistema adquire as transações do dispositivo em tempo real e as salva no banco de dados do sistema. No entanto, quando a rede é interrompida ou a comunicação é interrompida por qualquer motivo, e as transações do dispositivo não foram enviadas para o sistema em tempo real, o recurso **Obter Transações** pode ser usado para adquirir as transações do dispositivo manualmente. Além disso, por padrão, o sistema adquire automaticamente as transações do dispositivo às 00:00 de cada dia.

Observação: Uma controladora de acesso pode armazenar até 100 mil transações. Quando as transações excedem esse número, o dispositivo automaticamente exclui as transações armazenadas mais antigas (exclui 10 mil transações por padrão).

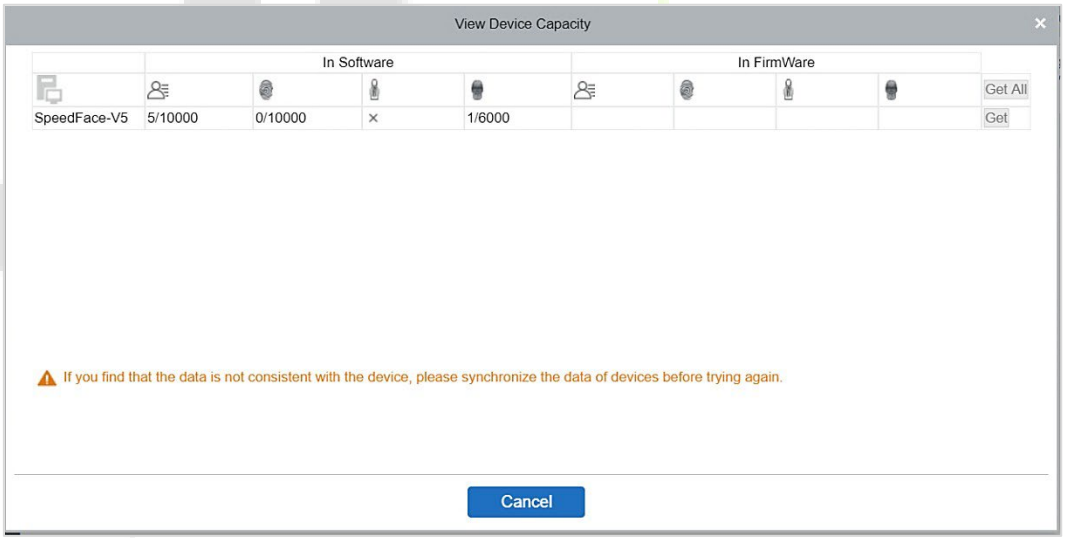
- **Visualizar Regras dos Dispositivos**

Mostra as regras de acesso no dispositivo.



- **Visualizar Capacidade do Dispositivo**

Isso exibe a capacidade de templates biométricos no dispositivo.



- **Modificar Endereço IP**

Selecione um dispositivo e clique em **[Modificar endereço IP]** para abrir a interface de modificação. Ele irá obter um gateway de rede e uma máscara de sub-rede em tempo real do dispositivo (se não conseguir, você não poderá modificar o endereço IP). Em seguida, digite um novo endereço IP, gateway e máscara de sub-rede. Clique em **OK** para salvar e sair. Esta função é semelhante à função [Modificar Endereço IP] no dispositivo.

- **Modificar Senha de Comunicação**

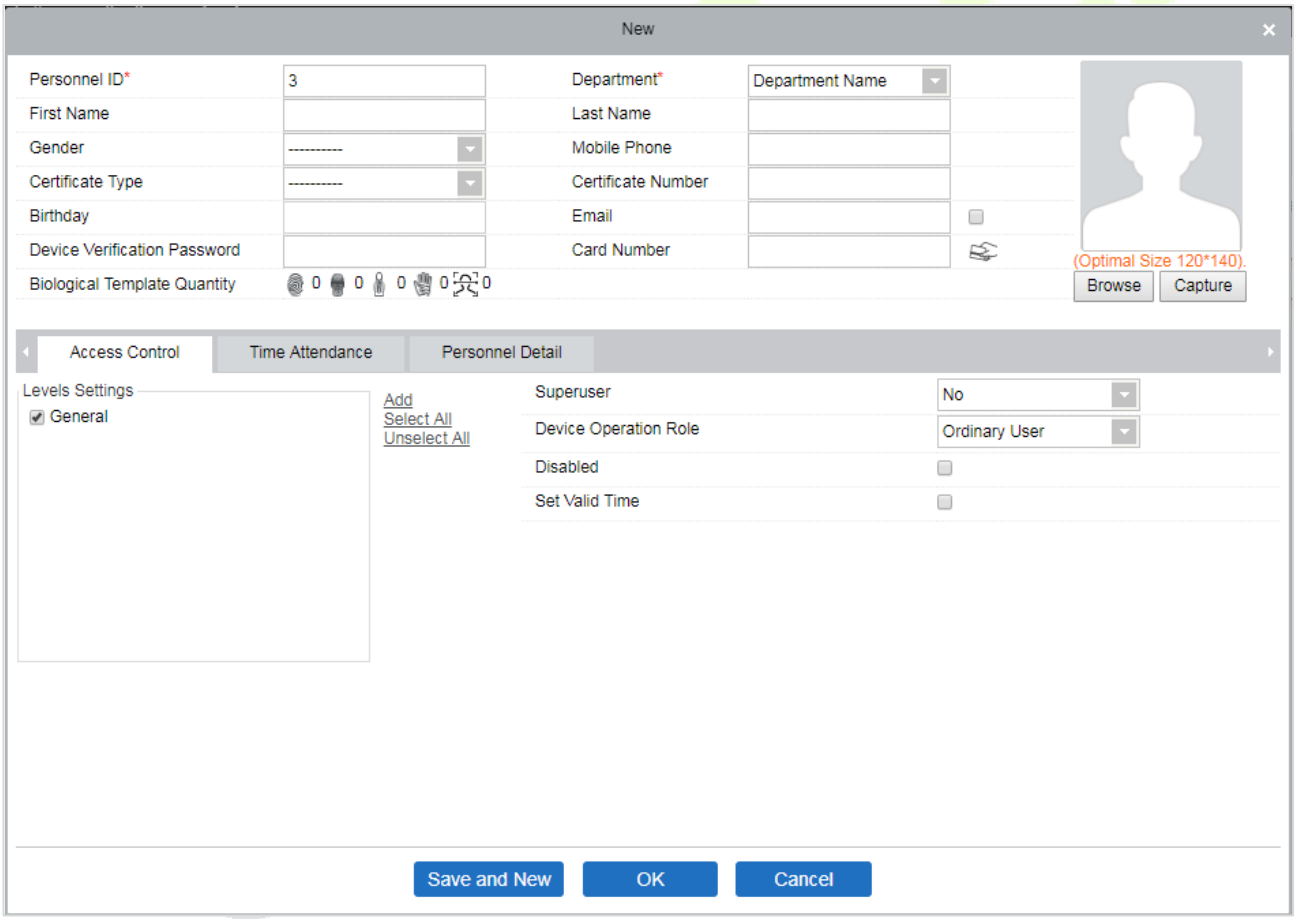
O sistema solicitará a senha antiga de comunicação antes de modificá-la. Após a verificação, digite a nova senha duas vezes e clique em **OK** para alterar a senha de comunicação.

Observação: A senha deve ser uma combinação de números e letras de 6 dígitos.

Os usuários podem modificar os limiares de identificação de impressões digitais nos dispositivos; eles variam de 35 a 70, sendo 55 o valor padrão. O sistema lerá os limiares do dispositivo. Os usuários podem visualizar a lista de dispositivos com limiares. Mais de um dispositivo pode ser alterado usando a função de operação em lote.

5.5 Adicionar um usuário e um cartão

1. Clique em **Gerenciamento de Pessoal > Pessoal > Novo**.



Os campos são os seguintes:

ID do pessoal: Um ID pode ter até 9 caracteres, dentro do intervalo de 1 a 79999999. Ele pode ser configurado com base em suas necessidades. O ID do pessoal contém apenas números por padrão, mas também pode incluir letras.

Observação:

1. Ao configurar um número de pessoal, verifique se o dispositivo atual suporta o comprimento máximo e se letras podem ser usadas no ID do pessoal.
2. Para editar as configurações do número máximo de caracteres de cada número de pessoal e se letras também podem ser usadas, clique em **Pessoal > Parâmetros.**

Departamento: Selecione no menu suspenso e clique em **OK**. Se o departamento não tiver sido definido anteriormente, aparecerá apenas um departamento chamado "Nome da Empresa".

Nome/Sobrenome: O número máximo de caracteres é 50.

Gênero: Defina o gênero do funcionário.

Telefone Celular: Digite o número de telefone do usuário.

Tipo de Documento: Existem quatro tipos de documentos: RG, Passaporte, Carteira de Motorista e outros.

Número do Documento: Insira o número do documento.

Data de Nascimento: Insira a data de nascimento do funcionário.
E-mail: Insira o e-mail do funcionário. O comprimento máximo é de 30 caracteres.

Senha de Verificação no Dispositivo: Defina a senha para verificação com o dispositivo usando as contas de pessoal. Ela pode conter apenas até 6 dígitos. Não pode ser igual à senha de outros usuários nem à senha de emergência.

Número do Cartãor: O comprimento máximo é de 10 caracteres e não deve ser repetido.

Foto Pessoal: A função de visualização de imagens é fornecida, suportando formatos comuns de imagens, como JPG, JPEG, BMP, PNG, GIF, etc. O tamanho ideal é de 120×140 pixels.

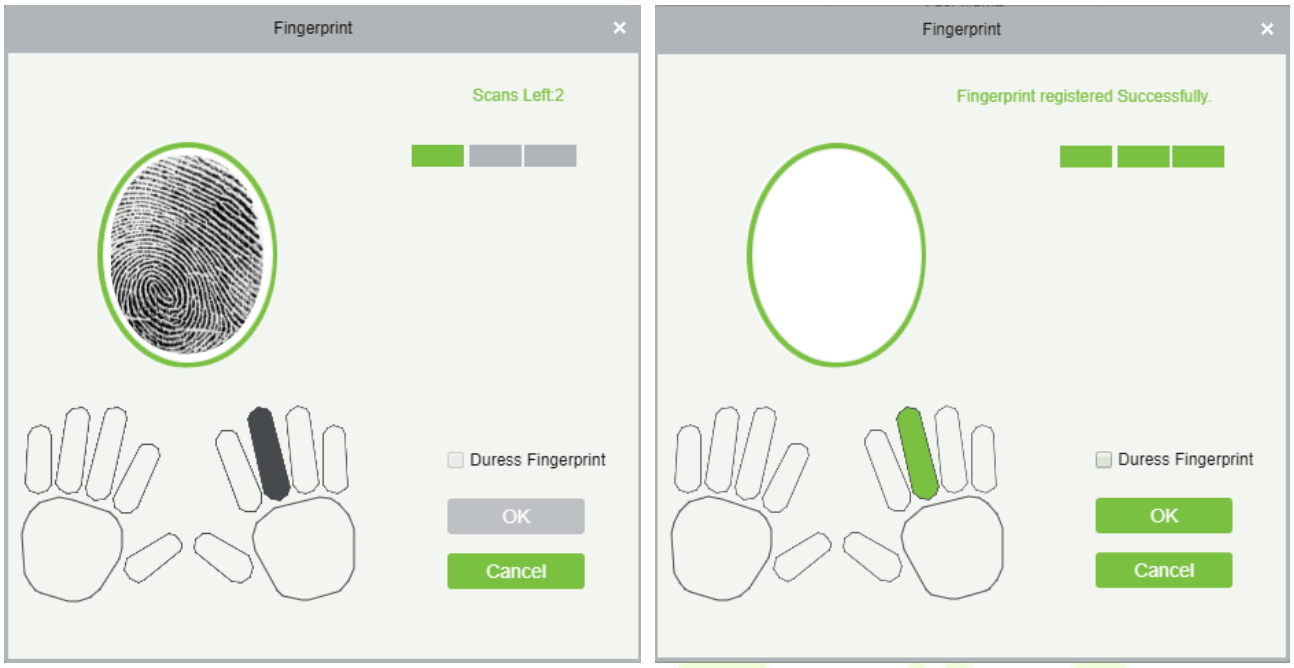
Procurar: Clique em **Procurar** para selecionar uma foto em seu disco local para fazer o upload.

Capturar: É permitido tirar uma foto com uma câmera quando o servidor está conectado a uma câmera.

Registrar Impressão Digital / Veia do Dedo: Matricule a Impressão Digital, Veia do Dedo, Palma ou Rosto do Funcionário. Para acionar o alarme e enviar o sinal ao sistema, escaneie a Impressão Digital de Emergência.

Como registrar a impressão digital:

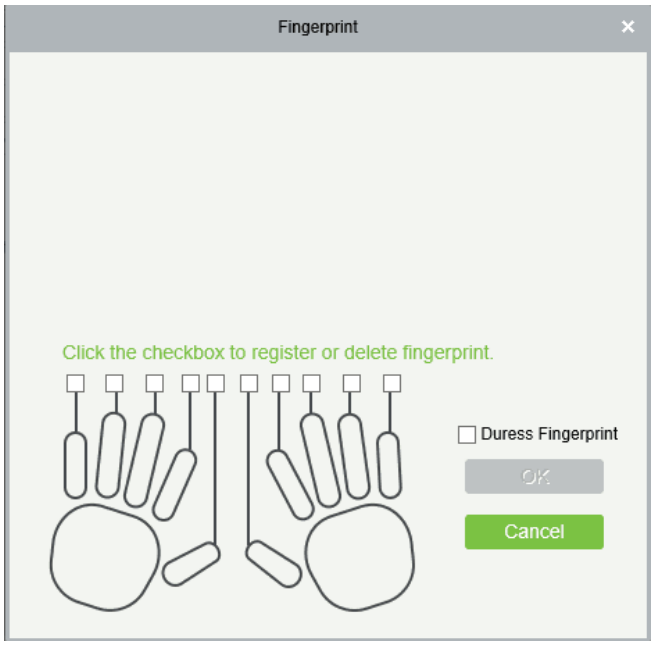
1. Mova o cursor para a posição do ícone de impressão digital, uma janela pop-up de registro ou uma caixa de diálogo para download de drivers aparecerá, clique em **Registrar**.
2. Selecione uma impressão digital, pressione o dedo no sensor continuamente até que a mensagem **"Impressão digital registrada com sucesso"** seja exibida.
3. Clique em **OK** para concluir o registro.

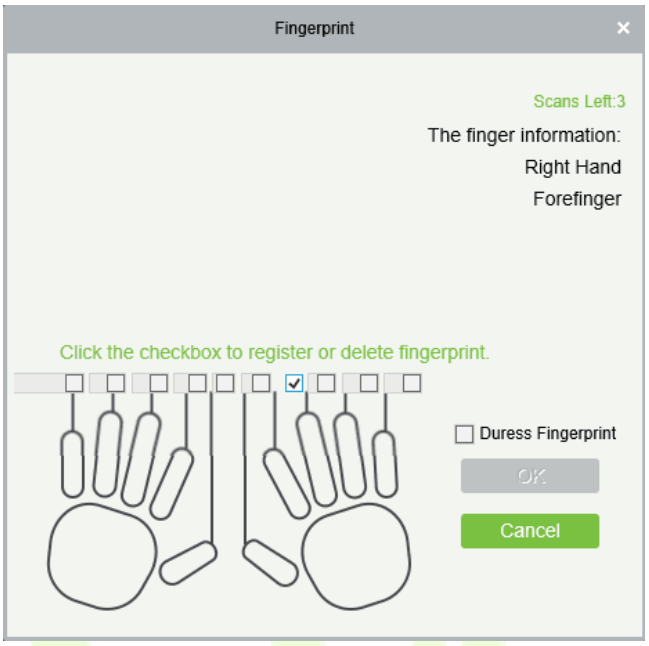


Clique em uma impressão digital para excluir. Se você precisar registrar uma impressão digital de emergência, marque a caixa de seleção "Impressão Digital de Emergência".

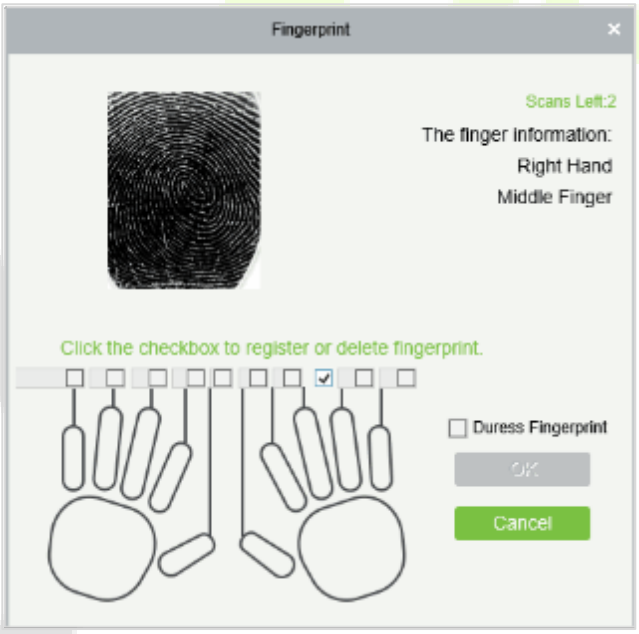
Observações:

1. Se as impressões digitais estiverem duplicadas, será exibida a mensagem "Não repita a entrada da impressão digital".
2. Se o driver do sensor de impressão digital não estiver instalado, clique em "Instalar driver" e o sistema solicitará o download e a instalação do driver.
3. Após instalar o driver do sensor de impressão digital, se o botão de registro de impressão digital estiver cinza no navegador IE, mas normal em outros navegadores (como Firefox, Google), você pode alterar as configurações do navegador IE da seguinte forma:
   a) No Internet Explorer, clique em **Ferramentas > Opções da Internet > Segurança > Sites Confiáveis**, adicione http://localhost aos sites confiáveis e, em seguida, reinicie o Internet Explorer.
   b) b) No Internet Explorer, clique em **Ferramentas > Opções da Internet > Avançadas > Redefinir** para abrir uma caixa de diálogo de Redefinir Configurações do Internet Explorer, clique em **Redefinir** para confirmar e, em seguida, reinicie o Internet Explorer (você pode tentar quando o Ponto 1 não ajudar).
   c) c) Se todas as configurações acima não funcionarem, execute as seguintes operações (usando o navegador IE11 como exemplo): clique em **Ferramentas > Opções da Internet > Avançadas > Segurança**, marque a opção [Permitir que o software seja executado ou instalado mesmo que a assinatura seja...] e desmarque a opção [Verificar revogação do certificado do servidor], em seguida, reinicie o IE.
   d) d) Se a versão do navegador for anterior ao IE8, a página de registro de impressões digitais será diferente:

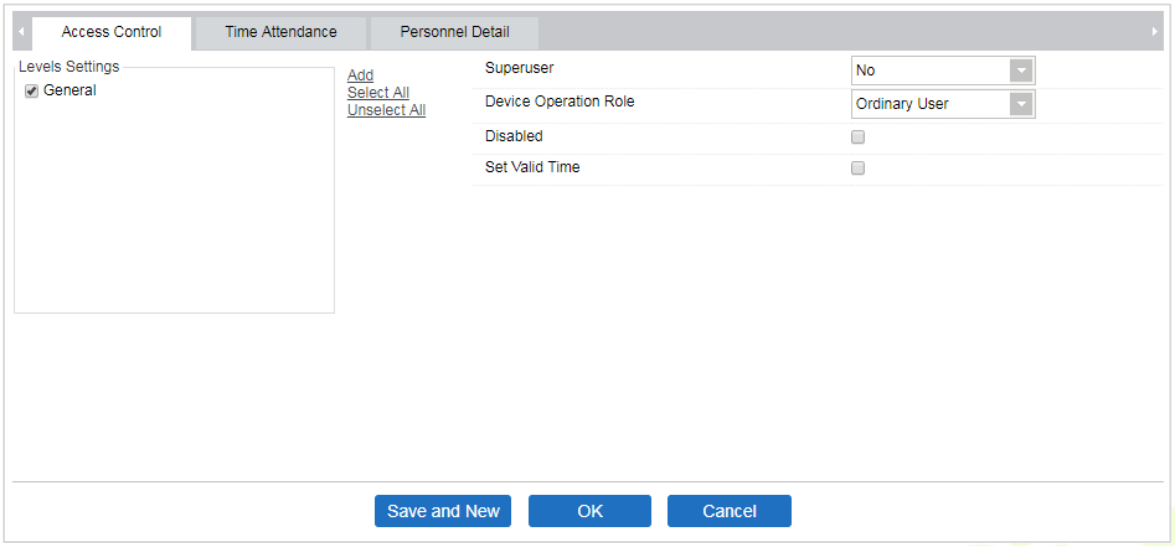




e) O sistema suporta o acesso pelo dispositivo de impressão digital Live20R e a função de prevenção de falsificação de impressão digital.

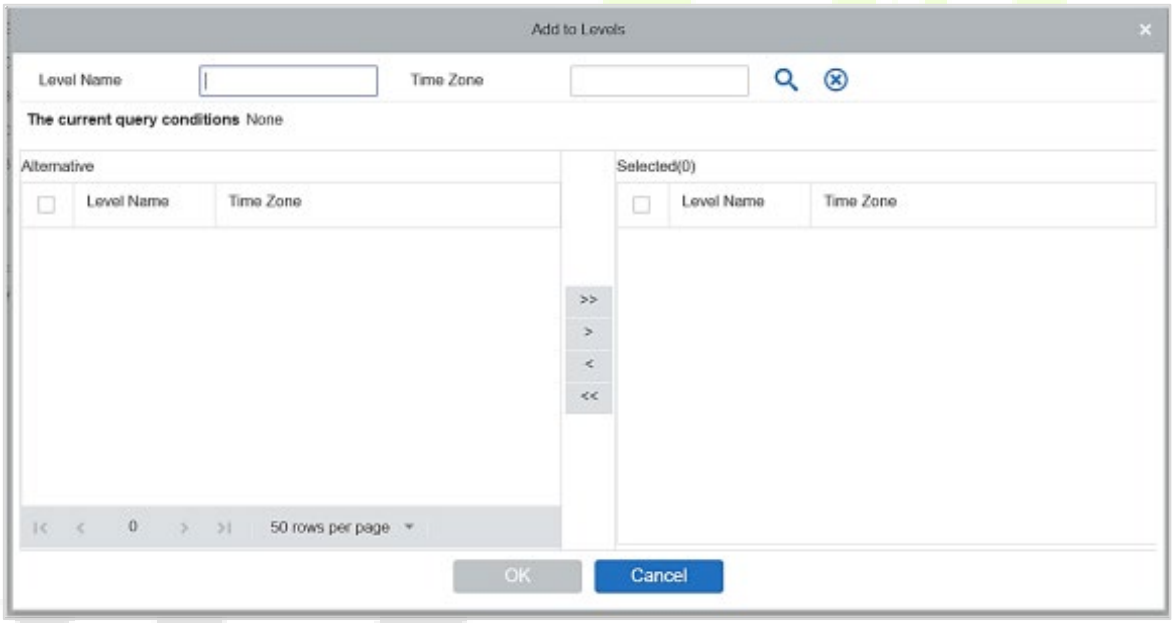


4. Para configurar os parâmetros de Controle de Acesso para o pessoal, clique em **Controle de Acesso.**



Os campos são os seguintes:

Configurações de Nível: Clique em **Adicionar** e, em seguida, defina as regras de passagem de posições específicas em diferentes fusos horários.



Superusuário: Na operação do controlador de acesso, um superusuário não está sujeito às restrições dos fusos horários e possui uma prioridade extremamente alta de abertura de portas.

Função de Operação do Dispositivo: Ela definirá o nível de autoridade no dispositivo do usuário.

Desabilitado: Desativa temporariamente o nível de acesso do pessoal.

Definir Horário Válido: As portas podem ser configuradas para abrir apenas em períodos específicos. Se a caixa de seleção não estiver marcada, a porta estará sempre aberta.

Observação: O sistema irá automaticamente buscar os números relevantes na biblioteca de partidas durante a verificação.

A Lista de Informações do Pessoal, por padrão, é exibida como uma tabela. Se a opção de Exibição Gráfica for selecionada, fotos e números serão mostrados. Coloque o cursor em cima de uma foto para visualizar os detalhes sobre o pessoal.

Observações:

- Nem todos os dispositivos suportam a função "Desabilitado". Quando um usuário adiciona um dispositivo, o sistema notificará o usuário se o dispositivo atual suporta ou não essa função. Por favor, atualize o dispositivo para utilizar esta função.
- Nem todos os dispositivos suportam a função "Definir Horário Válido". Alguns dispositivos permitem apenas que os usuários definam o ano, mês e dia do horário local. Quando um usuário adiciona um dispositivo, o sistema notificará o usuário se o dispositivo atual suporta ou não essa função. Por favor, atualize o dispositivo para utilizar esta função.

1. Clique em **Detalhes do Pessoal** para acessar a interface de detalhes e edição, e insira as informações.

2. Após inserir as informações, clique em **OK** para salvar e sair. Os detalhes pessoais serão exibidos na lista adicionada.

5.6 Configurações de Controle de Acesso

O sistema de Controle de Acesso pode definir os níveis de acesso dos usuários registrados, ou seja, permitir que alguns funcionários abram determinadas portas por meio de verificação durante um período. A Gestão do Sistema de Controle de Acesso inclui principalmente Zonas de Tempo de Controle de Acesso, Feriados de Controle de Acesso, Configurações de Portas, Níveis de Acesso, Níveis de Acesso do Pessoal, Monitoramento em Tempo Real e Relatórios, etc.

Parâmetros do sistema de controle de acesso

- *255 fusos horários.*
- *Níveis de acesso ilimitados.*
- *Três tipos de feriados e um total de 96 feriados.*
- *Função de anti-retorno.*
- *Função de abertura multi-cartão.*
- *Monitoramento em tempo real.*
- *Função de intertravamento.*
- *Função de interligação.*
- *Função de abertura normal com o primeiro cartão.*
- *Configurações do leitor.*
- *Configurações de E/S auxiliares.*

Para obter mais detalhes, consulte o **"Manual do Usuário do ZKBioAccess".**

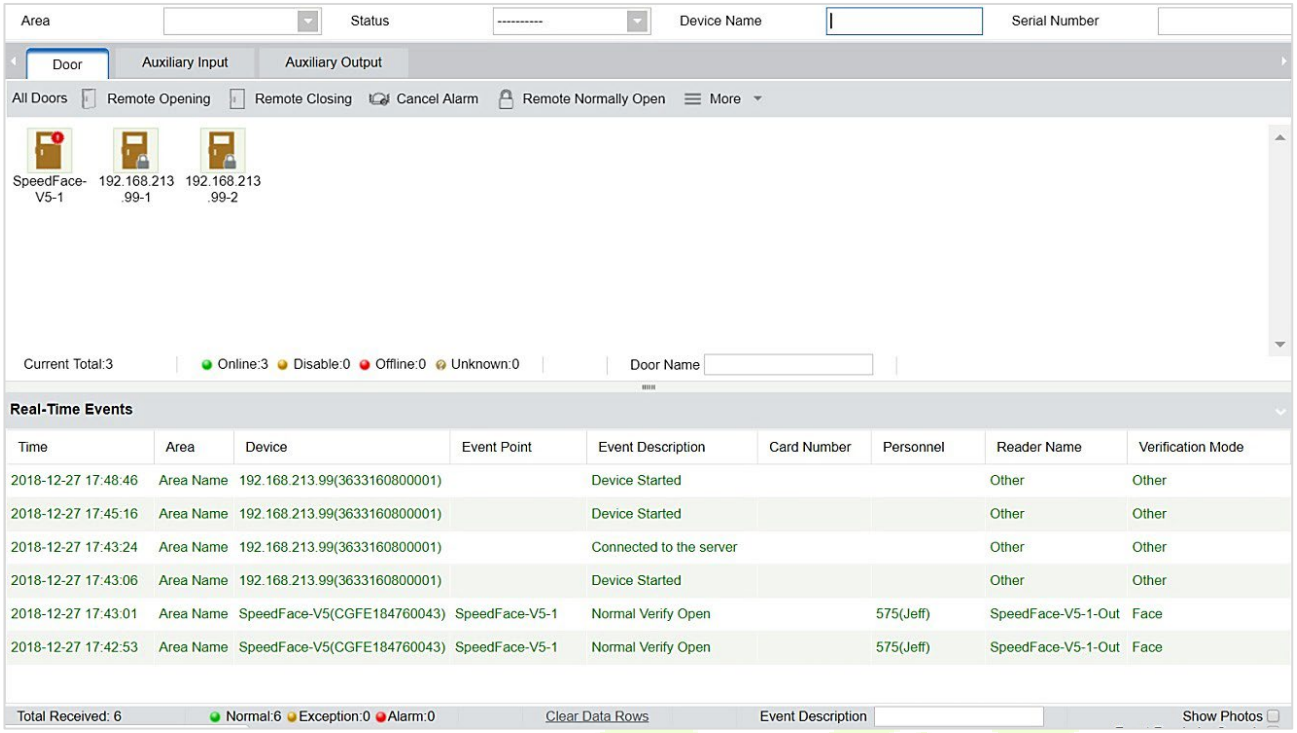
5.7 Monitoramento em tempo real

Clique em **Acesso ao Dispositivo > Monitoramento em Tempo Real**.

Ele monitora o status e os eventos em tempo real das portas configuradas nos painéis de controle de acesso do sistema, incluindo eventos normais e eventos anormais (incluindo eventos de alarme).

A interface de Monitoramento em Tempo Real é mostrada da seguinte forma:

Ícone	Status	Ícone	Status
	Dispositivo bloqueado		Porta offline
	Sensor da porta não configurado; relé fechado		Sensor da porta não configurado; relé aberto
	Sensor da porta não configurado e o firmware atual não suporta a ação atual no dispositivo		
	Status online: Porta fechada; Relé fechado		Status online: Porta fechada; Relé aberto
	Status online: Porta fechada e o firmware atual não suporta a ação atual no dispositivo		
	Status online: Porta aberta; Relé fechado		Status online: Porta aberta; Relé aberto
	Status online: Porta aberta e o firmware atual não suporta a ação atual no dispositivo		
	Alarme de porta aberta; Relé fechado		Alarme de porta aberta; Relé aberto
	Tempo de abertura da porta expirado, relé fechado		Tempo de abertura da porta expirado, relé aberto
	Tempo de abertura da porta expirado e o firmware atual não suporta a ação atual no dispositivo		
	Tempo de abertura da porta expirado, relé fechado/sensor da porta fechado		Tempo de abertura da porta expirado, relé aberto/sensor da porta fechado
	Alarme de porta fechada; Relé fechado		Alarme de porta fechada; Relé aberto
	Alarme de porta fechada, indica que o firmware atual não suporta a ação atual no dispositivo		
	Sensor da porta não configurado, alarme de porta, relé fechado		Sensor da porta não configurado, alarme de porta, relé aberto
	Tempo de abertura da porta expirado, sem status de relé/sensor da porta fechado		Trava da porta
Sem status de relé, isso indica que o firmware atual não suporta a ação no dispositivo.			



Ícones diferentes representam os seguintes status:

1. Porta

Abertura/Fechamento Remoto: É possível controlar uma porta específica ou todas as portas.

Para controlar uma única porta, clique com o botão direito sobre ela e selecione **Abertura/Fechamento Remoto** na janela pop-up. Para gerenciar todas as entradas, clique diretamente em **Abertura/ Fechamento Remoto** na opção **Todos Atuais**.

Durante a abertura remota, o usuário pode definir a duração da abertura da porta (o padrão é 15 segundos). Você pode selecionar [**Habilitar Modo de Passagem Intradiário por Fusos Horários**] para permitir o modo de passagem intradiário por fusos horários ou definir a porta como "Abertura Normal", e então a porta não estará limitada a nenhum fusos horário (pode ser aberta a qualquer momento).

Para fechar uma porta, selecione [**Desabilitar Modo de Passagem Intradiário por Fusos Horários**] primeiro, para evitar que outros fusos horários de abertura normal abram a porta, e então selecione [**Fechamento Remoto**].

Observação: Se a [**Abertura/Fechamento Remoto**] falhar, verifique se os dispositivos estão desconectados ou não. Se estiverem desconectados, verifique a conectividade de rede.

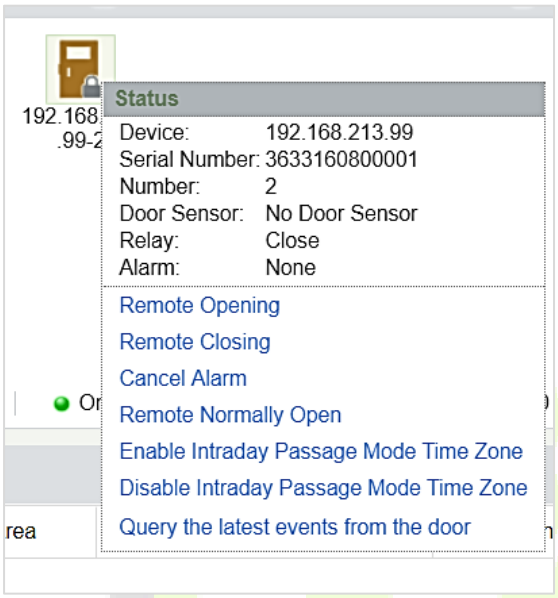
Cancelar o alarme: Quando uma porta com alarme aparecer na interface, o som do alarme será reproduzido. O cancelamento do alarme pode ser feito para uma única porta ou todas as portas. Para controlar uma única porta, mova o cursor sobre o ícone da porta, um menu será exibido e, em seguida, clique em **Abertura/Fechamento Remoto** no menu. Para gerenciar todas as portas, clique diretamente em **Abertura/Fechamento Remoto** na opção **Todos Atuais**.

Observação: Se o cancelamento do alarme falhar, verifique se há dispositivos desconectados. Se houver, verifique a rede.

Abertura Normal Remota: Isso irá configurar o dispositivo como Normalmente Aberto de forma remota.

- **Gerenciamento rápido das portas**

Se você mover o cursor sobre o ícone de uma porta, poderá realizar rapidamente as operações explicadas acima. Além disso, você pode consultar os eventos mais recentes da porta.

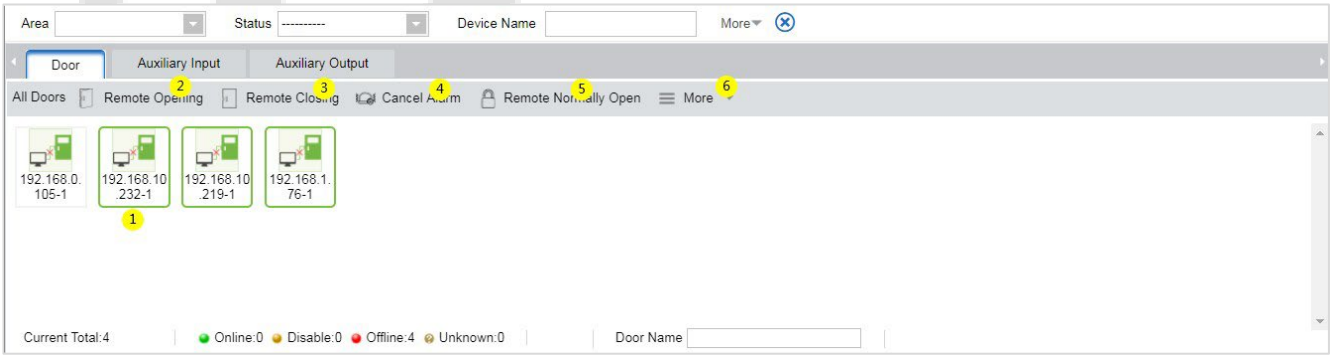


Consultar os eventos mais recentes da porta: Clique para visualizar rapidamente os eventos atuais da porta.

Emitir um cartão para uma pessoa: Se você inserir um cartão não registrado, um registro com um número de cartão será exibido na interface de monitoramento em tempo real. Clique com o botão direito nesse número de cartão e um menu será exibido. Clique em **Emitir cartão para pessoa** para atribuir esse cartão a uma pessoa.

- **Seleções múltiplas**

Você pode selecionar várias portas ao mesmo tempo para realizar operações como abertura remota, fechamento remoto, cancelamento de alarme, etc. Dê um duplo clique no ícone da porta para editar as propriedades da porta.



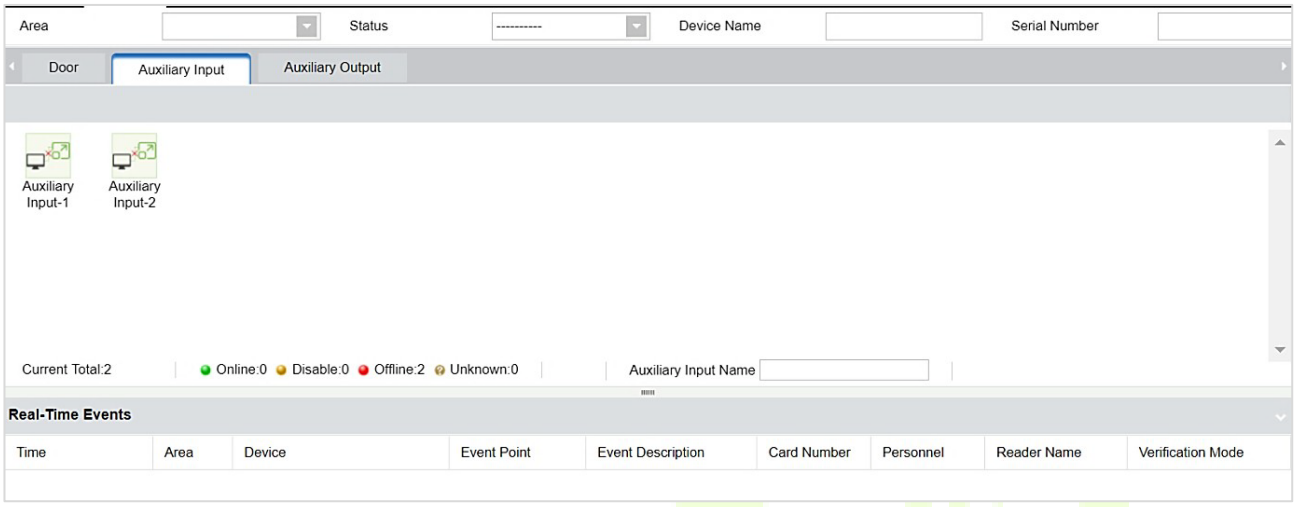
- **Monitoramento de eventos**

O sistema irá adquirir automaticamente os registros dos dispositivos sendo monitorados (por padrão, exibe 200 registros), incluindo eventos normais e anormais de controle de acesso (incluindo eventos de

alarme). Os eventos normais aparecerão em verde; eventos de alarme aparecerão em vermelho; outros eventos anormais aparecerão em laranja.

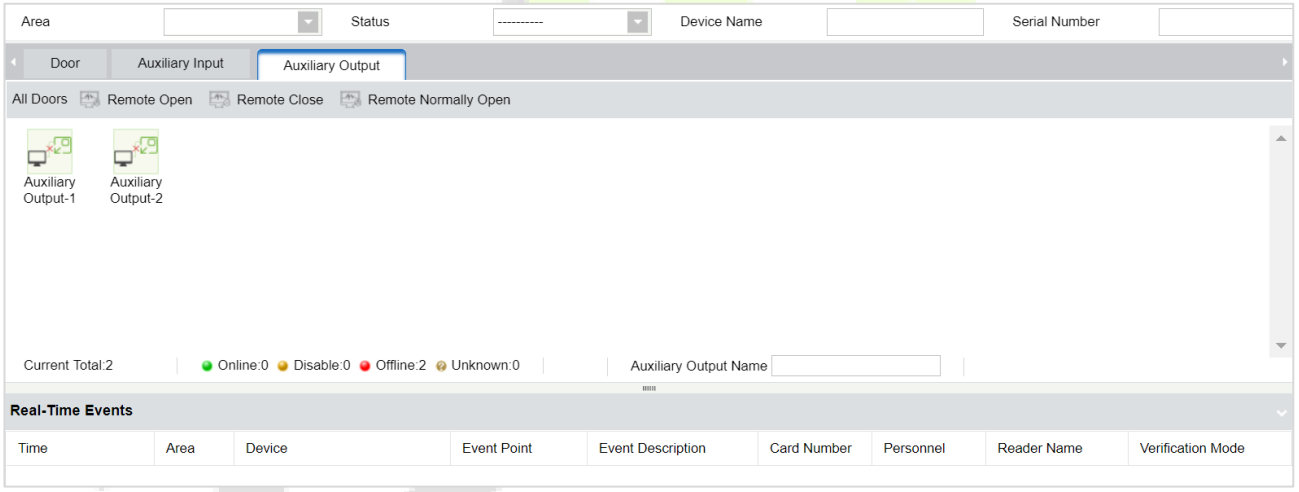
2. Entrada Auxiliar

Ele monitora em tempo real os eventos atuais de entrada auxiliar.



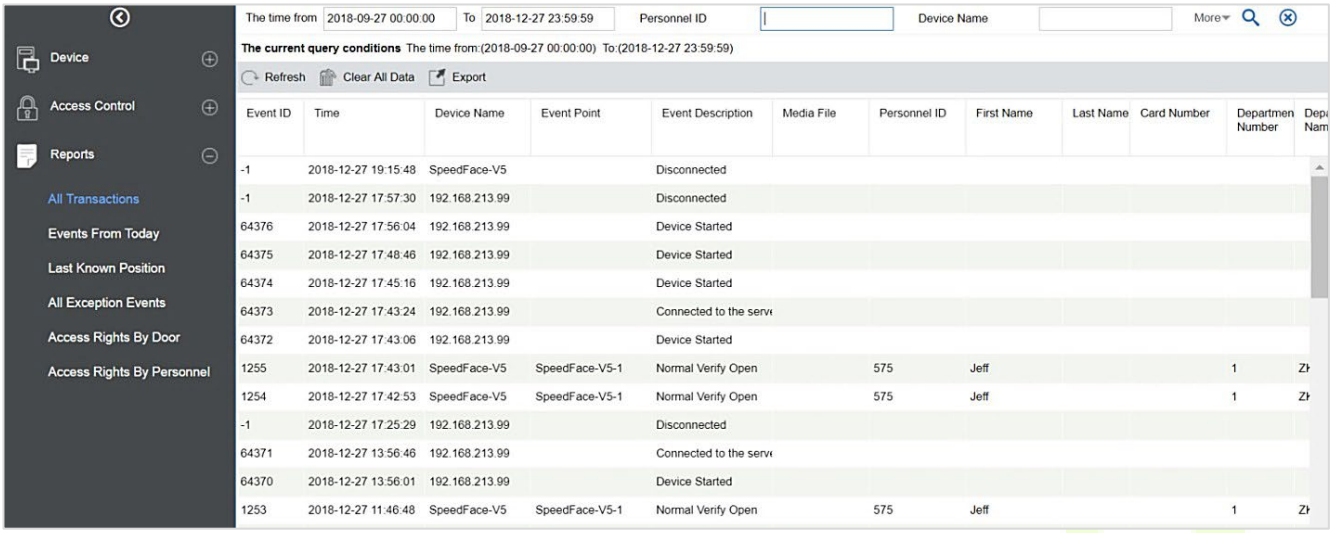
3. Saída Auxiliar

Aqui você pode realizar as funções de Abertura Remota, Fechamento Remoto e Abertura Normal Remota.



5.8 Relatórios

Como a quantidade de dados de eventos de controle de acesso é grande, você pode visualizar eventos de controle de acesso específicos por meio de condições de consulta. Por padrão, o sistema exibe as transações dos últimos três meses. Clique em **[Relatórios] > [Todas as Transações]** para visualizar todas as transações.



Arquivo de Mídia: Você pode visualizar ou baixar fotos e vídeos.

Limpar Todos os Dados: Essa função é usada para limpar todas as transações. Clique em **[Limpar Todos os Dados]**. Na janela pop-up que aparecer, clique em OK para remover todas as transações.

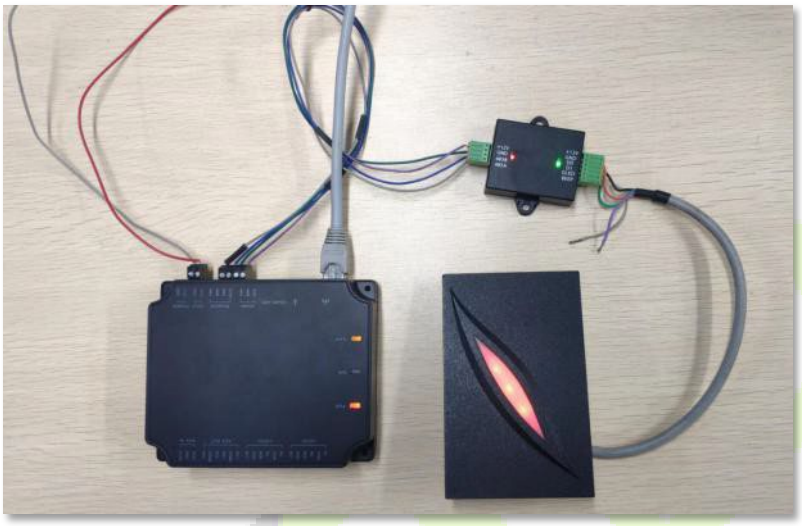
Exportar: Você pode exportar todas as transações em formato Excel, PDF e CSV.

All Transactions

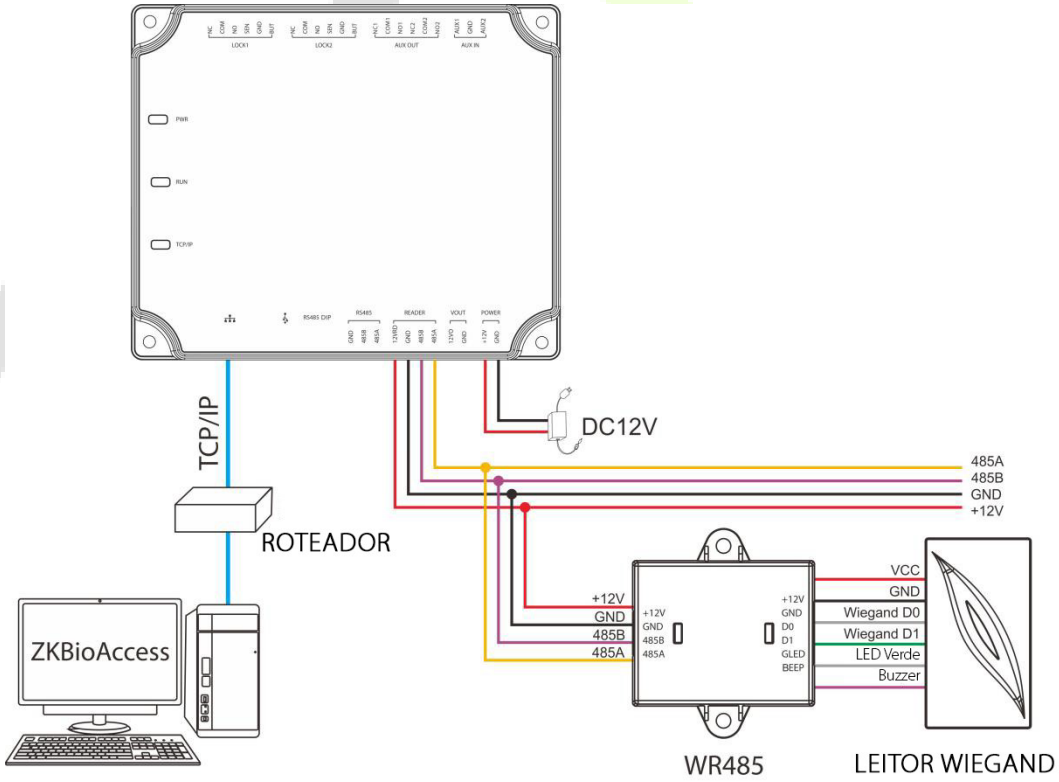
Event ID	Time	Device Name	Event Point	Event Description	Personnel ID	First Name	Last Name	Card Number	Department Number	Department Name	Reader Name	Verification Mode	Area Name	Remark
-1	2018-12-27 19:15:48	SpeedFace-V5		Disconnected							Other	Other	Area Name	
-1	2018-12-27 17:57:30	192.168.213.99		Disconnected							Other	Other	Area Name	
64376	2018-12-27 17:56:04	192.168.213.99		Device Started							Other	Other	Area Name	
64375	2018-12-27 17:48:46	192.168.213.99		Device Started							Other	Other	Area Name	
64374	2018-12-27 17:45:16	192.168.213.99		Device Started							Other	Other	Area Name	
64373	2018-12-27 17:43:24	192.168.213.99		Connected to the server							Other	Other	Area Name	
64372	2018-12-27 17:43:06	192.168.213.99		Device Started							Other	Other	Area Name	
1255	2018-12-27 17:43:01	SpeedFace-V5	SpeedFace-V5-1	Normal Verify Open	575	Jeff			1	ZKTeco	SpeedFace-V5-1-Out	Face	Area Name	
1254	2018-12-27 17:42:53	SpeedFace-V5	SpeedFace-V5-1	Normal Verify Open	575	Jeff			1	ZKTeco	SpeedFace-V5-1-Out	Face	Area Name	
-1	2018-12-27 17:25:29	192.168.213.99		Disconnected							Other	Other	Area Name	
64371	2018-12-27 13:56:46	192.168.213.99		Connected to the server							Other	Other	Area Name	
64370	2018-12-27 13:56:01	192.168.213.99		Device Started							Other	Other	Area Name	
1253	2018-12-27 11:46:48	SpeedFace-V5	SpeedFace-V5-1	Normal Verify Open	575	Jeff			1	ZKTeco	SpeedFace-V5-1-Out	Face	Area Name	

Apêndice 1

Demonstração operacional de conexão da C2-260, WR485 e leitor Wiegand:

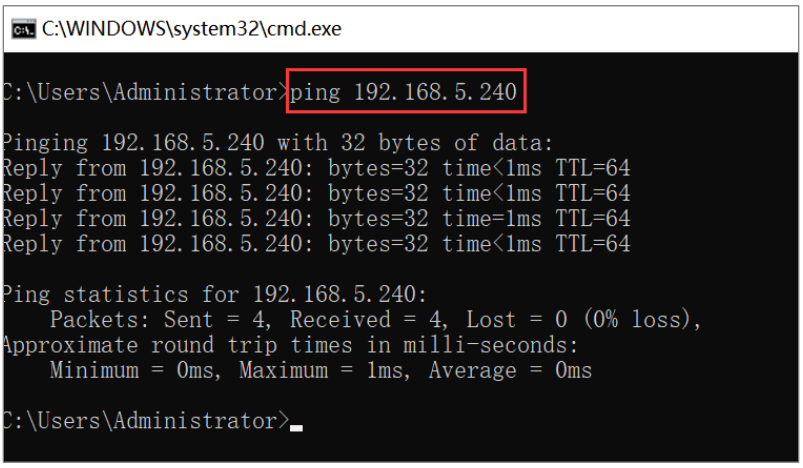


Passo 1: Conecte a C2-260, o WR485 e o leitor Wiegand de acordo com o seguinte diagrama de circuito.



Passo 2: Ligue a C2-260 e conecte-a à rede.

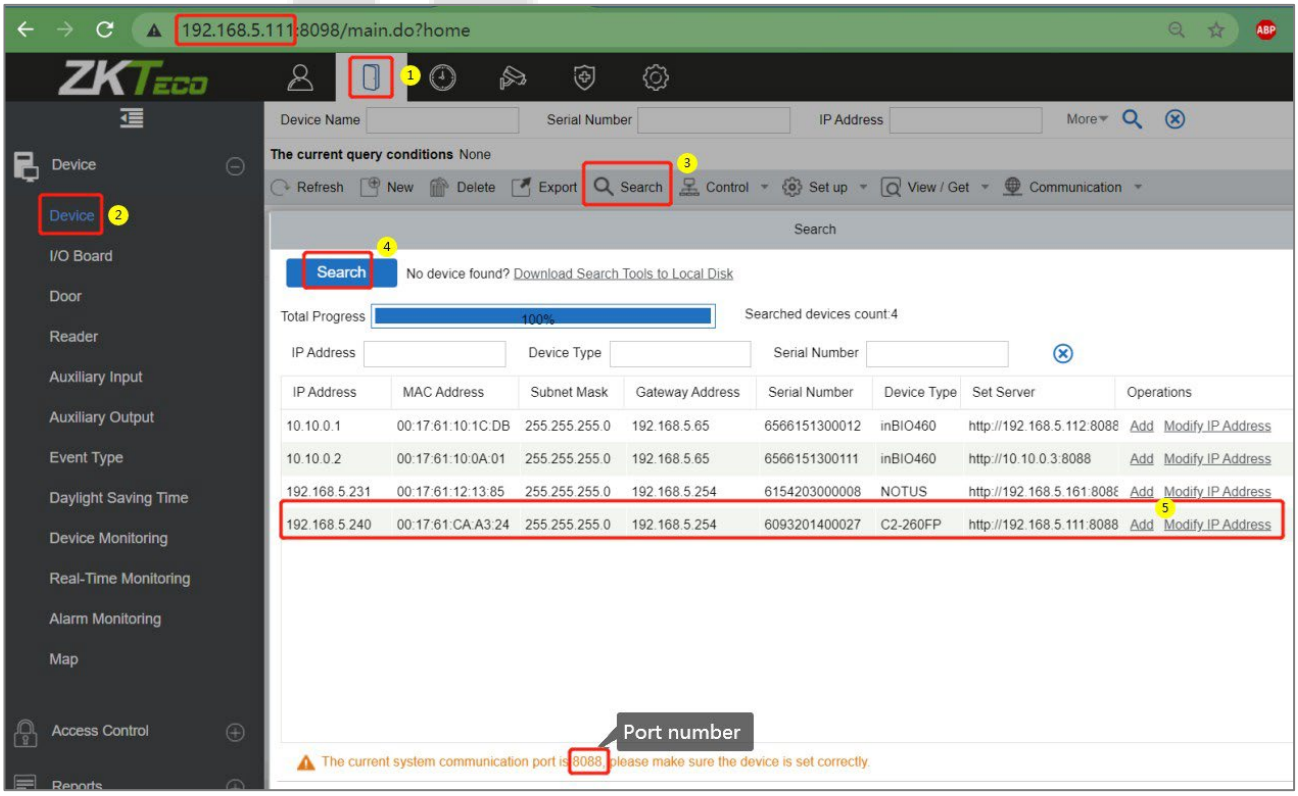
Passo 3: Faça o procedimento de ping na C2-260 para verificar se a rede está funcionando corretamente.



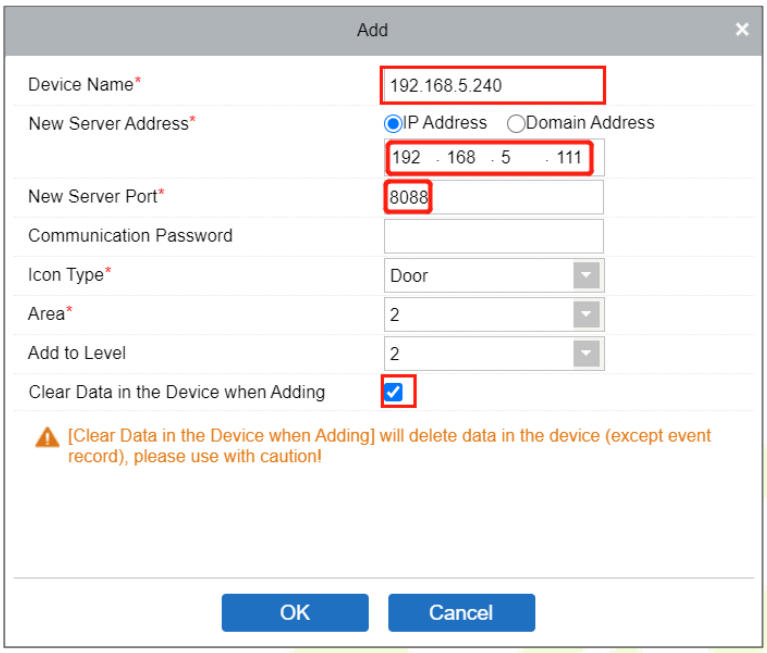
1) Pressione **[Windows + R]** no computador ao mesmo tempo para abrir a janela **Executar** e digite **"cmd".**
2) Digite "ping device IP address" para fazer ping na C2-260 e verificar se a comunicação está conectada. Conforme mostrado na figura acima.

Passo 4: Adicionar o dispositivo no software ZKBioAccess IVS.

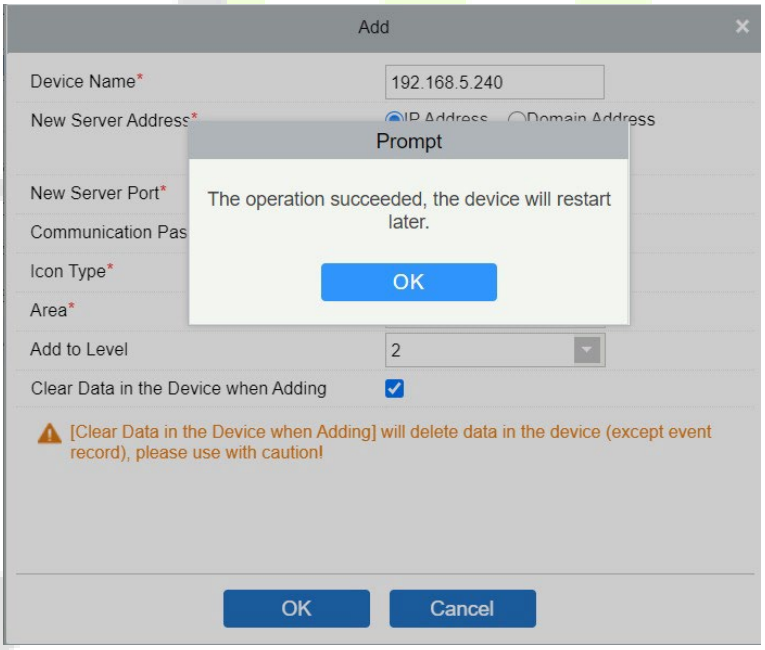
1) Abra o software ZKBioAccess IVS e clique em **Acesso > Dispositivo > Buscar** para entrar na interface de busca. Clique em **Buscar** para procurar o dispositivo.
2) Após a busca ser concluída, o número da porta será exibido na parte inferior da interface de busca. A partir da imagem a seguir, podemos ver o IP do servidor (**192.168.5.111**) e o número da porta (**8088**).



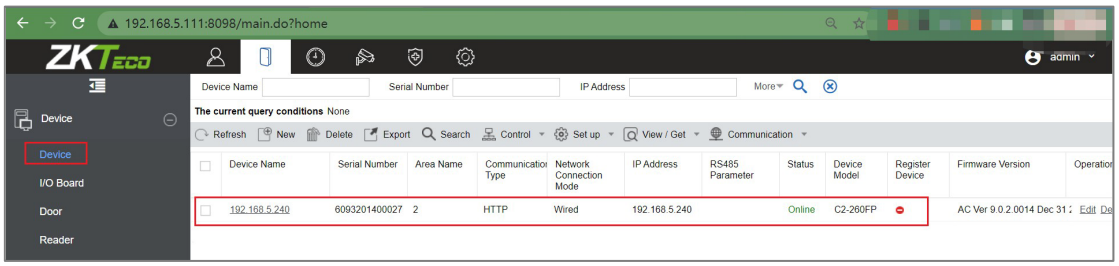
3) Clique em **Adicionar** na lista de busca. Em seguida, insira o endereço do servidor(**192.168.5.111**), a porta (**8088**) e os outros parâmetros na janela pop-up.



4) Clique em **OK** para salvar a configuração. A seguinte janela será exibida se o dispositivo for adicionado com sucesso.

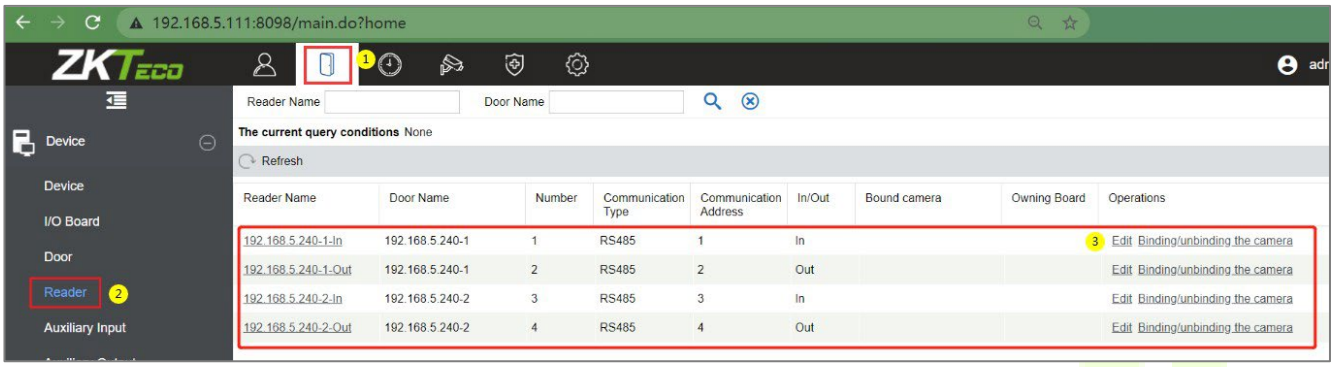


5) Após a conclusão, o dispositivo adicionado ao software será exibido na lista de dispositivos.



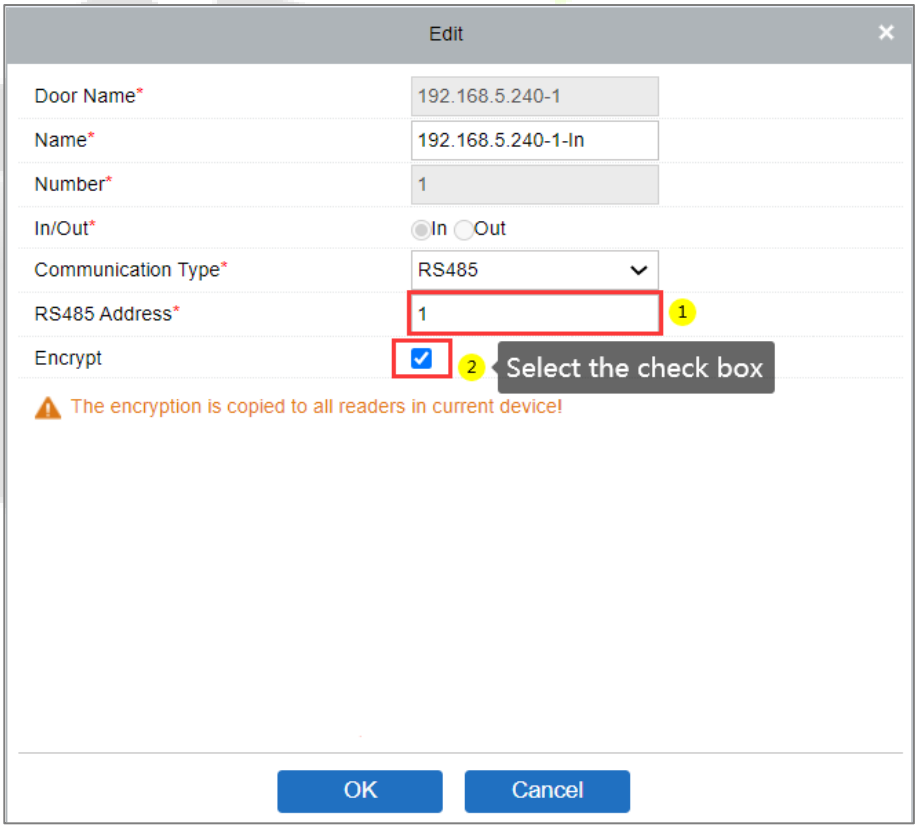
Passo 5: Configurando os parâmetros do leitor Wiegand.

1) Após adicionar a C2-260 ao software, clique em Acesso > Dispositivo > Leitor para visualizar o leitor.



2) Defina o endereço WR485 como 1. Colocando o Nº1 da chave DIP na posição LIGADO. Isso significa que o leitor Wiegand, que está conectado através do WR485, será configurado como leitor da Porta 1 (Entrada) (Observação: é recomendado configurar os endereços WR485 pela chave DIP antes de fornecer alimentação).

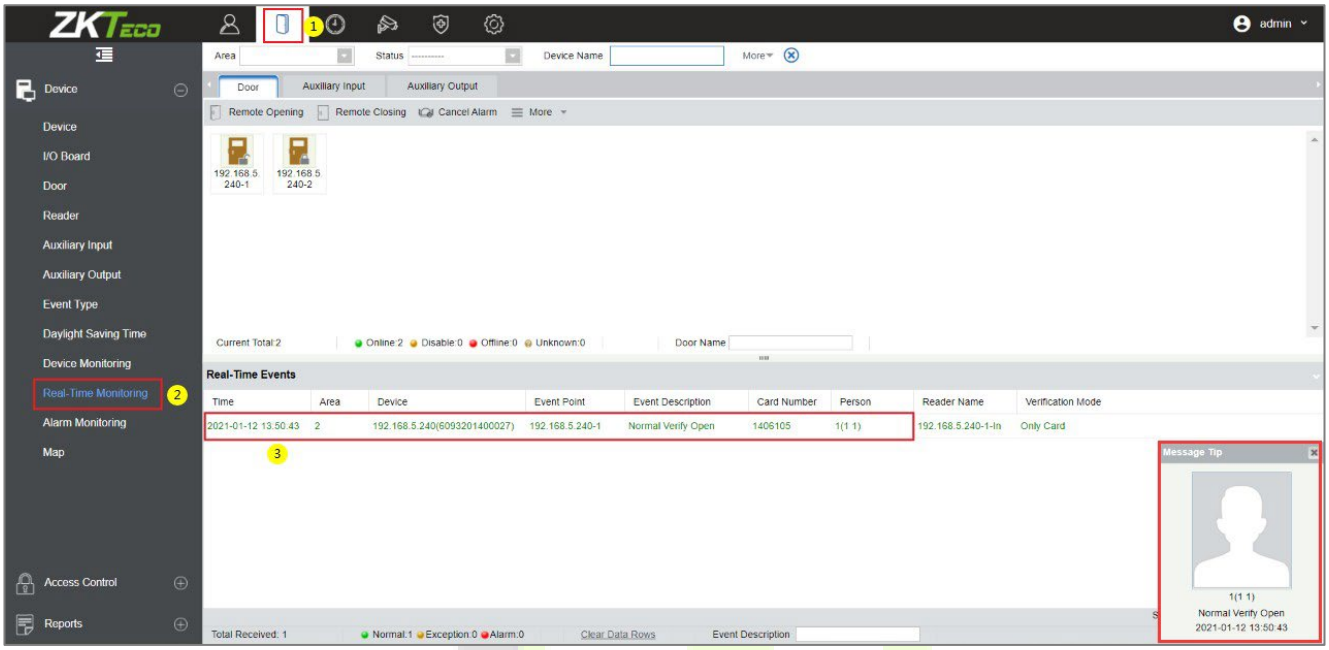
3) Clique em **Editar** "192.168.5.240-1-In" para configurar os parâmetros. Como o WR485 está em modo de criptografia, você precisa selecionar a caixa de seleção de criptografia. Isso permitirá que o leitor Wiegand seja usado normalmente. Conforme mostrado na figura a seguir.



Passo 6: Visualizar os registros em tempo real.

Após a configuração ser concluída com sucesso, quando o funcionário passar o cartão no leitor Wiegand, o evento em tempo real poderá ser visualizado na página de **Monitoramento em Tempo Real**.

Clique em **Acesso > Dispositivo > Monitoramento em Tempo Real** para visualizar os registros.



Apêndice 2

Declaração sobre o Direito à Privacidade

Prezados clientes,

Agradecemos por escolherem nosso produto híbrido de reconhecimento biométrico, projetado e fabricado pela ZKTeco. Como provedores renomados de tecnologias de reconhecimento biométrico, estamos constantemente desenvolvendo e pesquisando novos produtos, e nos esforçamos para seguir as leis de privacidade de cada país onde nossos produtos são vendidos.

Declaramos que:

1. Todos os nossos dispositivos de reconhecimento de impressão digital civil capturam apenas características, não imagens das impressões digitais, e não envolvem proteção de privacidade.
2. Nenhuma das características da impressão digital que capturamos pode ser utilizada para reconstruir uma imagem da impressão digital original e não envolvem proteção de privacidade.
3. Como provedores deste dispositivo, não assumiremos qualquer responsabilidade direta ou indireta por quaisquer consequências que possam resultar do uso deste dispositivo.
4. Se você deseja contestar questões de direitos humanos ou privacidade relacionadas ao uso de nosso produto, entre em contato diretamente com seu revendedor.

Nossos outros dispositivos de impressão digital para aplicação em aplicação da lei ou ferramentas de desenvolvimento podem capturar as imagens originais das impressões digitais dos cidadãos. Quanto a se isso constitui ou não uma violação de seus direitos, por favor, entre em contato com seu governo ou o fornecedor final do dispositivo. Como fabricante do dispositivo, não assumiremos qualquer responsabilidade legal.

Observação: A lei chinesa inclui as seguintes disposições sobre a liberdade pessoal de seus cidadãos:

1. Não deve haver prisão, detenção, busca ilegal ou violação de pessoas.
2. A dignidade pessoal está relacionada à liberdade pessoal e não deve ser infringida.
3. A residência de um cidadão não pode ser violada.
4. O direito de comunicação de um cidadão e a confidencialidade dessa comunicação são protegidos pela lei.

Como último ponto, gostaríamos de enfatizar ainda mais que o reconhecimento biométrico é uma tecnologia avançada que certamente será utilizada no comércio eletrônico, setor bancário, seguradoras, judiciário e em outros setores no futuro. Todos os anos, o mundo sofre grandes perdas devido à natureza insegura das senhas. Os produtos biométricos servem para proteger sua identidade em ambientes de alta segurança.

Operação Ecologicamente Correta

O "período de operação ecologicamente correto" do produto refere-se ao tempo durante o qual este produto não liberará nenhuma substância tóxica ou perigosa quando usado de acordo com os pré-requisitos deste manual. O período de operação ecologicamente correto especificado para este produto não inclui baterias ou outros componentes que se desgastam facilmente e devem ser substituídos periodicamente. O período operacional ecologicamente correto da bateria é de 5 anos.

Substâncias tóxicas ou perigosas e suas quantidades

Nome do Componente	Substância/Elemento Perigoso/Tóxico					
	Chumbo (Pb)	Mercúrio (Hg)	Cádmio (Cd)	Crómio hexavalente (Cr6+)	Bifenilas Polibromadas (PBB)	Éteres difenil-polibromados (PBDE)
Resistores	×	○	○	○	○	○
Capacitores	×	○	○	○	○	○
Indutores	×	○	○	○	○	○
Diodo	×	○	○	○	○	○
Componentes ESD	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adaptador	×	○	○	○	○	○
Parafusos	○	○	○	×	○	○

○ indica que a quantidade total de conteúdo tóxico em todos os materiais homogêneos está abaixo do limite, conforme especificado no SJ/T 11363—2006.

× indica que a quantidade total de conteúdo tóxico em todos os materiais homogêneos excede o limite, conforme especificado no SJ/T 11363—2006.

Observação: 80% dos componentes deste produto são fabricados utilizando materiais que não são tóxicos e ecologicamente corretos. Os componentes que contêm toxinas ou elementos nocivos são incluídos devido às atuais limitações econômicas ou técnicas que impedem sua substituição por materiais não tóxicos.

Garantia

Este produto é garantido pela ZKTeco por um período de 3 meses (garantia legal), acrescidos de 9 meses de garantia adicional (garantia contratual), em um total de 1 ano, contra eventuais defeitos de material ou fabricação, desde que observadas as seguintes condições:

a) A garantia se aplica exclusivamente a produtos fornecidos pela ZKTeco do Brasil ou por Revenda Autorizada ZKTeco no Brasil.
b) O período de garantia será contado a partir da data de emissão da nota fiscal do produto.
c) Durante a garantia legal estão cobertos os custos de peças e serviços de reparo, que deverão ser realizados obrigatoriamente em Assistência Técnica ZKTeco ou na própria fábrica, conforme orientação da ZKTeco. Para o período de garantia contratual estão cobertos apenas os custos de peças que eventualmente necessitem substituição para reparo do produto, ficando excluídos os custos em relação aos serviços de manutenção (mão de obra), a remoção do produto (envio e retorno) e a visita/estadia de técnico especializado, se aplicável.
d) Detectado o defeito no produto, o usuário deverá entrar em contato com a ZKTeco nos canais de comunicação disponíveis em https://www.zkteco.com.br/suporte/, fornecendo informações sobre os produtos e problemas observados por meio do preenchimento e envio do formulário de Remessa de Material para Assistência Técnica (RMA) disponível em https://www.zkteco.com.br/manutencao/.
e) Recebidas as informações e o RMA, a ZKTeco analisará o caso e informará ao usuário sobre os próximos passos, bem como sobre a documentação que deve ser encaminhada em caso de envio do produto para a ZKTeco ou Assistência Técnica ZKTeco e/ou sobre opções para agendamento de visita técnica, quando aplicável.
f) Produtos enviados para a ZKTeco ou para Assistência Técnica ZKTeco sem notificação prévia e expressa autorização da ZKTeco não serão recebidos.
g) O produto e as peças substituídas serão garantidas pelo restante do prazo original, sendo que as peças retiradas dos produtos e/ou produtos eventualmente descartados serão de propriedade da ZKTeco.
h) Em caso de dúvidas o usuário deverá entrar em contato com a ZKTeco nos canais de comunicação disponíveis em https://www.zkteco.com.br/suporte/

Resultará nula e sem efeito esta garantia em caso de:

a) Produto que apresente lacres rompidos e/ou etiqueta de identificação violada.
b) Uso anormal do produto, inclusive em desconformidade com seu manual, especificações, desenhos, folhas de instruções ou quaisquer outros documentos relacionados, bem como em capacidade além de seus limites e taxas prescritas.
c) Uso indevido ou erro de instalação, operação, testes, armazenamento e/ou manuseio do produto.
d) Manutenção e/ou alteração no produto não aprovada previamente pela ZKTeco.
e) Defeitos e danos causados por agentes naturais (enchente, maresia e outros) ou exposição excessiva ao calor.
f) Defeitos e danos causados pelo uso de software e/ou hardware não compatíveis com especificações do produto.
g) Surtos e/ou picos de tensão na rede elétrica típicos de algumas regiões, para as quais deve-se utilizar dispositivos de proteção contra surtos elétricos.
h) Fatos ou eventos imprevisíveis ou de difícil previsão e de força maior.
i) Transporte do produto em embalagem ou de forma inadequada.
j) Furto ou roubo.
k) Desgaste natural do produto.
l) Danos exclusivamente causados pelo usuário ou por terceiros.

Em nenhum caso a ZKTeco será responsável por indenização superior ao preço da compra do produto, por qualquer perda de uso, perda de tempo, inconveniência, prejuízo comercial, perda de lucros ou economias ou outros danos diretos ou indiretos, decorrentes do uso ou impossibilidade de uso do produto.

A ZKTeco reserva-se o direito de alterar as condições e procedimentos aqui estabelecidos independente de aviso prévio, sendo de responsabilidade do usuário verificar periodicamente eventuais atualizações, que estarão disponíveis em https://www.zkteco.com.br/manutencao/. Nenhuma Revenda Credenciada ou Assistência Técnica ZKTeco tem autorização para modificar as condições aqui estabelecidas ou assumir outros compromissos em nome da ZKTeco.

Telefone: (31) 3055-3530

Endereço: Rodovia MG-010, KM 26

Loteamento 12 - Bairro Angicos Vespasiano -

MG - CEP: 33.206-240

www.zkteco.com.br