Manual do Usuário

G4 Pro Series

Data: Setembro de 2023

Versão do documento: 1.2

Português

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

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

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

Este produto pode conter um ou mais módulos listados abaixo, de acordo com o modelo adquirido por você.

ANATEL 01094-23-12720
Módulo: IC11
"Incorpora produto homologado pela ANATEL sob número 01094-23-12720"

ANATEL 07935-23-12720
Módulo: MTR11
"Incorpora produto homologado pela ANATEL sob número 07935-23-12720"

ANATEL 07937-23-12720
Módulo: MTR10
"Incorpora produto homologado pela ANATEL sob número 07937-23-12720"

ANATEL 12509-20-12720
Módulo: IC01 (M330-L_V3.4)
"Incorpora produto homologado pela ANATEL sob número 12509-20-12720"

ANATEL 14815-21-12720
Módulo: EM05 (V2.01)
"Incorpora produto homologado pela ANATEL sob número 14815-21-12720"

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

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 **Série G4 Pro**.

Todas as imagens exibidas são apenas para fins ilustrativos. As imagens neste manual podem não ser exatamente consistentes com os produtos reais.
Recursos e parâmetros com ★ não estão disponíveis em todos os dispositivos.

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 Visão geral

A Série G4 Pro é uma versão totalmente atualizada do Terminal de Reconhecimento Facial de Luz Visível, utilizando algoritmos de reconhecimento facial inteligentes e a mais recente tecnologia de visão computacional. Ele também integra suporte ao sensor QR para leitura de códigos QR com aplicativo móvel, além de melhorar o desempenho de segurança em todos os aspectos. A Série G4 Pro possui dois modelos, o G4 Pro[TI] é a versão aprimorada do G4 Pro com algoritmo de reconhecimento facial inteligente por imagem térmica.

A Série G4 Pro suporta reconhecimento facial com grande capacidade e velocidade de reconhecimento, além de outros métodos de autenticação, incluindo identificação com cartão, senha e impressão digital★. O G4 Pro[TI] adota tecnologia de reconhecimento sem contato e novas funções, como:

1) Detecção de Temperatura Corporal
2) Detecção de Uso de Máscara Facial

Também está equipado com um algoritmo antifraude de última geração para reconhecimento facial, que combate praticamente todos os tipos de fotos falsas e intrusões de vídeo. Este dispositivo é a escolha perfeita para reduzir a propagação de germes e ajudar a prevenir infecções diretamente em cada ponto de acesso de qualquer estabelecimento e áreas públicas, como hospitais, fábricas, escolas, prédios comerciais e estações, durante a condição pandêmica recente, com suas funções de medição rápida e precisa de temperatura corporal e detecção de uso de máscara facial durante a verificação facial.

Características

- Compatível com rede 4G, atendendo a diversos mercados, incluindo Europa, Oriente Médio, África, Coreia do Sul, Tailândia e Índia
- Digitalização de códigos QR dinâmicos de Ponto e Acesso/Controle de Acesso no aplicativo móvel ZKBioSecurity
- Protocolo de Dispositivo Supervisionado Aberto (OSDP v2.1.7)
- Módulo de cartão de dupla frequência (125kHz e 13,56MHz) (padrão)
- Cartão HID iClass (opcional)
- Demonstração do Android LCDK para integração de aplicativos de terceiros
- Alimentação por PoE 802.3af/at
- Detecção de máscara
- Algoritmo antifraude contra ataques com impressões (laser, coloridas e em preto e branco) e ataques de vídeo

* O reconhecimento facial para indivíduos usando máscaras aumentará a Taxa de Falsas Aceitações (FAR)

Funções Especiais

- Detecção de máscara
- Detecção de temperatura corporal
- Distância de medição de temperatura: 30cm a 120cm (0,98 pés a 3,94 pés)
- Precisão de medição de temperatura: ±0,3°C (±0,54°F)
- (Testado a uma distância de 80cm (2,63 pés) sob temperatura de 25°C (77°F)
- Faixa de medição de temperatura: 20°C a 50°C (68°F a 122°F)

2 Instruções de Uso

Antes de conhecer as características do dispositivo e suas funções, é recomendado estar familiarizado com os fundamentos abaixo.

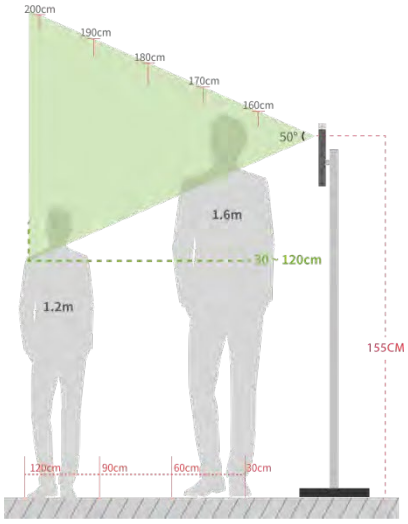
2.1 Como escanear o código QR?

Abra o aplicativo ZKBioSecurity no seu celular e alinhe a tela do telefone com o scanner de código QR do dispositivo.

Observação: Coloque o seu celular a uma distância de 15 a 50cm do dispositivo (a distância depende do tamanho da tela do celular), não bloqueie o scanner de código QR do dispositivo e o código QR na tela do celular.

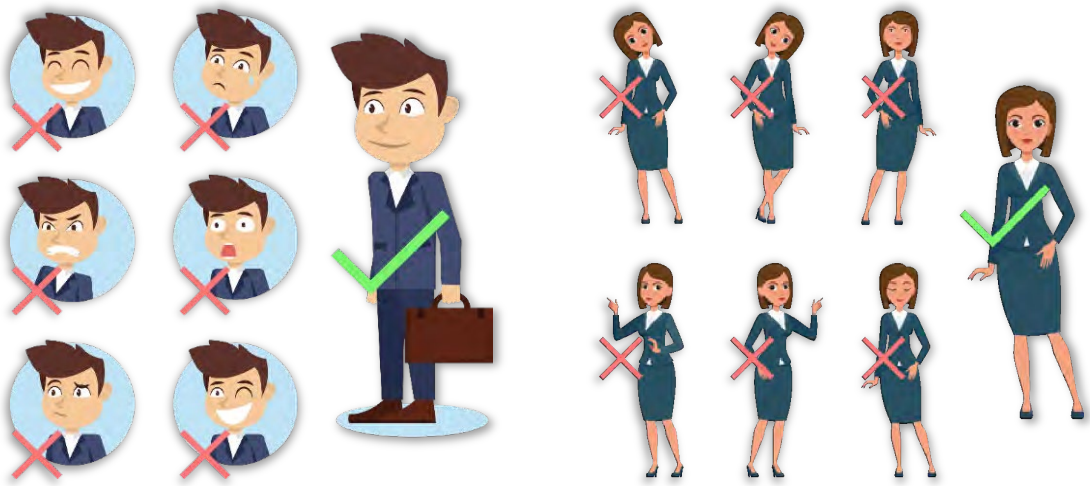
2.2 Posição em pé, Expressão Facial

- **A distância recomendada**



A distância recomendada entre o dispositivo e um usuário com altura entre 1,55m e 1,85m é de 0,3 a 2,5m. Os usuários podem se mover ligeiramente para frente ou para trás para melhorar a qualidade das imagens faciais capturadas.

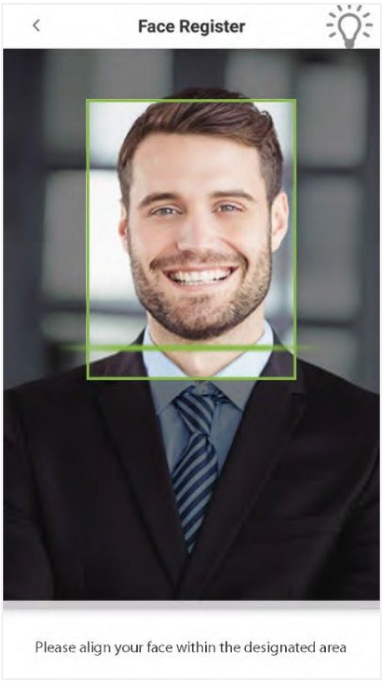
- **Postura em pé recomendada e Expressão Facial**



OBSERVAÇÃO: Por favor, mantenha sua expressão facial e postura em pé de forma natural durante o cadastramento ou verificação.

2.3 Registro Facial

Tente manter o rosto no centro da tela durante o registro. Por favor, vire-se em direção à câmera e mantenha-se parado durante o registro facial. A tela deve estar assim:



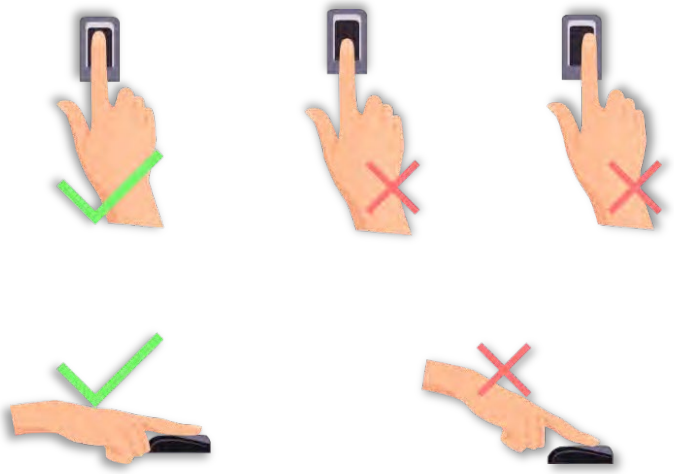
Método correto de registro e autenticação facial

- **Recomendação para registrar uma face**
  - Ao registrar uma face, mantenha uma distância de 40cm a 80cm entre o dispositivo e a face.
  - Tenha cuidado para não alterar a expressão facial (rosto sorridente, rosto tenso, piscar de olhos, etc.).
  - Se não seguir as instruções na tela, o registro facial pode levar mais tempo ou falhar.
  - Tenha cuidado para não cobrir os olhos ou sobrancelhas.
  - Não use chapéus, máscaras, óculos de sol ou óculos.
  - Tenha cuidado para não exibir dois rostos na tela. Registre uma pessoa por vez.
  - É recomendado que um usuário que usa óculos registre o rosto com e sem óculos.
- **Recomendação para autenticar um rosto**
  - Certifique-se de que o rosto apareça dentro das diretrizes exibidas na tela do dispositivo.
  - Se os óculos forem trocados, a autenticação pode falhar. Se o rosto sem óculos tiver sido registrado, autentique o rosto sem óculos. Se o rosto com óculos tiver sido registrado, autentique o rosto com os óculos previamente usados

- Se uma parte do rosto estiver coberta com um chapéu, uma máscara, um tapa-olho ou óculos de sol, a autenticação pode falhar. Não cubra o rosto, permita que o dispositivo reconheça tanto as sobrancelhas quanto o rosto.

2.4 Posicionamento do Dedo

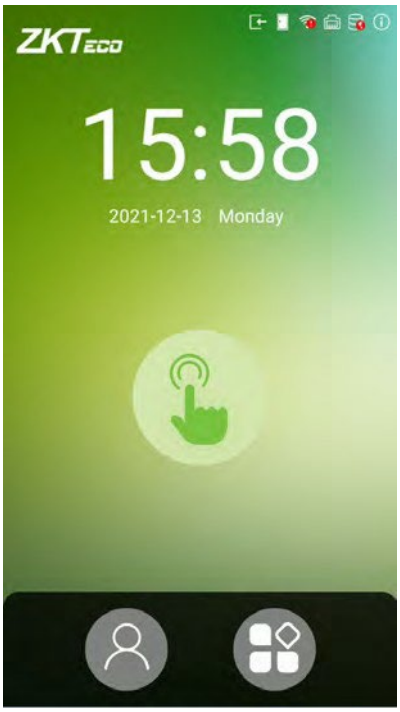
Dedos recomendados: indicador, médio ou anelar.
Evite usar o polegar ou o mindinho, pois eles são difíceis de tocar com precisão no leitor de impressões digitais.



Observação: Por favor, utilize o método correto ao pressionar os dedos no leitor de impressões digitais para o registro e identificação.

2.5 Tela principal

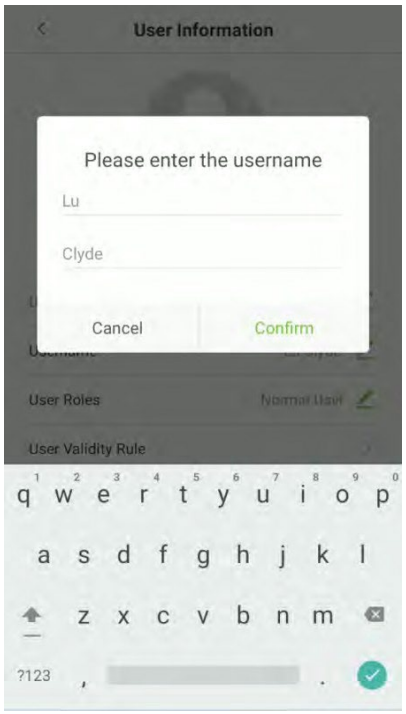
Após conectar a fonte de alimentação, o dispositivo exibe a seguinte tela:



Observação:

1. Toque no botão para acessar a tela de entrada de ID do pessoal.
2. Toque no botão para acessar o menu principal.
3. Se um superadministrador já foi registrado para este dispositivo, você precisará da permissão do superadministrador para acessar o menu principal.

2.6 Teclado Virtual



Observação:

1. Pressione [?123] para alternar para o teclado numérico e de símbolos.
2. Clique na caixa de entrada, o teclado virtual aparecerá.

2.7 Modo de Autenticação

2.7.1 Autenticação por QR Code

Neste modo de verificação, o dispositivo compara a imagem do código QR coletada pelo coletor de código QR com todos os dados de código QR no dispositivo.

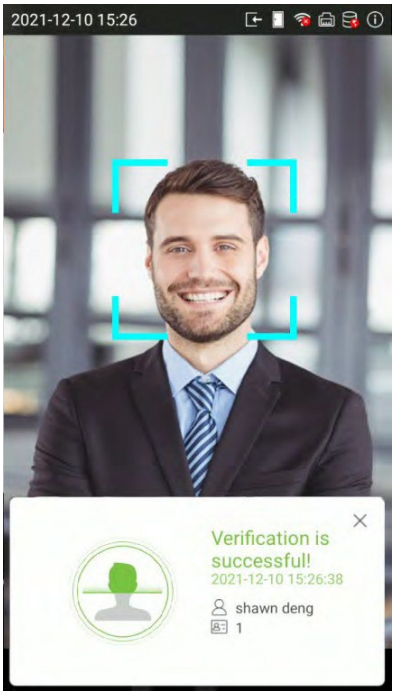
Toque em [Credencial Móvel] no aplicativo ZKBioSecurity e um código QR aparecerá, que inclui o ID do funcionário e o número do cartão (apenas o código QR estático inclui o número do cartão). O código QR pode substituir um cartão físico em um dispositivo específico para realizar autenticação sem contato. Consulte a seção 11.3 Credencial Móvel para obter mais informações.

2.7.2 Autenticação Facial

- **Modo de Autenticação Facial 1:N (Um para Muitos)**

  1. **Autenticação convencional**

Neste modo de autenticação, o dispositivo compara as imagens faciais coletadas com todos os dados faciais registrados no dispositivo. A seguir está a mensagem pop-up de um resultado de comparação bem-sucedido.

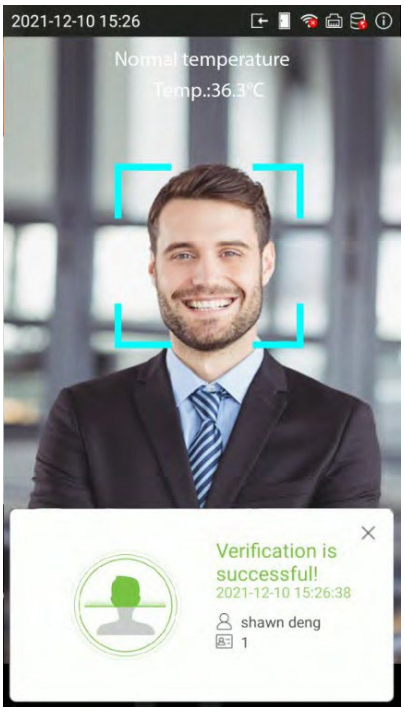


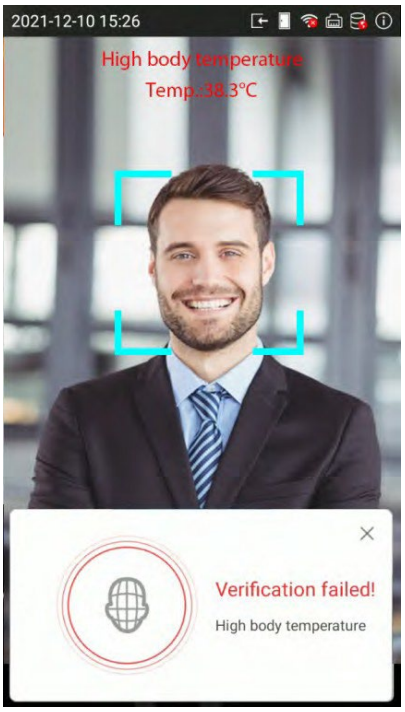
2. Ativar triagem de temperatura com infravermelho ★

Quando o usuário habilita a função de Triagem de temperatura com infravermelho, durante a verificação do usuário, além do método de verificação convencional, o rosto do usuário deve estar alinhado com a área de medição de temperatura para que a temperatura corporal possa ser medida antes da verificação ser realizada. A seguir estão as mensagens pop-up da interface de prompt de resultado de comparação.

Observação:

Esta função é aplicável apenas a produtos com módulo de medição de temperatura. Os dados de medição de temperatura são apenas para referência e não têm finalidade médica.

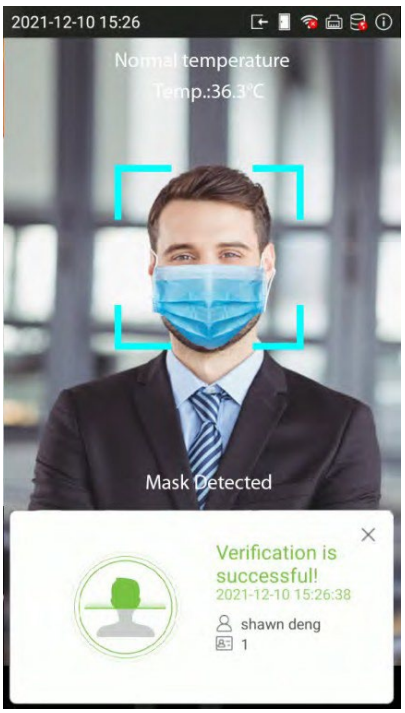


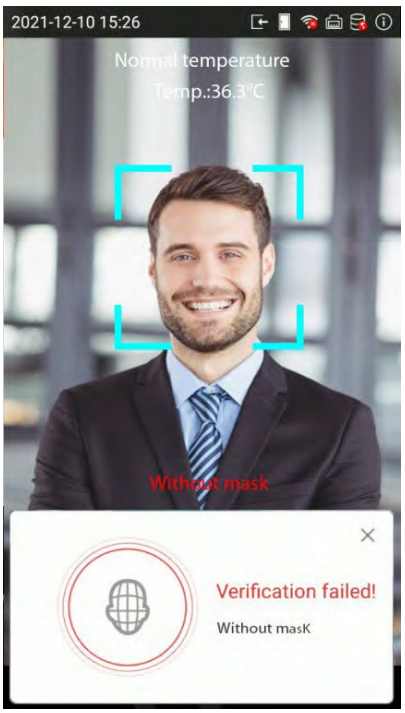


3. Ativar detecção de máscara ★

Quando o usuário habilita a função de detecção de máscara, o dispositivo irá identificar se o usuário está usando uma máscara ou não durante a verificação. A seguir estão as mensagens pop-up da interface de prompt de resultado de comparação. (Observação: esta função é aplicável apenas a produtos com módulo de medição de temperatura.)

OBSERVAÇÃO: Os dados de medição de temperatura são apenas para referência e não têm finalidade médica.

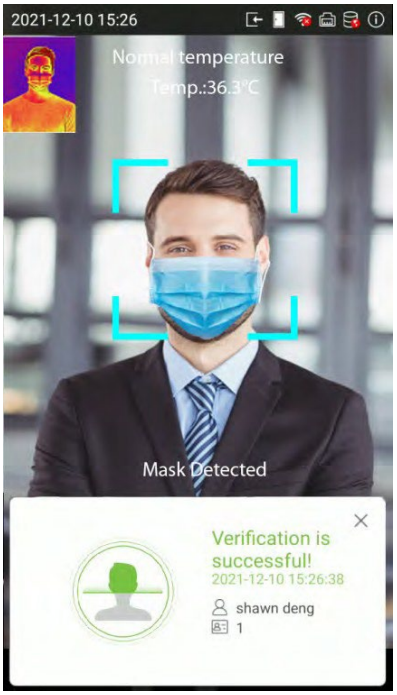


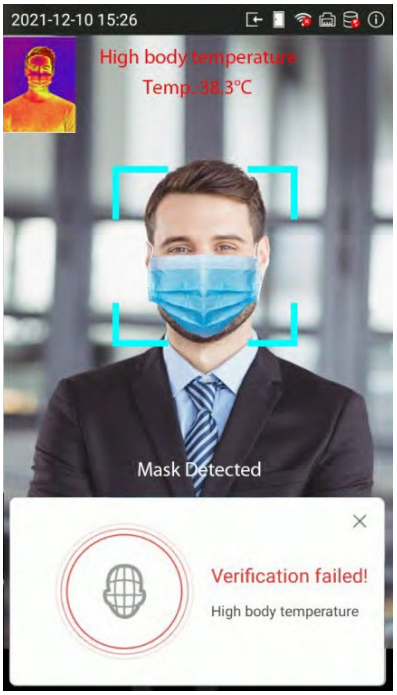


4. Exibir figura de termodinâmica ★

Quando o usuário habilita a função de exibição da figura de termodinâmica, a imagem térmica da pessoa é exibida no canto superior esquerdo do dispositivo durante a verificação. Como mostrado nas imagens abaixo:

Observação: Os dados de medição de temperatura são apenas para referência e não têm finalidade médica.





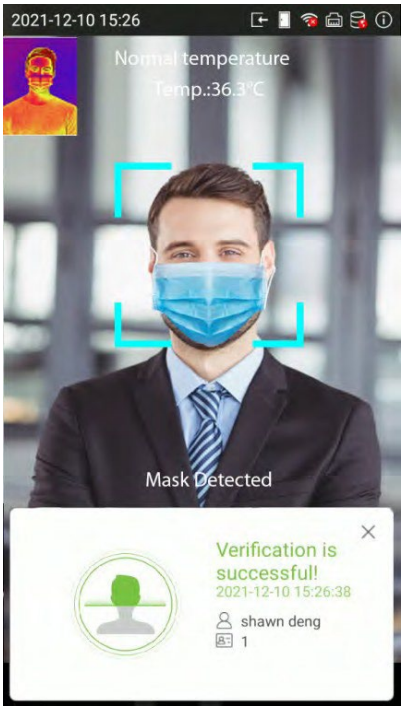
- **Modo de Autenticação Facial 1:1 (Um para Um)**

Neste modo de verificação, o dispositivo compara o rosto capturado pela câmera com o modelo facial relacionado ao ID de usuário inserido. Pressione na interface principal, entre no modo de verificação facial 1:1, insira o ID do usuário e pressione **OK**.

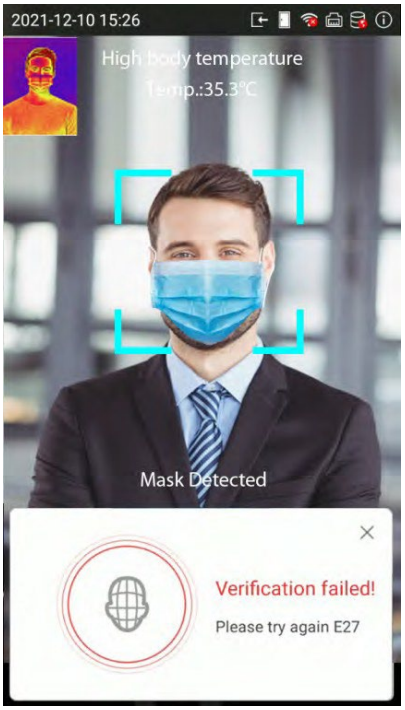
Se o usuário tiver registrado cartão, senha e impressão digital★, além do rosto, e o método de verificação estiver configurado para verificação por rosto/ cartão/ senha/ impressão digital★, a seguinte tela será exibida.

Selecione o ícone para entrar no modo de verificação facial. Após o aviso "Por favor, verifique seu rosto", ajuste seu rosto no centro da tela do dispositivo para a verificação facial.

Abaixo estão os exemplos de verificação bem-sucedida e mal-sucedida:



Verificação bem-sucedida

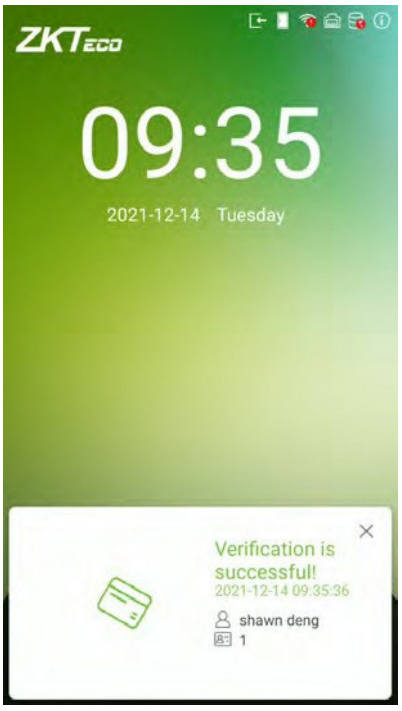


Verificação mal-sucedida

2.7.3 Autenticação de Cartão

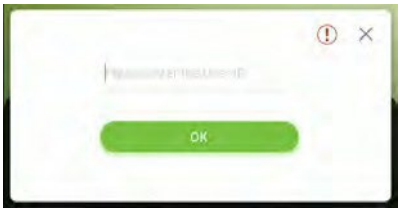
- **Autenticação de Cartão 1: N (Um para Muitos)**

Para entrar no modo de identificação de cartão 1: N, por favor, coloque o cartão registrado no leitor de cartão.

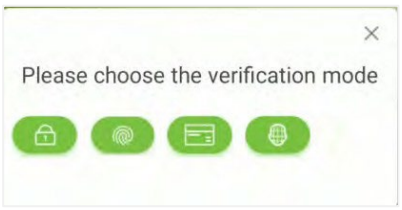


- **Autenticação de Cartão 1:1 (Um para Um)**

Pressione na interface principal e entre no modo de verificação de cartão 1:1, insira o ID do usuário e pressione **OK**.

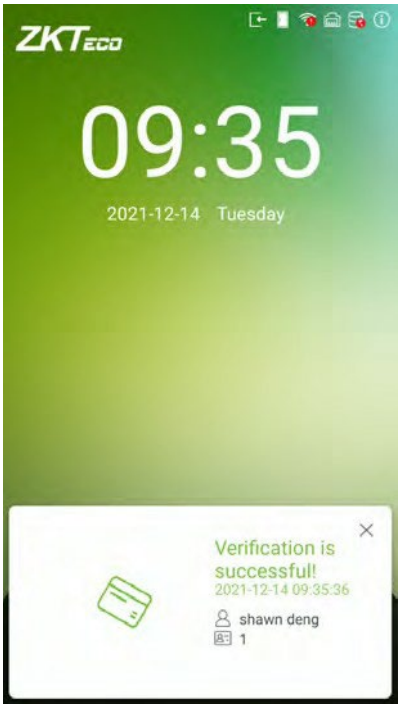


Se o usuário tiver registrado rosto, senha e impressão digital★, além do cartão, e o método de verificação estiver configurado para verificação por rosto/ cartão/ senha/ impressão digital★, a seguinte tela será exibida.



Selecione o ícone para entrar no modo de verificação de cartão. Após o aviso "Por favor, passe o seu cartão para a verificação".

Abaixo estão os exemplos de verificação bem-sucedida e mal-sucedida:



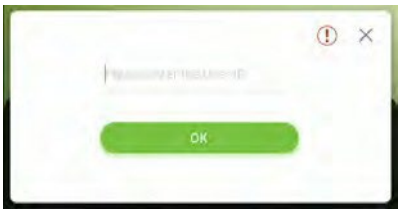
Verificação bem-sucedida:

Verificação mal-sucedida

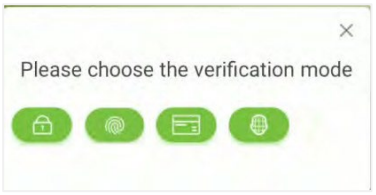
2.7.4 Autenticação de Senha

Quando um usuário insere seu ID de usuário e senha no dispositivo, os dados serão comparados com o ID de usuário e senha desse usuário pré-armazenados no sistema. Esse processo é recomendado para usuários administradores.

Pressione na interface principal e entre no modo de verificação de senha 1:1, insira o ID do usuário e pressione **OK**.

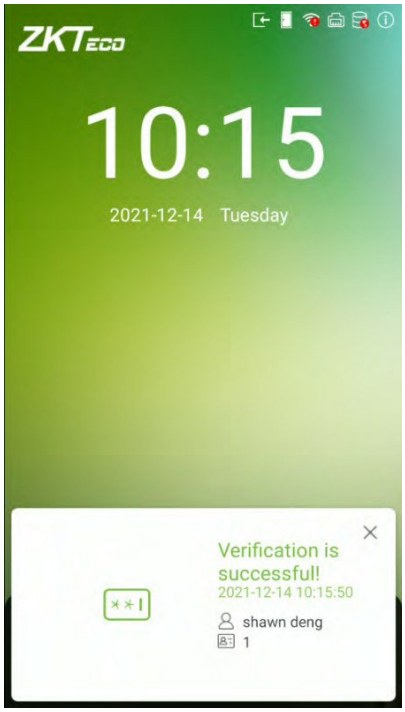


Se o usuário tiver registrado face, cartão e impressão digital★, além da senha, e o método de verificação estiver configurado para verificação por face/ cartão/ senha/ impressão digital★, a seguinte tela será exibida.



Selecione o ícone para entrar no modo de verificação de senha. Após o aviso "Por favor, digite a senha".

Abaixo estão os exemplos de verificação bem-sucedida e mal-sucedida:



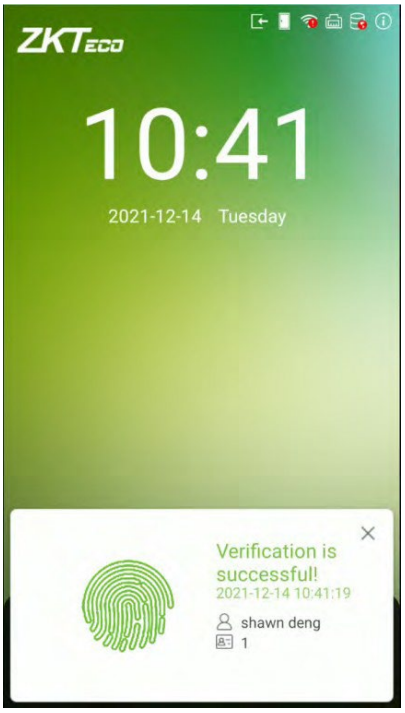
Verificação bem-sucedida:

Verificação mal-sucedida

2.7.5 Autenticação de Impressão Digital ★

- **Autenticação de Impressão Digital 1: N (Um para Muitos)**

Este método compara a impressão digital do usuário que está sendo pressionada no leitor de impressões digitais com todos os dados de impressões digitais pré-armazenados no dispositivo. Para entrar no modo de identificação por impressão digital, basta tocar o dedo no leitor de impressões digitais.

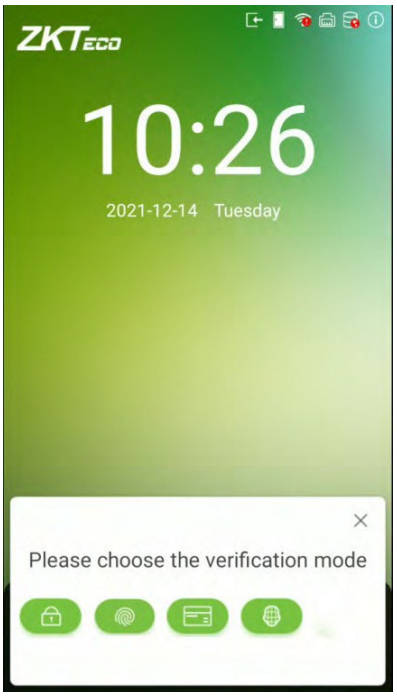


- **Autenticação de Impressão Digital 1:1 (Um para Um)**

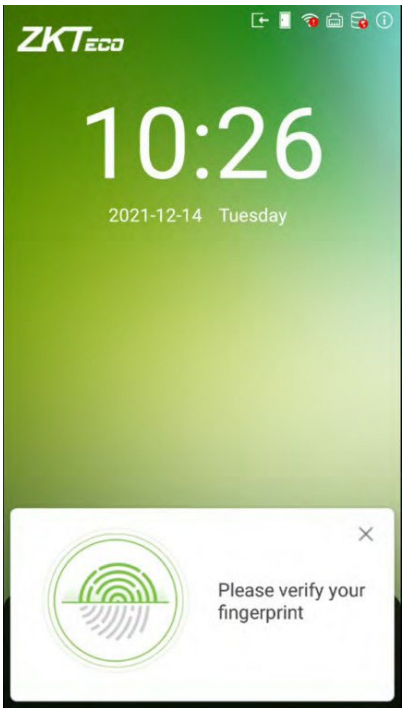
Neste modo de verificação, o dispositivo compara a impressão digital que está sendo pressionada no leitor de impressões digitais com os modelos de impressões digitais associados ao respectivo ID do usuário. Este método pode ser usado quando o sistema tem dificuldade em reconhecer as impressões digitais do usuário.

Pressione na interface principal e entre no modo de verificação de impressão digital 1:1 e digite o ID do usuário e pressione **OK**.

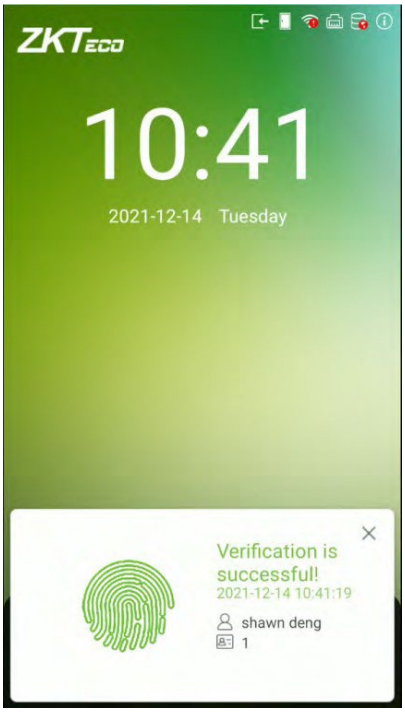
Se o usuário tiver registrado rosto, senha e cartão, além da impressão digital, e o método de verificação estiver configurado como verificação de rosto/cartão/senha/impressão digital★, a seguinte tela será exibida.



Selecione o ícone para entrar no modo de autenticação de impressão digital. Após a mensagem "Por favor, verifique sua impressão digital".



Abaixo estão os exemplos de verificação bem-sucedida e mal-sucedida:



Verificação bem-sucedida:

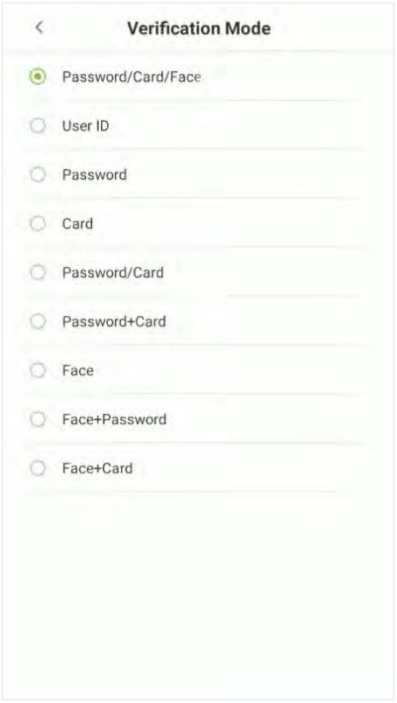
Verificação mal-sucedida

2.7.6 Autenticação Combinada

Para aumentar a segurança, este dispositivo oferece a opção de usar múltiplas formas de métodos de verificação. Um total de 10 combinações de verificação diferentes podem ser usadas, conforme mostrado abaixo:

Símbolo de Autenticação Combinada Definição

Símbolo	Definição	Explicação
/	ou	Este método compara a verificação inserida de uma pessoa com o modelo de verificação relacionado previamente armazenado para aquele ID de Pessoa no dispositivo
+	e	Este método compara a verificação inserida de uma pessoa com todos os modelos de verificação previamente armazenados para aquele ID de Pessoa no dispositivo.



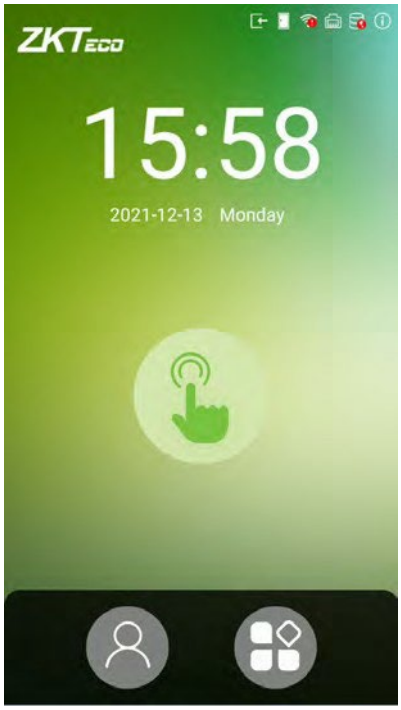
Procedimento para configurar o Modo de Autenticação Combinada:

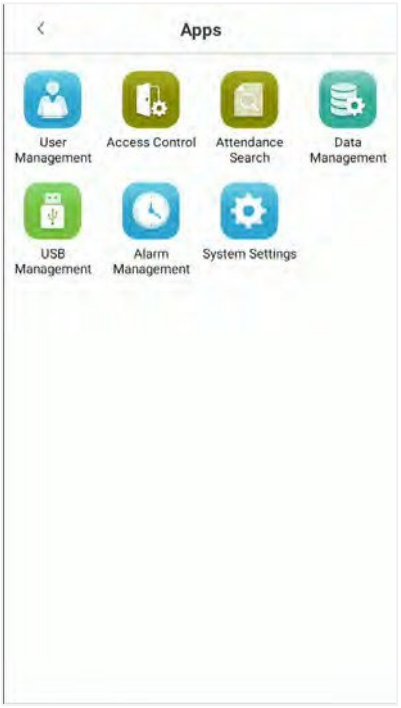
- Acesse as configurações do dispositivo.
- Procure a opção de segurança ou autenticação.
- Localize a opção de "Modo de Verificação Combinada" ou similar.
- Selecione essa opção para ativá-la.
- Na configuração do Modo de Verificação Combinada, escolha as opções de verificação que deseja utilizar em combinação (por exemplo, rosto, impressão digital, senha).
- Salve as configurações e saia do menu de configurações.

Agora, o dispositivo estará configurado para usar o Modo de Verificação Combinada, onde será necessário passar por todas as formas de verificação selecionadas para autenticar e acessar o dispositivo.

3 Menu Principal

Na interface de espera, toque em para entrar no Menu Principal.





Descrição da Função

Menu	Função
Usuário Adm.	Para adicionar, editar, visualizar e excluir informações básicas de um usuário.
Controle Acesso	Para configurar os parâmetros da fechadura e do dispositivo de controle de acesso relevantes, como opções de controle de acesso, regras de horário, configurações de feriados e configuração de anti-passback.
Proc. Registros	Consultar os registros de acesso especificados, verificar fotos de presença e fotos de lista de bloqueio.
Ger. Dados	Para excluir todos os dados relevantes no dispositivo.
Gerenciador USB	Para fazer o upload ou download de dados específicos de um dispositivo USB.
Gestão de Alarmes	Uma vez que um alarme tenha sido configurado, o dispositivo reproduzirá automaticamente o tom de alarme pré-selecionado quando o horário específico for alcançado. O alarme será interrompido após o tempo definido para o alarme ter decorrido.
Configurações do Sistema	Para configurar os parâmetros relacionados ao sistema, incluindo rede, data e hora, configuração de registros de acesso, serviço em nuvem, Wiegand, exibição e som, porta serial, parâmetros biométricos, gerenciamento de detecção, teste automático, avançado e segurança, e restaurar para as configurações de fábrica.

Observação:

1. Se o dispositivo não possuir um super administrador, qualquer usuário pode acessar o menu pressionando a tecla .
2. Após um super administrador ter sido configurado no dispositivo, será necessária a verificação de ID para acessar o menu. Uma vez que a verificação da senha seja bem-sucedida, os usuários podem acessar o menu.
3. Para garantir a segurança do dispositivo, recomendamos registrar um administrador na primeira vez em que você usar este dispositivo. Para obter instruções detalhadas sobre como fazer isso, consulte a seção Adicionar Usuário.

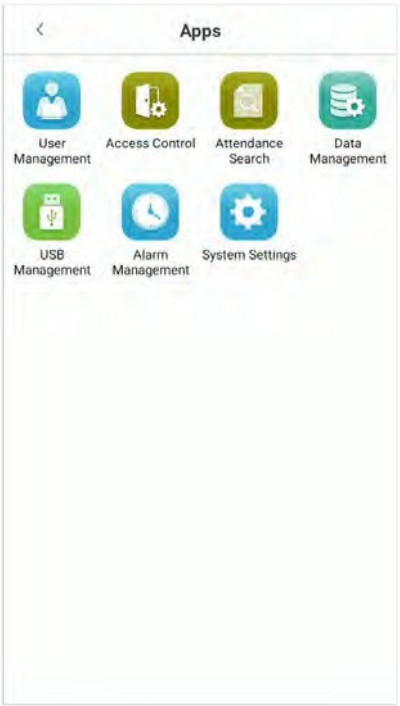
4 Gestão de Usuários

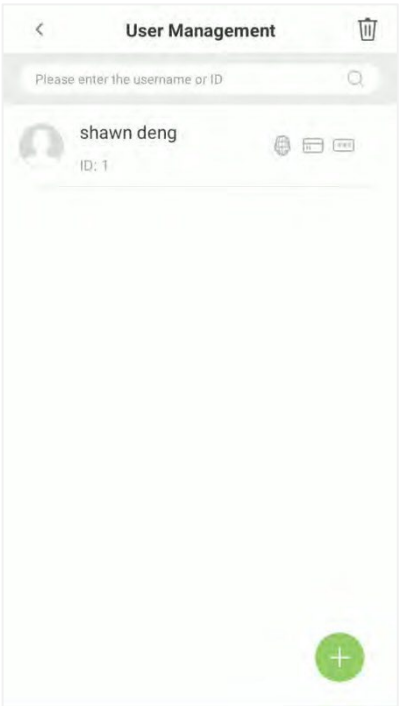
4.1 Cadastro de Usuários

Existem dois métodos para adicionar usuários: Adicionar usuário via Software ou Adicionar via Dispositivo.

4.1.1 Adicionar Usuários via Dispositivo

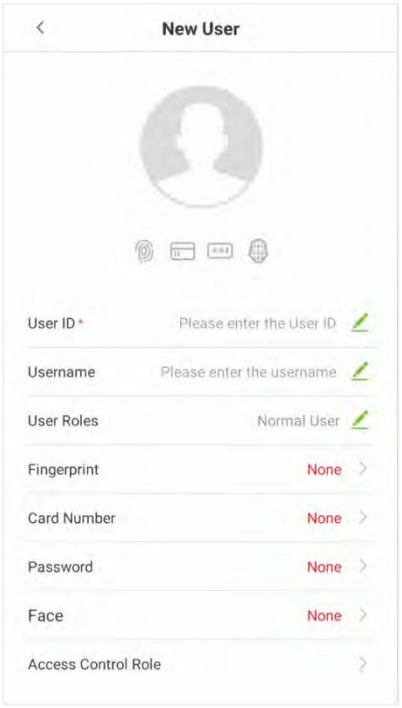
Toque no botão na interface de Gestão de Usuários para entrar na interface de criação de usuário.





Registrar Informações Básicas do Usuário

Na interface do Novo Usuário, toque em **ID do Usuário** e insira o número de identificação exclusivo e, em seguida, toque em **Nome de Usuário** e insira o nome de usuário.



Observação:

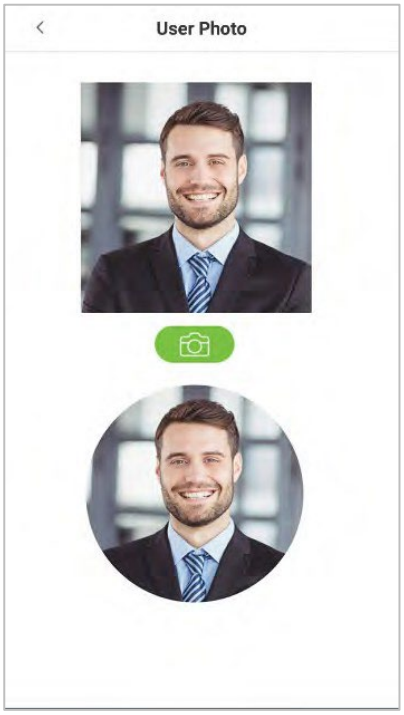
- Nome: O comprimento máximo de caracteres é de 24.
- ID do Usuário: O ID do usuário pode conter de 1 a 9 dígitos por padrão.
- Se você precisar de um leitor externo para passar o cartão, defina o número do cartão como o número de ID.
- O ID do usuário pode ser modificado antes do primeiro login, mas não pode ser modificado após o login.
- A mensagem "ID do usuário já existe, por favor tente novamente" indica que o número de ID inserido já está sendo usado. Nesse caso, é recomendado inserir outro número de ID.

Registrar Foto do Usuário

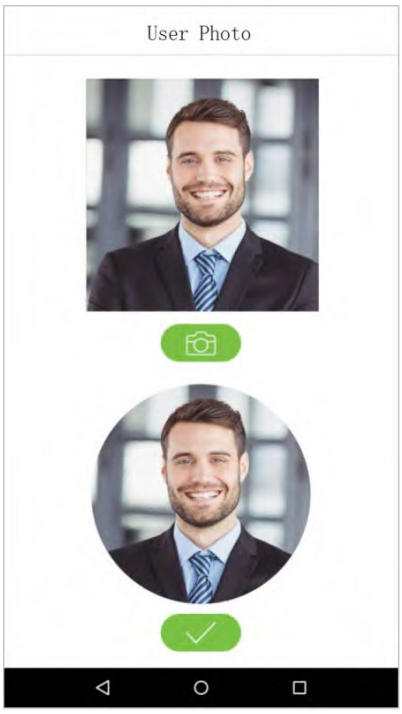
Na interface do Novo Usuário, toque no botão para entrar na interface da câmera.

É recomendado posicionar-se de frente para a lente e, em seguida, ajustar a posição conforme necessário.

Na interface da Foto do Usuário, toque no botão da câmera para capturar uma foto.



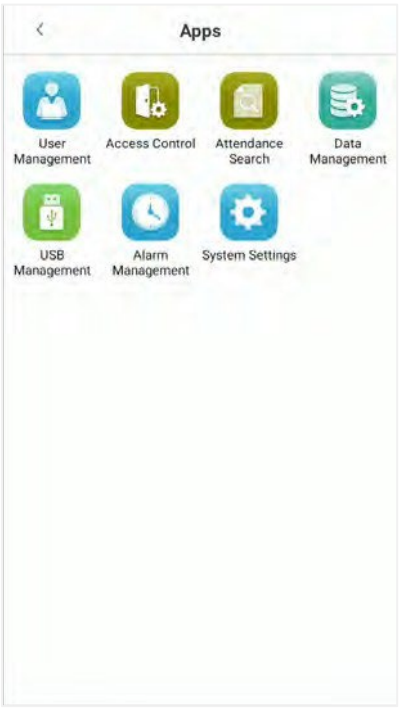
Toque no botão na parte inferior para adicionar com sucesso a foto capturada.



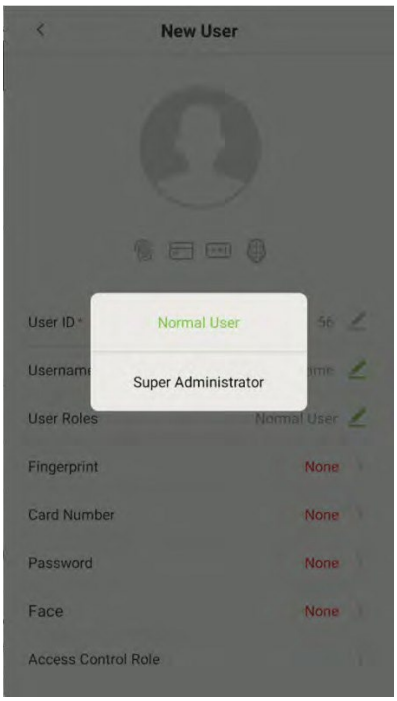
Privilégio do Usuário

Este dispositivo possui dois tipos de privilégios de usuário: Usuário Normal e Super Administrador. Se um Super Administrador existir no dispositivo, os Usuários Normais só poderão fazer login e visualizar suas contas usando diferentes modos de verificação que já foram configurados para o usuário. Porém, um Super Administrador terá mais privilégios, como acesso ao menu principal e também terá o mesmo acesso do usuário normal.

Na interface de **Gestão de Usuários**, toque no nome de usuário necessário na lista de usuários para configurar o privilégio do usuário.



Na interface **Informações do Usuário**, toque em **Privilégio do Usuário** e, em seguida, toque em **Usuário Normal** ou **Super Administrador** para definir o privilégio necessário.



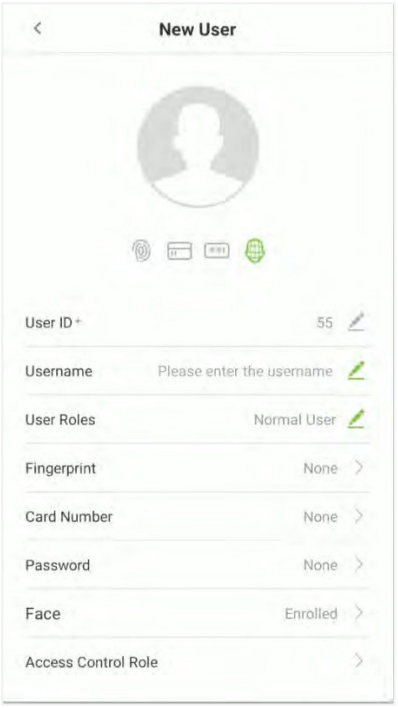
Observação: Quando um usuário recebe privilégios de super administrador, será necessária a verificação de ID para acessar o menu principal. O processo de verificação depende do método de verificação utilizado durante o registro do usuário. Consulte a descrição na seção "Modo de Verificação".

Registrar Modos de Verificação

Os diferentes modos de verificação são usados para verificar o login do usuário.

O modo de verificação inclui o registro de rosto, senha, impressões digitais★ ou número do cartão de um usuário.

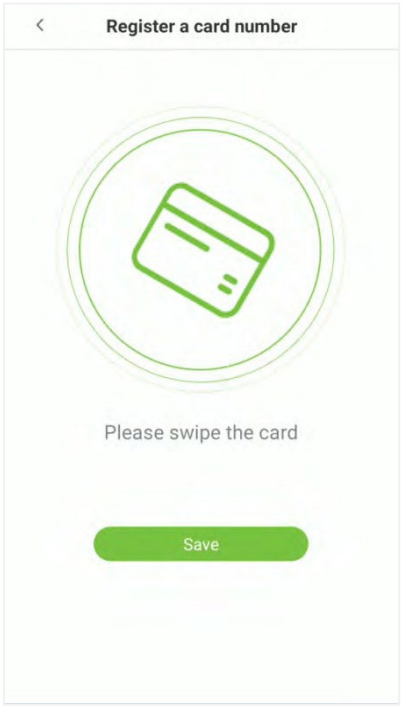
Na interface do **Novo Usuário**, toque no modo de verificação necessário (Número do Cartão, Senha, Rosto, Impressão Digital★) para registrar para verificação.

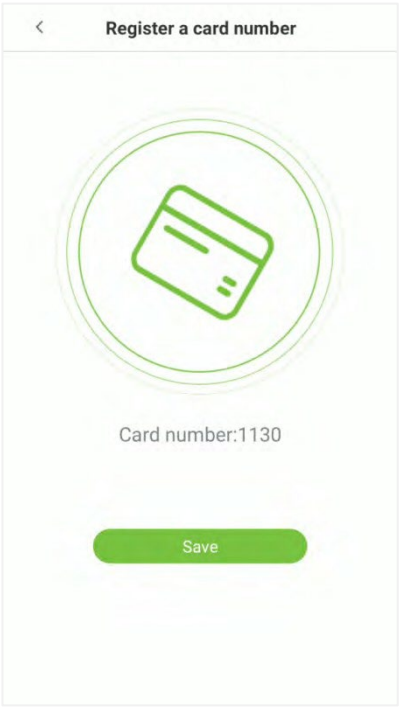


Registrar Número do Cartão

Na interface do **Novo Usuário**, toque em **Número do Cartão** para acessar a página de registro do número do cartão. Na interface de **Registro de um número de cartão**, passe o cartão para registrá-lo.

E uma vez que uma mensagem de sucesso seja exibida, toque em **Salvar** para atualizar os detalhes do cartão.





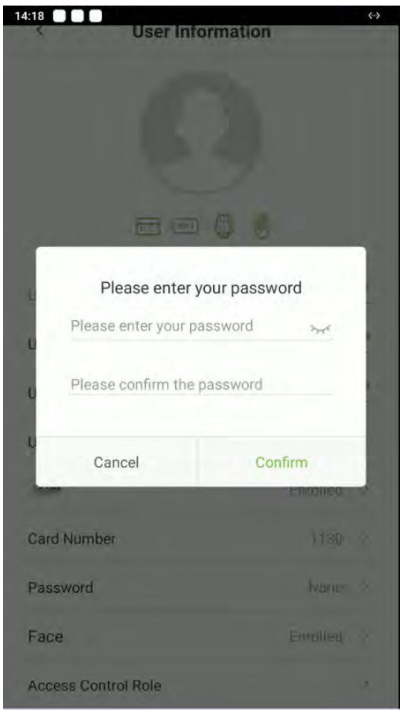
Registrar Senha

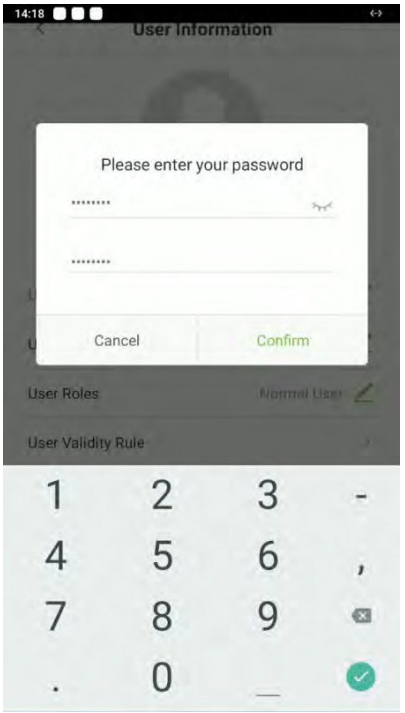
Na interface do **Novo Usuário**, toque em **Senha** para registrar uma senha.

No campo Digite a senha, insira a senha desejada e, em seguida, no campo Confirmar senha, insira novamente a mesma senha.

Toque em **Confirmar**.

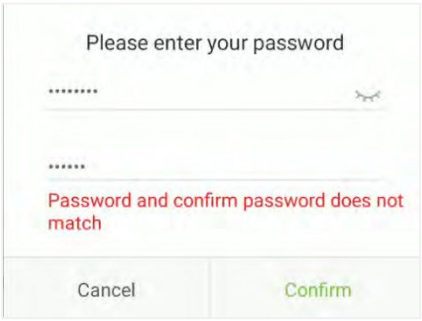
Observação: A senha do usuário deve ser um número de 8 dígitos.





Função	Descrição
	Toque neste botão para criptografar a senha.
	Toque neste botão para tornar a senha visível.

Se a senha digitada nos dois campos não corresponder, então digite novamente a senha correta.

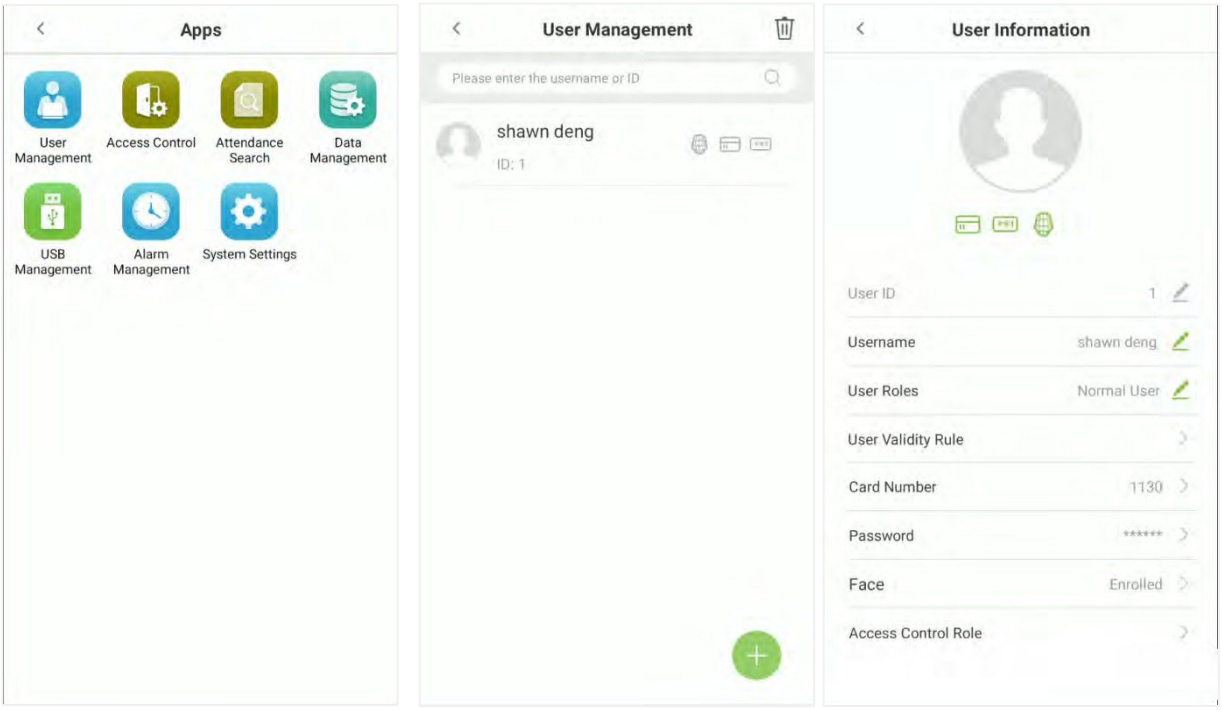


A senha registrada pode ser excluída ou modificada.

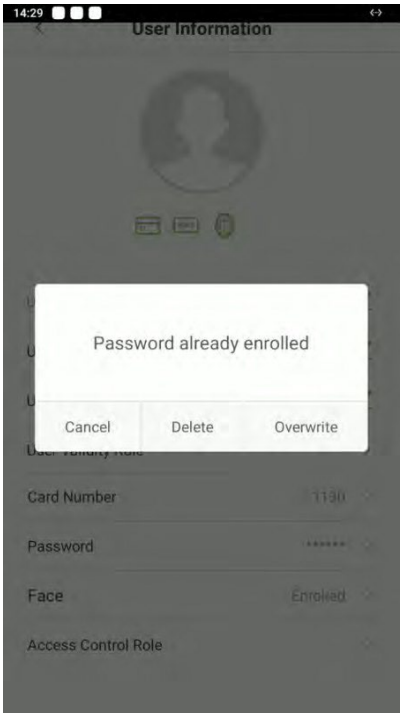
Excluir/Sobrescrever Senha Registrada

Na interface de **Gestão de Usuários**, toque no nome de usuário necessário na lista de usuários para excluir ou modificar a senha.

Na interface de **Informações do Usuário**, toque em **Senha** para excluir ou modificar.



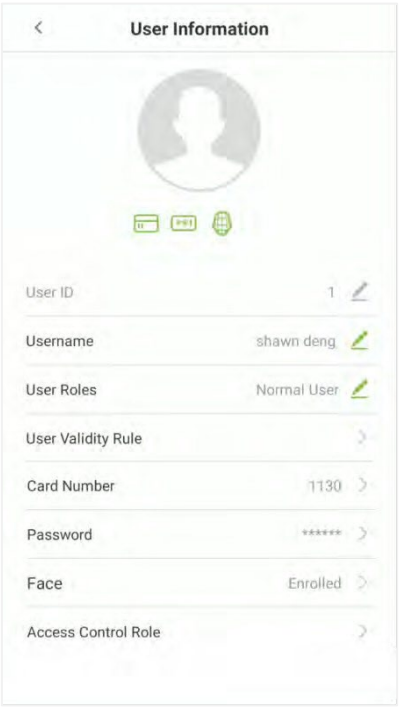
Na janela pop-up, toque em **Excluir/Sobrescrever** para excluir ou modificar a senha.

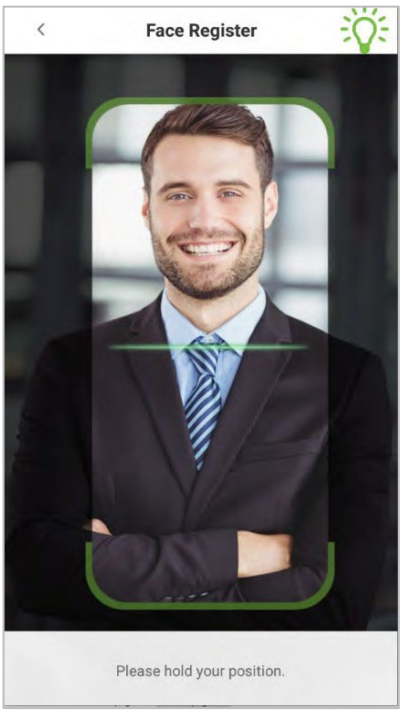


Registrar Face

Na interface de **Novo Usuário**, toque em Face para entrar na página de registro de face.

Na interface de Registro de Face, mova e ajuste seu rosto na área de registro.





Registrar Impressão Digital★

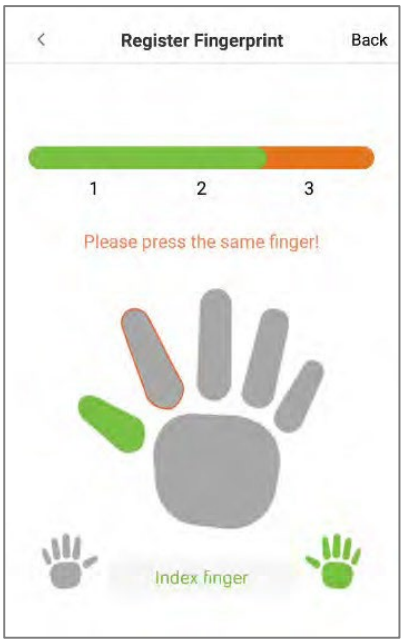
Na interface do Novo Usuário, toque em **Impressão Digital** para entrar na interface de registro de impressão digital.

Toque no botão necessário (esquerda ou direita) localizado nos lados esquerdo e direito da tela e, em seguida, toque no dedo desejado para registrar.

Após selecionar o dedo necessário, pressione o mesmo dedo no leitor de impressão digital três vezes.

A cor verde indica que a impressão digital foi registrada com sucesso.

Observação: Se você tocar diferentes dedos no scanner de impressão digital durante a segunda e terceira tentativas, o usuário receberá uma mensagem solicitando que "Use o mesmo dedo", conforme mostrado na imagem abaixo.



Se a impressão digital for registrada com sucesso, uma caixa de diálogo "Continuar registrando a próxima impressão digital?" será exibida.

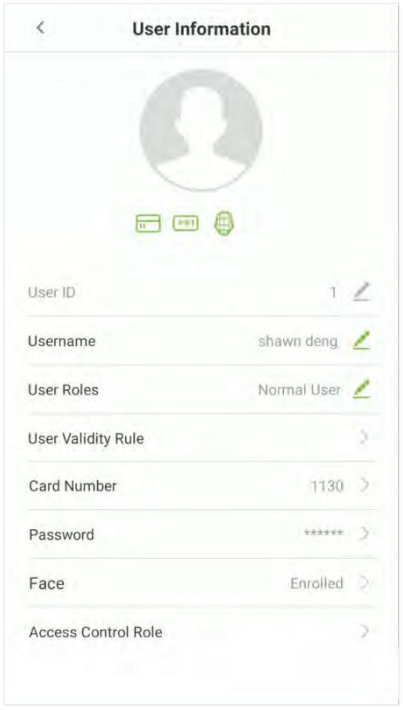
Toque em **Sim** para registrar a próxima impressão digital ou em **Não** para retornar à interface de registro de impressão digital.

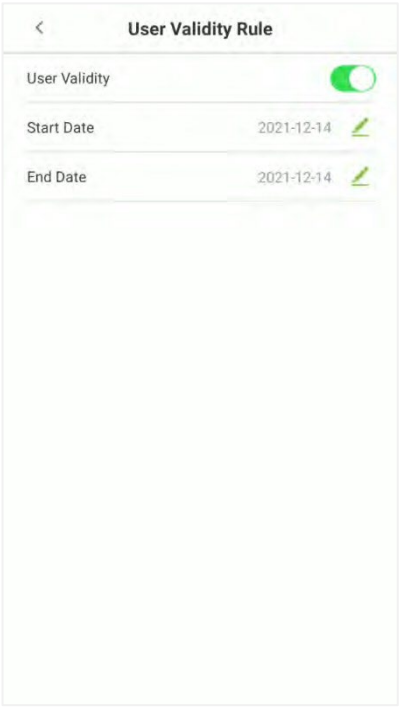
Configurações de Período de Validade

Essa função define o período de validade para o processo de verificação de presença de um funcionário. Uma vez que esse período de validade seja definido, o funcionário só poderá verificar a presença durante esse horário definido. Se o funcionário autenticar a presença antes ou depois do horário definido, a presença será considerada inválida.

A verificação de presença é válida dentro do período de tempo definido, iniciando a partir de um horário específico e encerrando em outro horário específico, durante um número definido de dias. Isso oferece precisão em dias específicos. O período de validade de um dia é das 00:00 às 23:59; uma vez que esse período de validade expire, a verificação de presença do funcionário será considerada inválida.

Na interface de Informações do **Usuário**, toque em **Regra de Validade do Usuário** para definir o período de validade.





Observação: Se a função **Regra de Validade do Usuário** não for exibida na interface de **Novo** Usuário, então no menu principal, toque em **Configurações do Sistema > Configurações de registro de controle de acesso** e habilite as **Configurações de validade do usuário**. Em seguida, a função "Regra de Validade do Usuário" aparecerá na interface de Novo Usuário.

Na **Regra de Validade do Usuário**, configure a regra de validade do usuário definindo a data e a hora necessárias.

Nível de Acesso

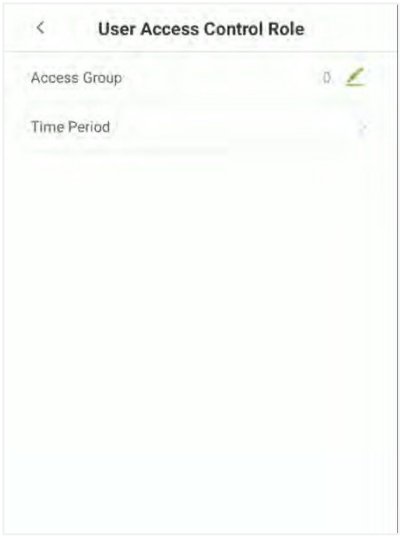
O **Papel de Controle de Acesso** define o privilégio de acesso à porta para cada usuário.

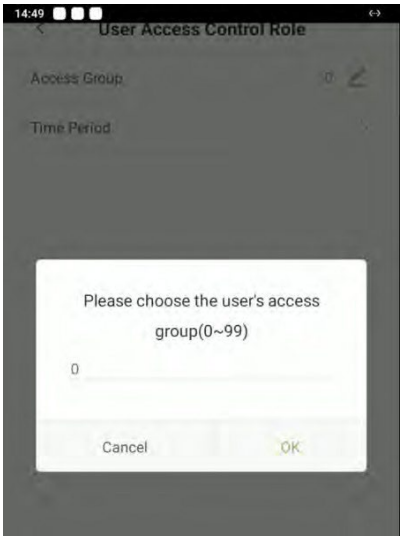
Isso inclui o grupo de acesso e o período de tempo.

Na interface de **Novo Usuário**, toque em **Papel de Controle de Acesso** para definir o nível de acesso.

Defina o Grupo de Acesso

Na interface do **Papel de Controle de Acesso do Usuário**, toque em **Grupo de Acesso** para atribuir os usuários registrados a diferentes grupos para uma melhor gestão.



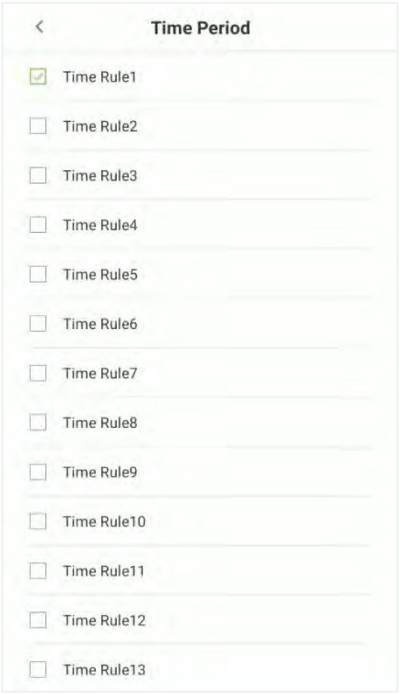


Por padrão, os novos usuários serão adicionados ao Grupo 1, mas podem ser realocados para outros grupos conforme necessário. O dispositivo suporta até 99 grupos de controle de acesso.

Definir uma Regra de Tempo

Toque em **Regra de Tempo** para configurar o horário de acesso para o usuário.
Por padrão, os usuários seguem as configurações definidas para seus grupos.
Se o período de tempo não for aplicado, o horário de acesso do usuário específico deve ser configurado.
Essa configuração não afetará as configurações de tempo dos outros membros do grupo.

Observação: Um total de 50 regras de tempo podem ser definidas.



4.1.2 Adicionar Usuários no Software

Conectar o Software

Recomenda-se usar o ZKBioSecurity V5000, caso contrário, a função e a interface podem ser diferentes.

Antes de adicionar funcionários, verifique se o dispositivo está conectado ao PC por meio do cabo de rede e defina o IP do dispositivo.

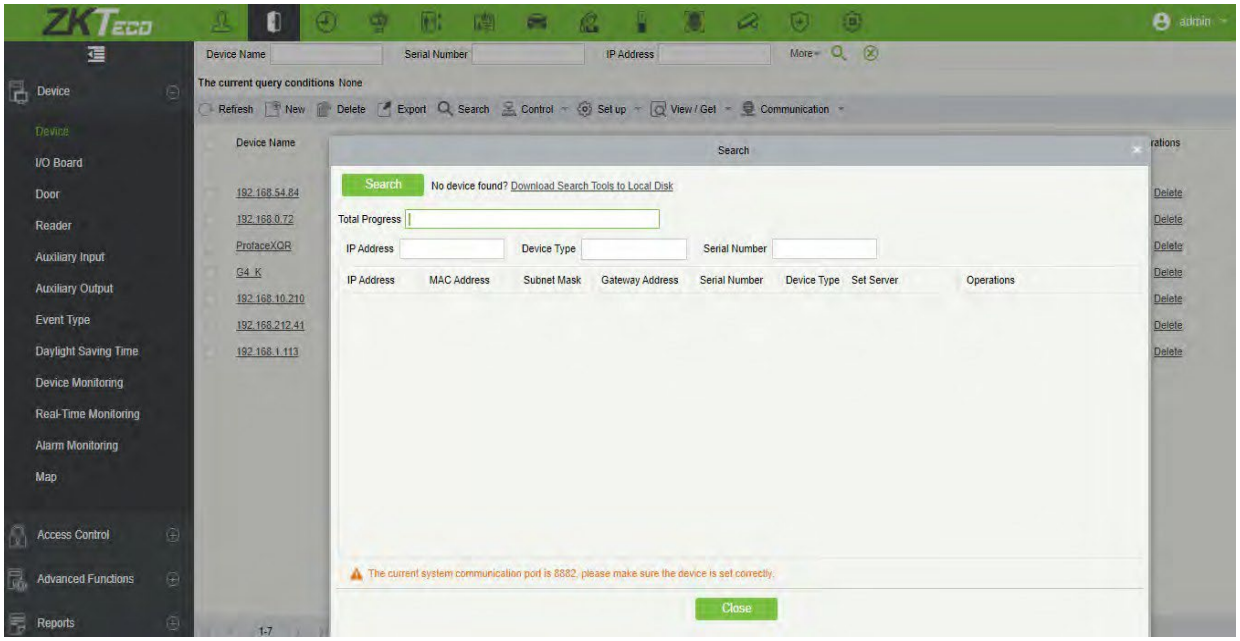
O IP do dispositivo e o IP do computador devem estar na mesma rede.
Consulte as Configurações de Ethernet para obter detalhes.

Toque em **Configurações do Sistema** > **Configurações de serviço em nuvem** para configurar os parâmetros do servidor em nuvem de acordo com o endereço do software exibido no navegador (Observação: a porta padrão do servidor é 8088).

Consulte as Configurações de Serviço em Nuvem para obter detalhes.

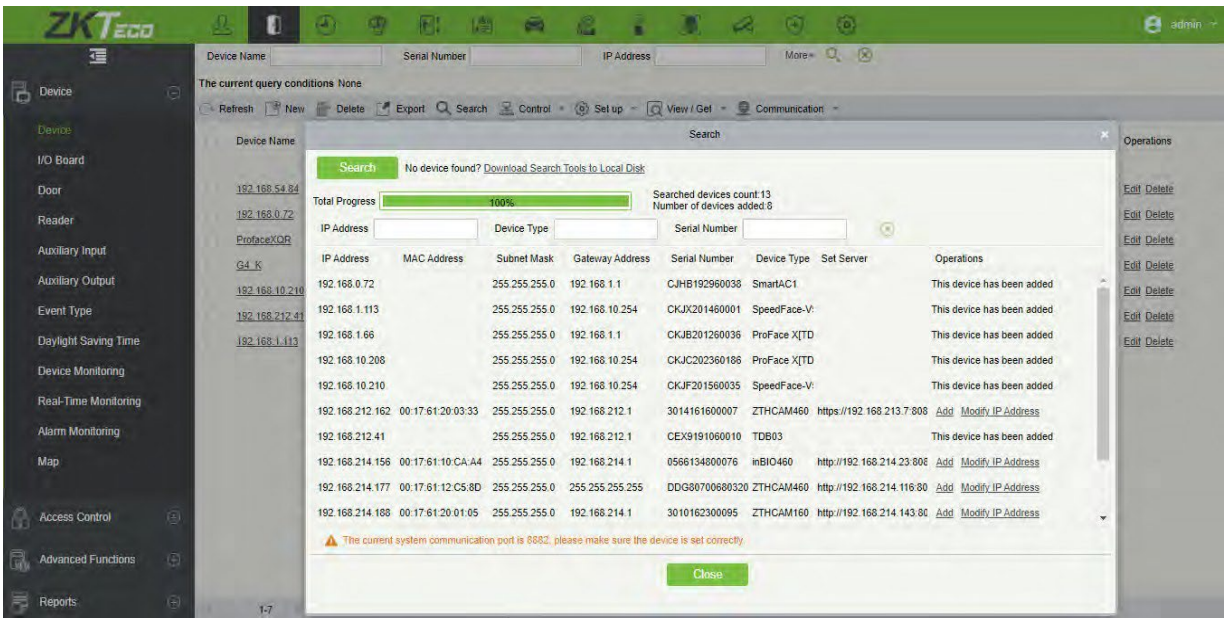
Adicionar Dispositivos

No software, clique em Acesso > Dispositivo > Pesquisar para buscar os dispositivos registrados ativos.

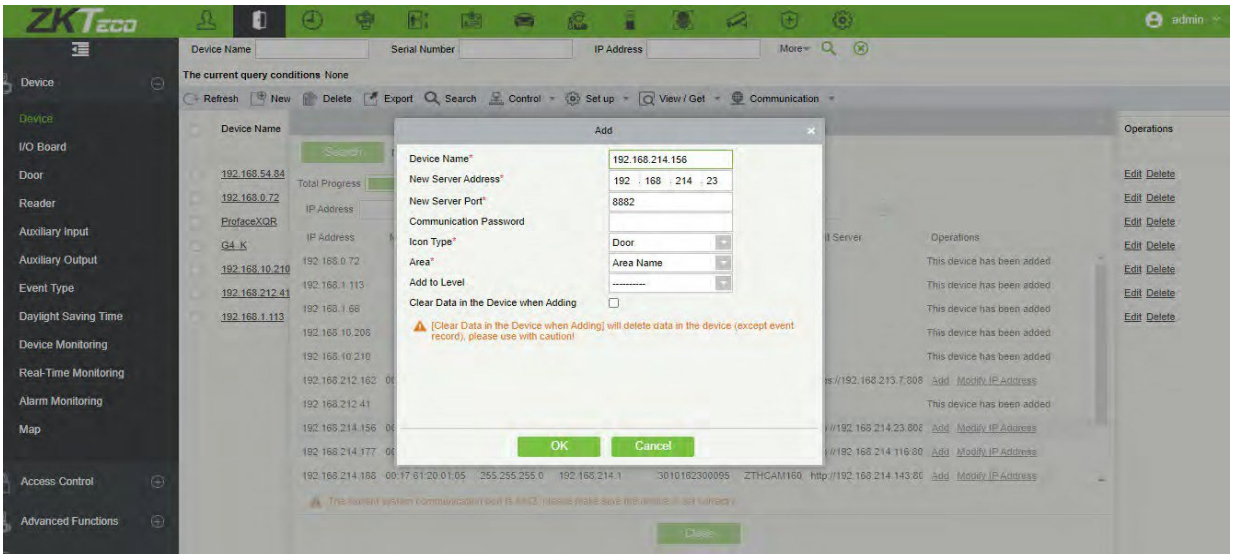


Clique em **Pesquisar** para buscar os dispositivos registrados.

Após a conclusão da busca, será exibido o número total de dispositivos registrados.



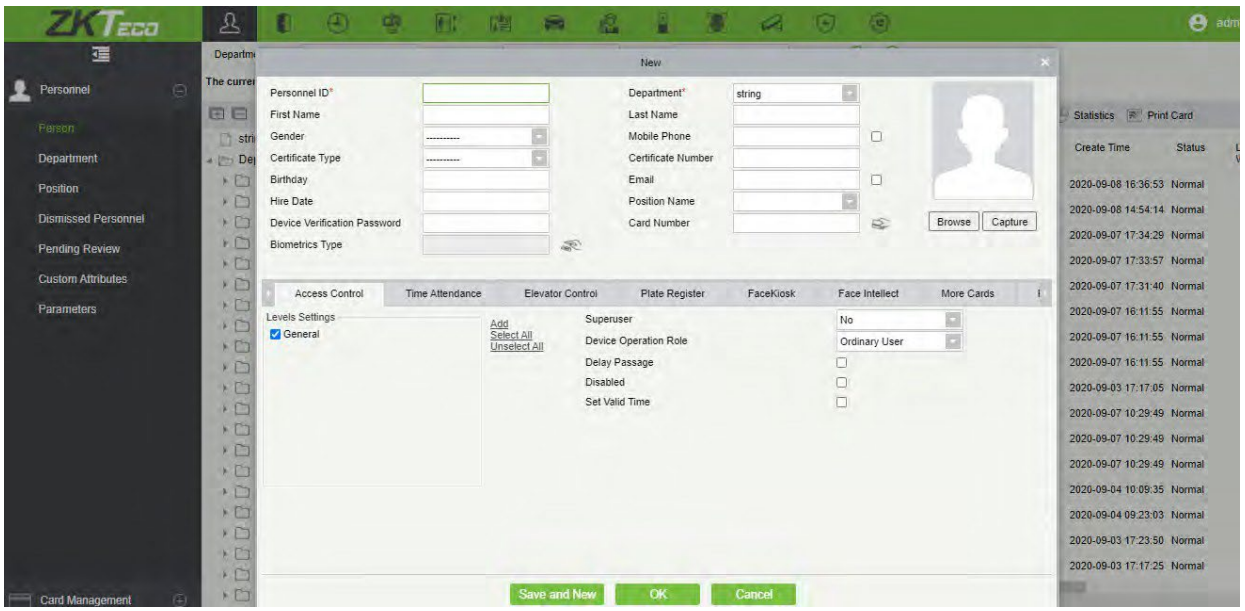
Clique em **Adicionar**, preencha os detalhes do dispositivo e, em seguida, clique em **OK** para concluir a adição dos dispositivos.



O endereço IP padrão do dispositivo pode entrar em conflito com outros na rede, por isso o endereço IP do novo dispositivo precisa ser modificado antes do uso.

Adicionar Pessoa

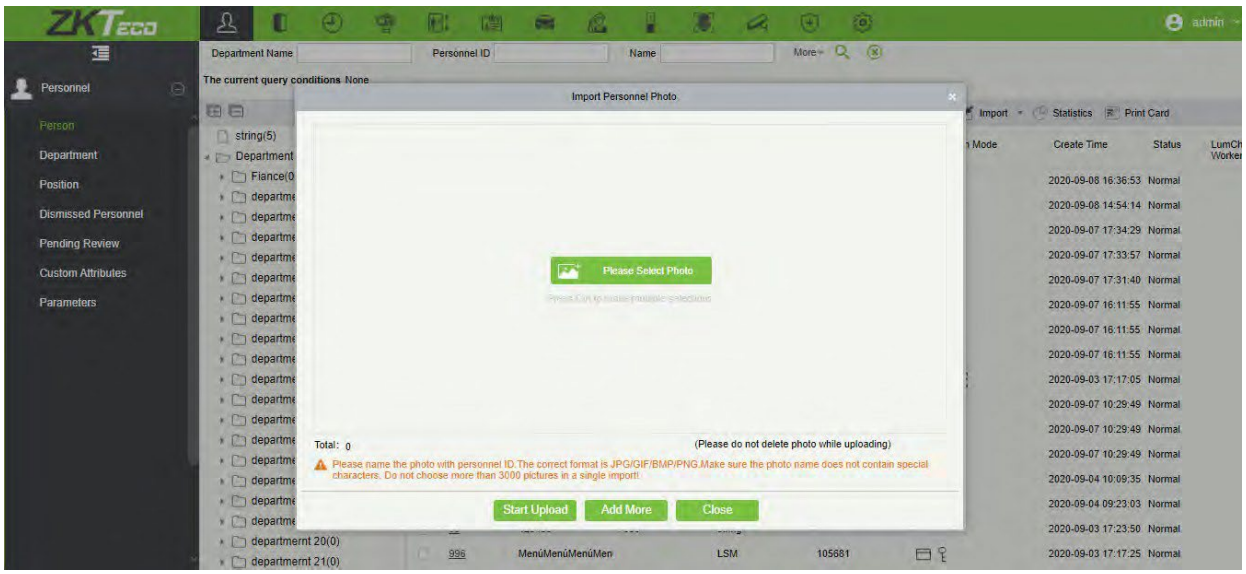
No módulo de Pessoal, clique em **Pessoa > Novo/Adicionar** para configurar os detalhes da pessoa.



Após preencher as informações da pessoa, clique em **OK** para salvar e sair, e a pessoa será exibida na lista de pessoal.

Importar fotos de pessoal em lote

No módulo de **Pessoal**, clique em **Pessoa > Importar > Importar Foto de Pessoal**, selecione a foto para importar.

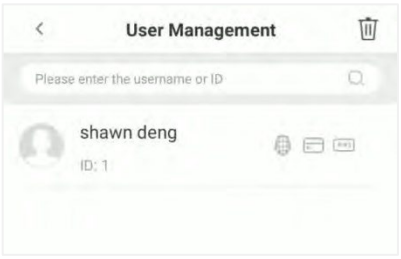


4.2 Pesquisar Usuário

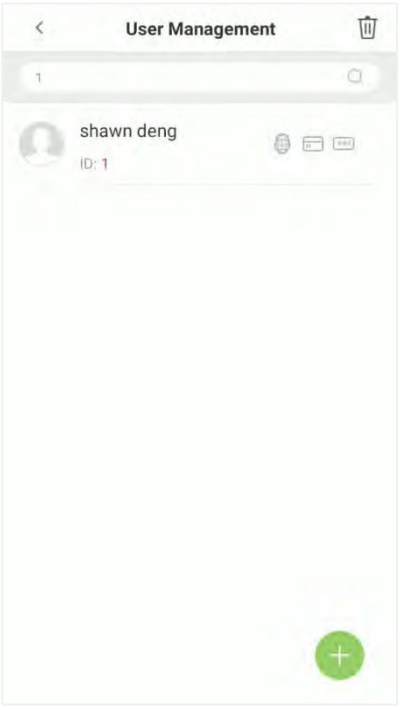
A função de pesquisa de usuário facilita a busca pelo usuário necessário na lista.

Toque na barra de busca localizada na interface de **Gerenciamento de Usuário** e procure pelo nome de usuário necessário.

Observação: Os usuários necessários podem ser buscados com base em seus IDs, nomes de usuário, sobrenomes ou nomes completos.



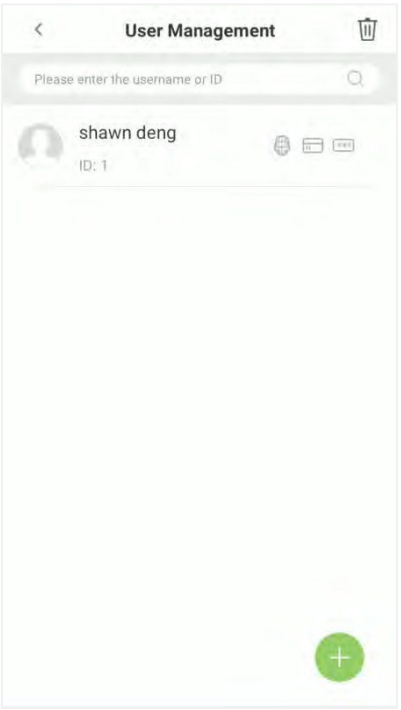
Toque na **barra de busca** para pesquisar pelos usuários com o ID/nome de usuário relevante, e o sistema encontrará automaticamente os usuários com informações relevantes à consulta de busca.

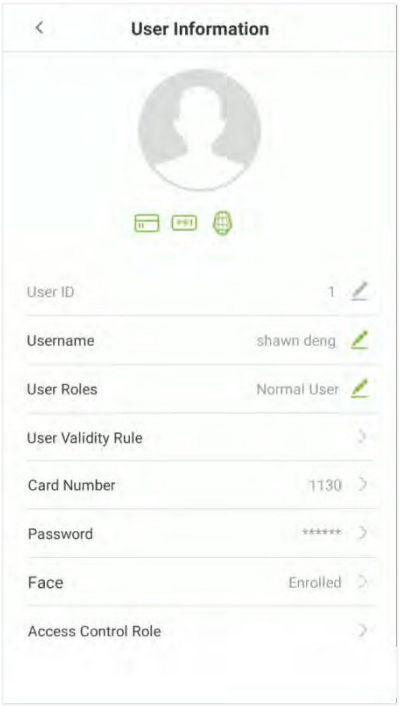


4.3 Editar Usuário

Na interface de **Gerenciamento de Usuário**, toque no usuário necessário da lista para editar.

Na interface de Informações do Usuário, toque no botão **Editar** correspondente para editar as informações do usuário necessário.



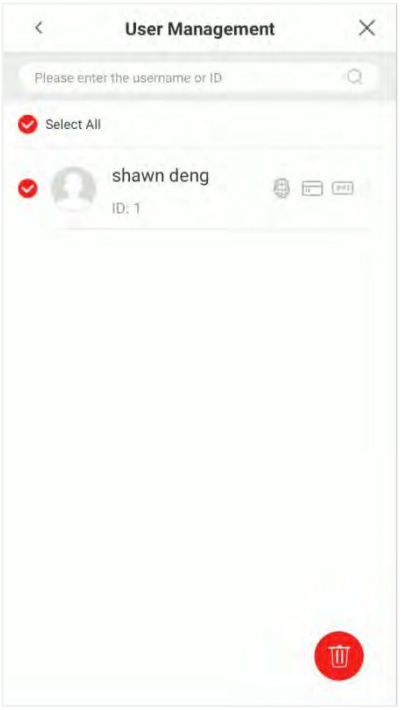


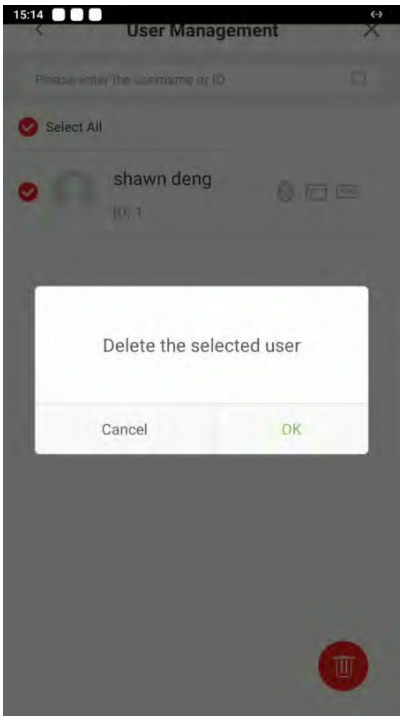
Observação: Por favor, observe que o ID do usuário não pode ser modificado, e as demais operações são similares à adição de um novo usuário. Para obter mais informações, consulte a seção "Adicionar Usuário".

4.4 Deletar Usuário

Na interface de **Gerenciamento de Usuário**, selecione o usuário necessário para deletar e toque no botão **Deletar** para excluir.

Na janela pop-up, toque em **OK** para confirmar a exclusão.





Observação: Ao deletar o usuário selecionado, todas as informações relacionadas ao usuário serão apagadas.

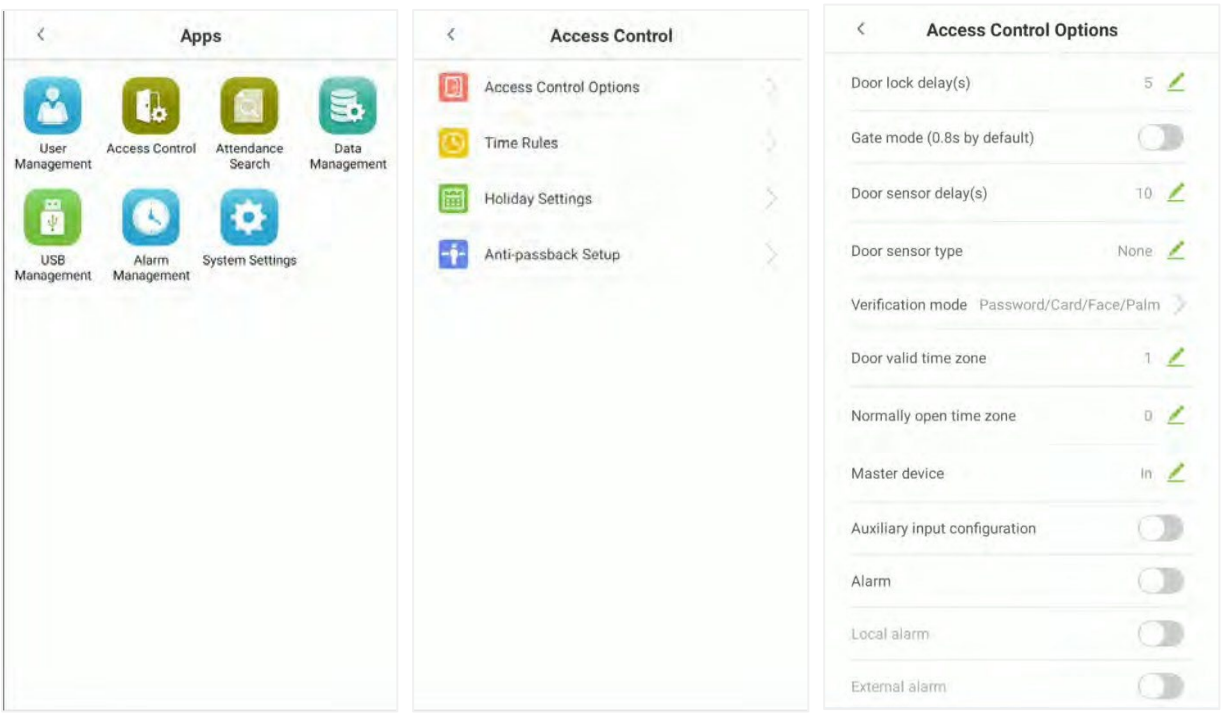
5 Configurações de Controle de Acesso

As **Configurações de Acesso** permitem definir os parâmetros de acesso.

5.1 Opções de Controle de Acesso

As **Opções de Controle de Acesso** são usadas para configurar os parâmetros de acesso. No menu principal, toque em **Controle de Acesso**.

As **Opções de Controle de Acesso** incluem as seguintes funções.



Descrição da Função

Função	Descrição
Atraso da Fechadura da Porta	O comprimento de tempo em que o dispositivo controla o trinco elétrico para estar no estado de desbloqueio. Valor válido: de 1 a 254 segundos.
Modo de Portão (0,8 segundos por padrão)	Alternar entre a opção **LIGADO** ou **DESLIGADO** para entrar ou sair do modo de portão. Quando definido como **LIGADO**, nesta interface, serão removidas as opções de Atraso do Trinco da Porta, Atraso do Sensor da Porta e Tipo de Sensor da Porta.
Atraso do Sensor de Porta	Se a porta não estiver trancada e permanecer aberta por um determinado período (Atraso do Sensor da Porta), um alarme será acionado. O valor válido para o Atraso do Sensor da Porta varia de 1 a 255 segundos.
Tipo de Sensor de Porta	Existem três tipos de sensores: **Nenhum**, **Normalmente Aberto** e **Normalmente Fechado**. Nenhum: Significa que o sensor da porta não está em uso. Normalmente Aberto: Significa que a porta está sempre deixada aberta quando a energia elétrica está ligada. Normalmente Fechado: Significa que a porta está sempre deixada fechada quando a energia elétrica está ligada.
Modo de Verificação	Os modos de verificação suportados incluem Senha/Cartão/Face, ID do Usuário, Senha, Cartão, Senha/Cartão, Senha+Cartão, Face, Face+Senha.

	Face+Cartão. O padrão é impressão digital/senha/rosto/cartão.
Período de Tempo Disponível da Porta	Para definir um período de tempo para a porta, de modo que a porta esteja disponível apenas durante esse período.
Período de tempo normalmente Fechado	Período de tempo programado para o modo Normalmente Fechado, para que a porta fique sempre fechada durante este período.
Equipamento mestre	Ao configurar o equipamento mestre, o status pode ser definido para sair ou entrar. **Saída**: O registro verificado no software é o registro de saída. **Entrada**: O registro verificado no software é o registro de entrada.
Configuração de entrada auxiliar	Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm.
Alarme	O padrão é Desativado.
Alarme local	Transmite um alarme sonoro ou um alarme de desmontagem a partir do local. Quando a porta está fechada ou a verificação é bem-sucedida, o sistema cancelará o alarme do local.
Alarme externo	O padrão é Desativado.
Redefinir configurações de acesso	Os parâmetros de redefinição do controle de acesso incluem atraso de fechadura da porta, atraso do sensor de porta, tipo de sensor de porta, modo de verificação, zona de tempo válida da porta, zona de tempo normalmente aberta, dispositivo principal e alarme. No entanto, os dados de controle de acesso apagados em Gerenciamento de Dados são excluídos.

5.2 Configurações de regras de tempo

Na interface de **Controle de Acesso**, toque em **Regras de Tempo** para configurar a Regra de Tempo.

Todo o sistema pode definir até 50 Regras de Tempo (ou seja, Regra de Tempo 1, Regra de Tempo 2, ... Regra de Tempo 50).

Cada Regra de Tempo representa 7 Zonas de Tempo, ou seja, 1 semana e 3 feriados, e cada Zona de Tempo é um período padrão de 24 horas por dia, em que o usuário só pode fazer a verificação dentro do período de tempo válido.

Para cada Zona de Tempo, é possível configurar no máximo 3 Períodos de Tempo. A relação entre esses Períodos de Tempo é "ou".

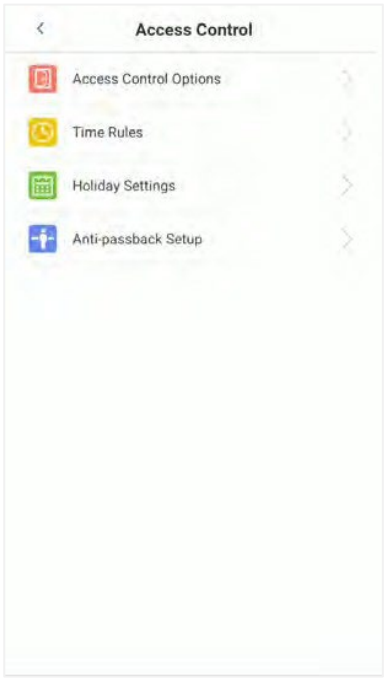
Quando o horário de verificação estiver dentro de qualquer um desses Períodos de Tempo, a verificação será bem-sucedida e válida.

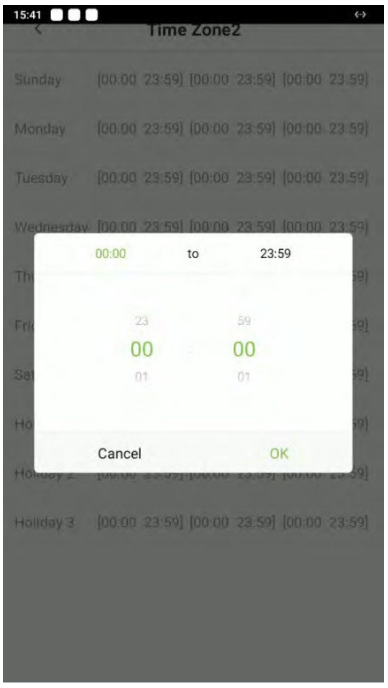
O formato da Zona de Tempo para cada Período de Tempo é HH MM-HH MM, com precisão de minutos no formato de 24 horas.

Toque na caixa cinza para pesquisar pela Regra de Tempo necessária. Insira o conjunto de Regras de Tempo necessário (por exemplo, pesquise como "Regra de Tempo 1"..."Regra de Tempo 50").

Na interface da Zona de Tempo, toque no dia (por exemplo, domingo, segunda-feira...) em que o Período de Tempo precisa ser configurado.

Na interface do **Período de Tempo 1**, defina o horário de início e término e, em seguida, toque em **OK**.





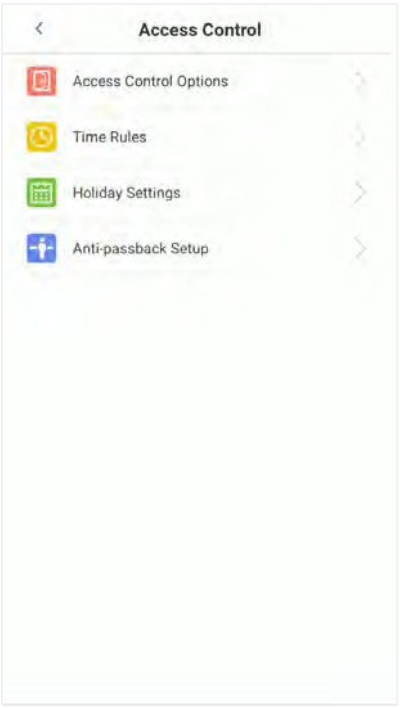
Observação:

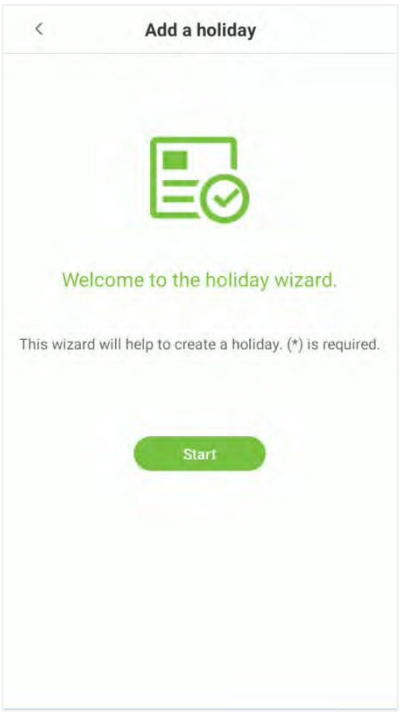
- Quando o horário de término é anterior ao horário de início (por exemplo, 23:57 ~ 23:56), isso indica que o acesso é proibido durante todo o dia.
- Quando o horário de término é posterior ao horário de início (por exemplo, 00:00 ~ 23:59), isso indica que o intervalo é válido.
- O Período de Tempo efetivo para manter a porta destrancada ou aberta o dia todo é (00:00 ~ 23:59), assim como quando o horário de término é posterior ao horário de início (por exemplo, 08:00 ~ 23:59).
- A Zona de Tempo 1 padrão indica que a porta permanece aberta o dia todo e não pode ser editada.

5.3 Configurações de feriado

Sempre que houver um feriado, talvez seja necessário um horário de acesso especial. No entanto, alterar o horário de acesso de cada usuário individualmente é extremamente trabalhoso. Portanto, é possível definir um horário de acesso para feriados que seja aplicável a todos os usuários, permitindo que eles abram a porta durante os feriados. O horário definido aqui será considerado como o padrão.

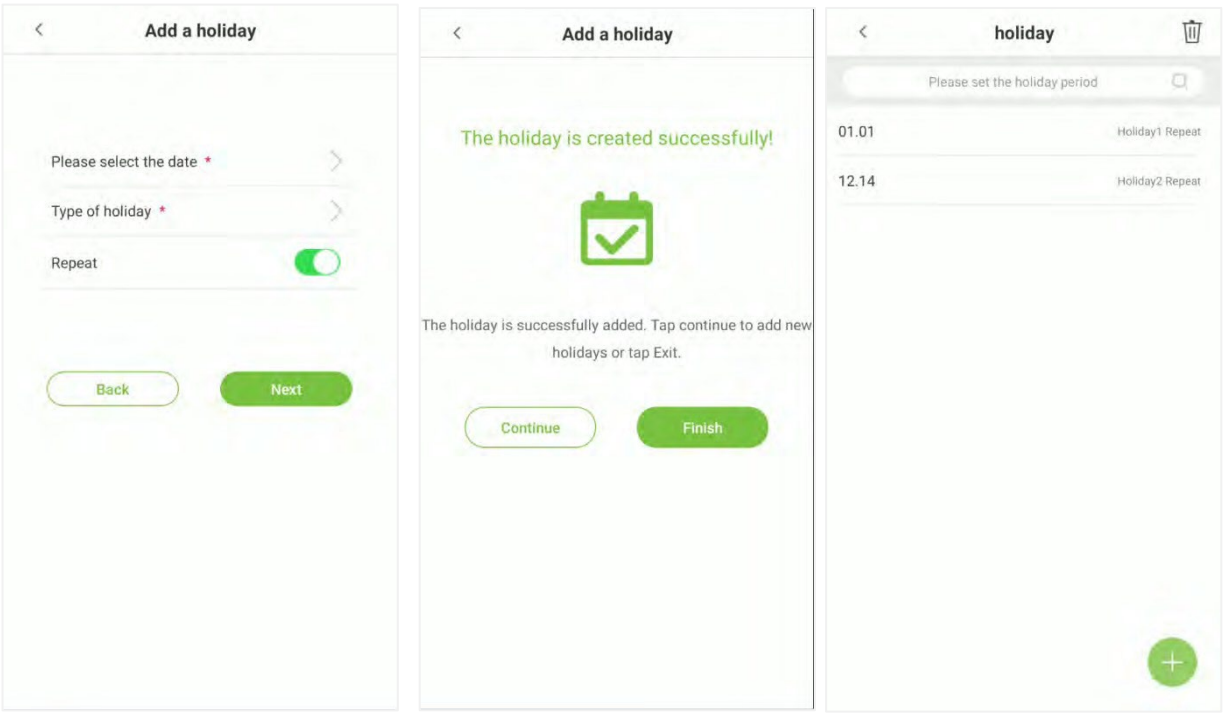
Toque em Configurações de Feriado e depois toque no botão + para criar um novo feriado.





Na interface de **Configurações de Feriado**, selecione uma data e o tipo de feriado. Ative **Repetir** para repetir o feriado anualmente e depois toque em **Próximo**.

Nesta interface, toque em **Concluir** para adicionar com sucesso o novo feriado criado, ou toque em **Continuar** para criar outro feriado.



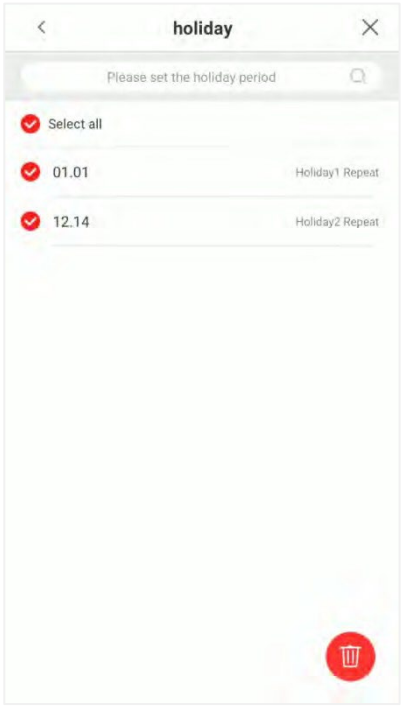
Editar Feriado

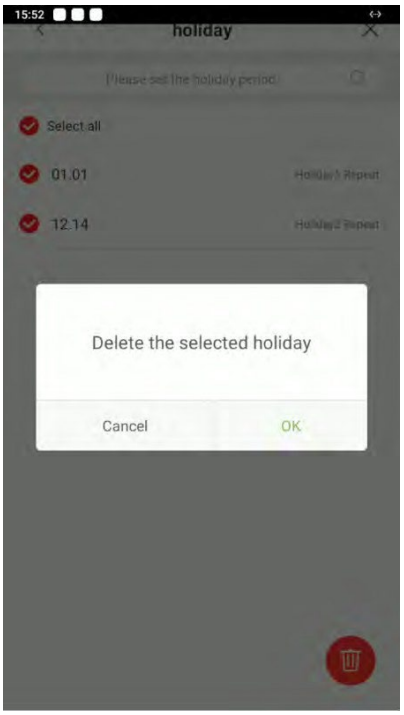
Na interface de **feriado**, toque no feriado necessário para fazer a modificação.

Delete um feriado

Na interface **feriado** toque em .

Selecione o feriado que deseja excluir, toque no botão no canto inferior direito. Na janela pop-up, toque em **OK** para confirmar a exclusão.





5.4 Configuração de anti-passback

O anti-passback é um método de controle direcional usado para controlar o uso indevido de um sistema de controle de acesso. Essa função envolve uma sequência específica em que os dispositivos de controle de acesso devem ser instalados tanto dentro quanto fora da porta para acesso.

Assim, se alguém entrar em uma área controlada por acesso seguindo outra pessoa sem autenticação no dispositivo biométrico, na próxima vez em que essa pessoa tentar sair da área, a porta não abrirá. Essa função é usada para detectar se o acesso do usuário é legal, determinando o último registro de acesso do usuário e a direção de controle local, o que pode efetivamente impedir a passagem indevida.

A configuração de anti-passback pode ser dividida em três tipos**:**

Sem anti-passback: A função de anti-passback está desativada, o que significa que a verificação bem-sucedida tanto no dispositivo mestre quanto no dispositivo escravo pode destrancar a porta. O estado de registro de frequência não é salvo nesta opção.

Anti-passback de saída: Após um usuário realizar o check-out, somente se o último registro for um check-in, o usuário poderá fazer check-out novamente; caso contrário, o alarme será acionado. No entanto, o usuário pode fazer check-in livremente.

Anti-passback de entrada: Após um usuário fazer check-in, somente se o último registro for um check-out, o usuário poderá fazer check-in novamente; caso contrário, o alarme será acionado. No entanto, o usuário pode fazer check-out livremente.

Anti-passback de Entrada/Saída: Depois que um usuário faz check-in/check-out, somente se o último registro for um registro de check-out, o usuário poderá fazer check-in novamente; ou se for um registro de check-in, o usuário poderá fazer check-out novamente; caso contrário, o alarme será acionado.

Observação: Quando o usuário não possui nenhum registro durante a primeira verificação, a aprovação do anti-passback é passada diretamente. Essa direção de acesso depende da seleção da direção de controle do dispositivo, correspondendo ao estado do dispositivo.

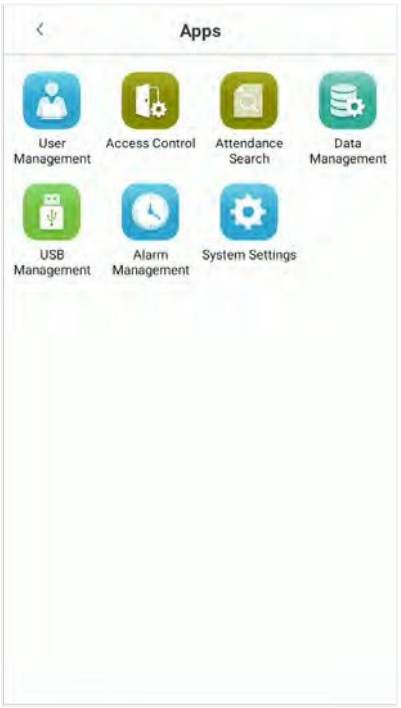
6 Procurar Registros

Os registros de acesso dos usuários serão salvos no dispositivo, facilitando a localização dos registros de frequência necessários dos usuários.

Os usuários podem buscar por registros de acesso, fotos de acesso e fotos de lista de bloqueio.

As buscas suportam a pesquisa por nome de usuário, ID ou uma combinação dos dois.

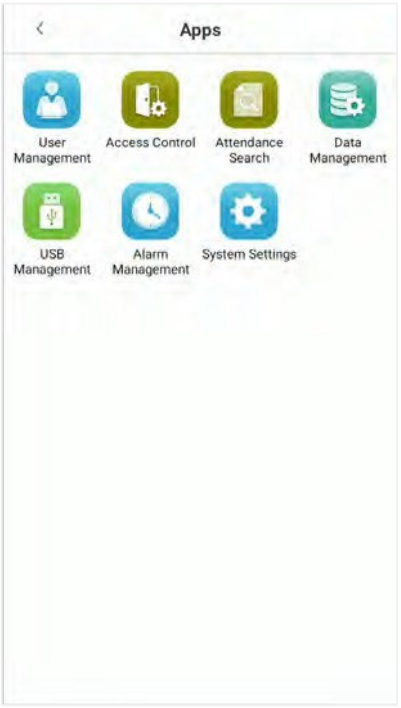
No menu principal, toque em **Procurar Registros** para buscar os registros de acesso do usuário desejado.

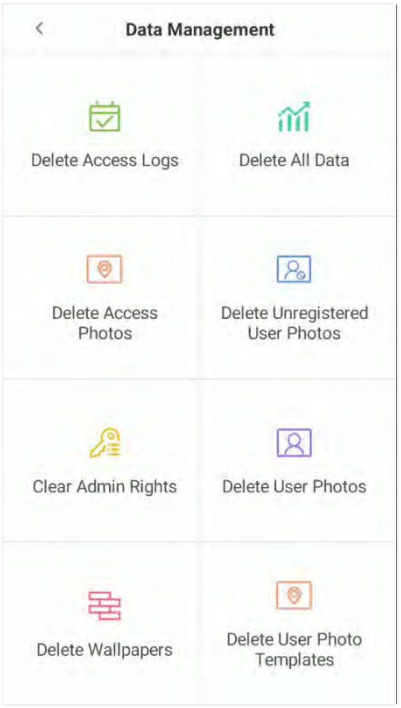


7 Gerenciamento de Dados

As Configurações de Gerenciamento de Dados permitem que os usuários gerenciem os dados do dispositivo, incluindo Excluir Registros de Acesso, Excluir Todos os Dados, Excluir Fotos de Acesso, Excluir Fotos de Usuários Não Registrados, Limpar Direitos de Administrador, Excluir Fotos de Usuários, Excluir Papéis de Parede e Excluir Modelos de Fotos de Usuários.

No menu principal, toque em **Gerenciamento de Dados** para gerenciar os dados.





Descrição da Função

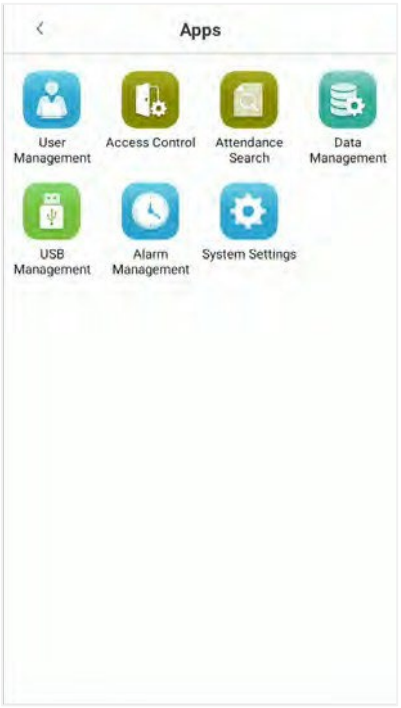
Função	Descrição
Excluir reg. de acesso	1. Exclui todos os registros. 2. Exclui os registros de acesso dentro de um intervalo de tempo especificado.
Excluir Todos os Dados	Exclui os dados comerciais armazenados no dispositivo, incluindo registros de acesso, dados biométricos de senha/facial/impressão digital★/cartão, privilégios do super administrador, fotos de usuários, dados de usuários e dados de controle de acesso.
Excluir Fotos de Acesso	Exclui todos os registros Exclui contas de usuário inválidas Exclui as fotos de acesso dentro de um intervalo de tempo especificado.
Excluir Fotos de Usuários Não Registrados	1. Exclui todos os dados (incluindo registros de acesso e as fotos do usuário na lista de bloqueio) 2. Exclui as fotos de usuários não registrados dentro de um intervalo de tempo especificado.
Limpar Direitos de Administrador	Transforma o super administrador em um usuário normal.
Excluir Fotos de Usuários	Exclui todas as fotos dos usuários.
Excluir Papéis de Parede	Exclui todos os papéis de parede armazenados no dispositivo.

Excluir Templates de Fotos de Usuários	Exclui os templates de rosto armazenados no dispositivo.

8 Gerenciamento USB

As funções específicas da interface de gerenciamento de USB são upload de disco USB, download de disco USB e configurações de disco USB.

No **menu principal**, toque em **Gerenciamento de USB** para gerenciar as configurações de USB.



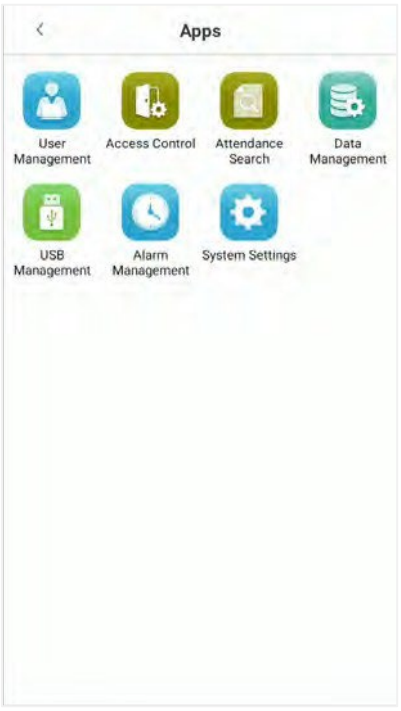
Descrição da Função

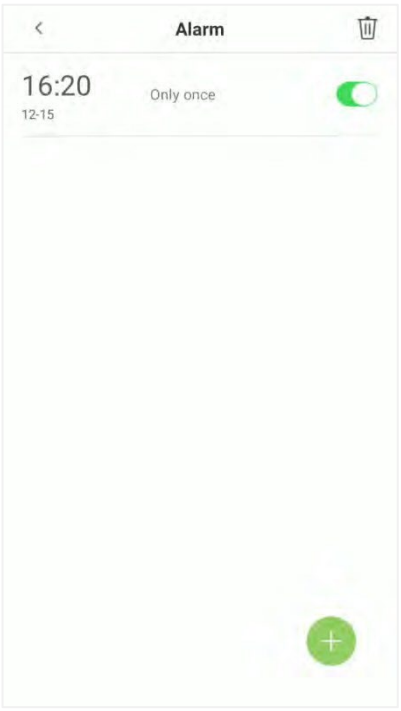
Função	Descrição
Carregar do USB	Carregar o conteúdo do disco USB para o dispositivo.
Baixar para USB	Baixar os dados do dispositivo para o disco USB.
Configurações USB	Configurar os parâmetros do disco USB.

9 Gerenciamento de Alarmes

Assim que um alarme for configurado, o dispositivo reproduzirá automaticamente o toque de alarme pré-selecionado quando o horário do alarme definido for alcançado. O toque do alarme será interrompido quando o tempo definido for decorrido.

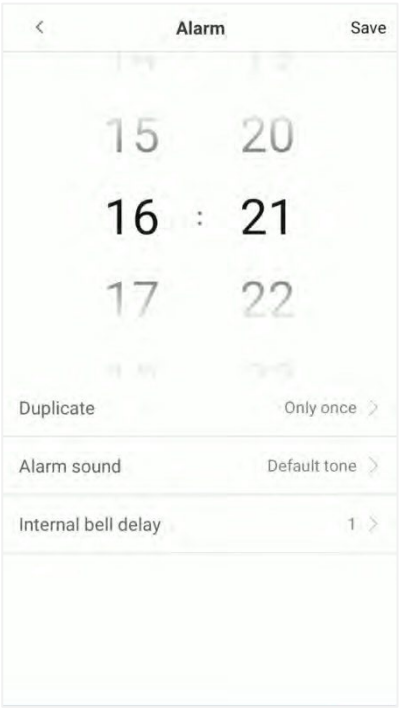
No **Menu Principal**, toque em **Gerenciamento de Alarmes** para configurar as configurações do alarme.





9.1 Adicionar Alarme

Na interface do Alarme, toque no botão + para configurar o alarme e, em seguida, toque em **Salvar** para salvar e atualizar.



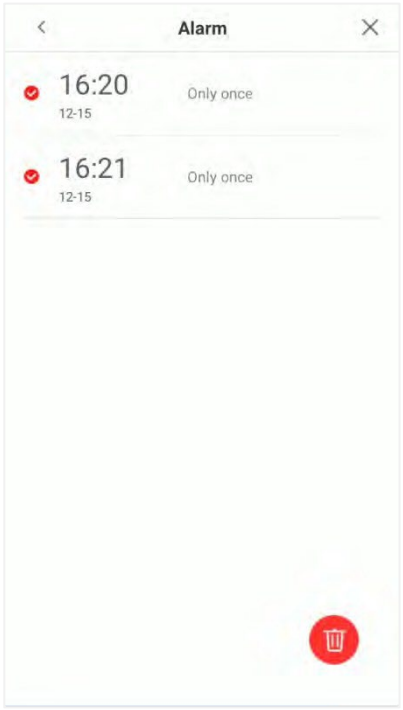
Descrição da Função

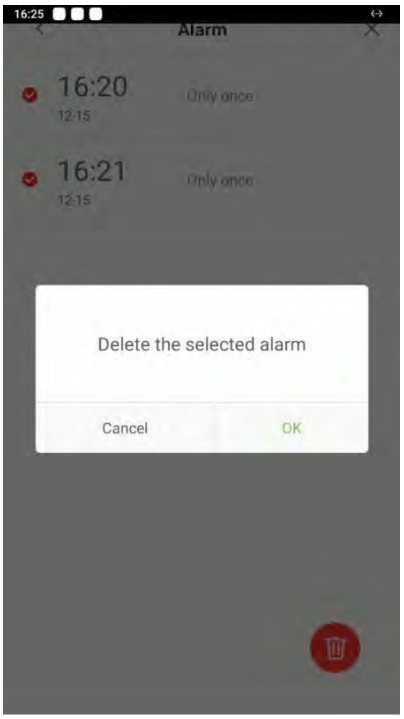
Função	Descrição
Duplicar	Defina o número necessário de repetições para repetir o toque programado.
Som do Alarme	Selecionar um toque de alarme.
Atraso do Sino Interno	Defina o tempo de repetição do sino interno. Os valores válidos variam de 1 a 999 segundos.

9.2 Excluir Alarme

Na interface do **Alarme**, toque no botão de exclusão e, em seguida, selecione o alarme desejado para excluir.

E então toque no botão que está sendo exibido no canto inferior direito da tela.

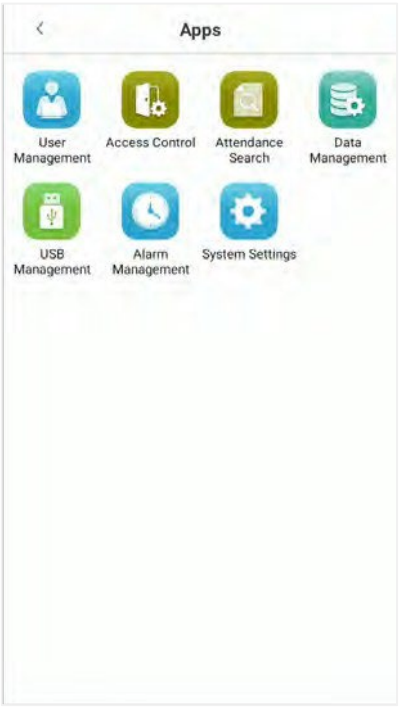


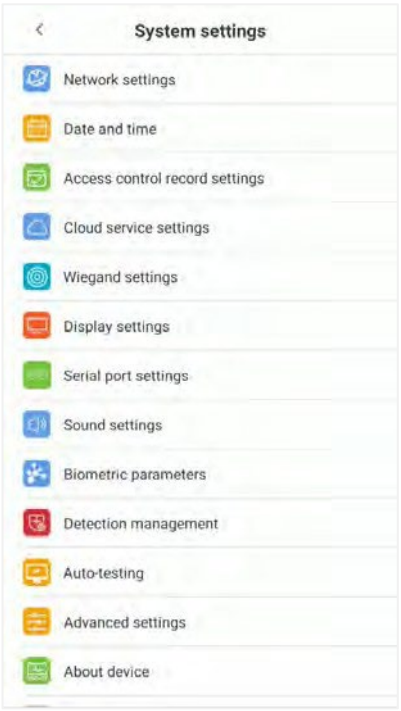


10 Configurações do Sistema

As Configurações do Sistema são usadas para configurar os parâmetros do sistema a fim de maximizar a capacidade do dispositivo de acordo com as necessidades do usuário. Nesta interface, o usuário pode editar as configurações de rede, data e hora, registros de controle de acesso, configurações de serviço em nuvem, configurações Wiegand, exibição e som, porta serial, parâmetros biométricos, gerenciamento de detecção, entre outros.

No menu principal, toque em **Configurações do sistema** para configurar as configurações do dispositivo.



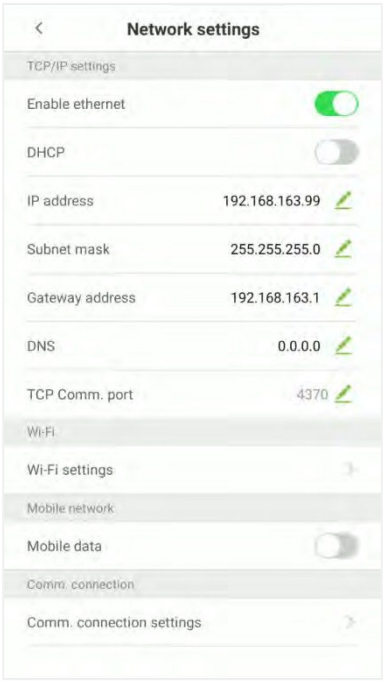


10.1 Configurações de Rede

Na interface de configurações do sistema, toque em **Configurações de Rede** para configurar as configurações.

10.1.1 Configurações Ethernet

Quando o dispositivo se comunica com um PC via Ethernet, a rede deve ser configurada para que o dispositivo e o computador estejam na mesma segmento de rede. Quando o dispositivo não está conectado à rede, toque em **Configurações TCP/IP** na interface de configurações de rede. A seguinte tela será exibida:



Descrição da Função

Função	Descrição
Ativar Ethernet	Habilitar para modificar os parâmetros do endereço de rede Ethernet. Se isso não estiver habilitado, os usuários não poderão modificar os parâmetros do endereço de rede Ethernet.
DHCP	Ativar o DHCP para atribuir um endereço IP à rede interna ou provedor de serviços de rede. Se o DHCP estiver ativado, você não poderá definir manualmente o IP do dispositivo.
Endereço IP	O IP padrão é 0.0.0.0 (pode ser alterado).
Máscara de sub-rede	O IP padrão é 0.0.0.0 (pode ser alterado).
Endereço do Gateway	O IP padrão é 0.0.0.0 (pode ser alterado).
DNS	O IP padrão é 0.0.0.0 (pode ser alterado).
Porta de comunicação TCP	A porta TCP padrão é 4370 (pode ser alterada).

Observação: Quando o dispositivo não está conectado à rede, os parâmetros, como o endereço IP e a máscara de sub-rede, são exibidos como 0.0.0.0; quando o dispositivo está conectado à rede, os parâmetros, como o endereço IP e a máscara de sub-rede, são automaticamente exibidos como valores configurados.

10.1.2 Configurações Wi-Fi

O dispositivo possui um módulo Wi-Fi, que pode ser embutido dentro do molde do dispositivo ou conectado externamente.

O módulo Wi-Fi permite a transmissão de dados por meio do Wi-Fi (Wireless Fidelity) e estabelece um ambiente de rede sem fio. O Wi-Fi é ativado por padrão no dispositivo. Se você não precisa usar a rede Wi-Fi, pode desativar o Wi-Fi ao alternar o botão correspondente.

Toque em **Configurações Wi-Fi** na interface de **Configurações deRede**. A seguinte tela será exibida:

- O Wi-Fi está desabilitado por padrão no dispositivo. Ative ou desative o Wi-Fi ao alternar o botão .
- Uma vez que o Wi-Fi é ativado, o dispositivo irá buscar pelas redes Wi-Fi disponíveis dentro do alcance da rede.
- Toque no nome do Wi-Fi apropriado na lista disponível, insira a senha correta na interface de senha e, em seguida, toque em Conectar ao Wi-Fi.

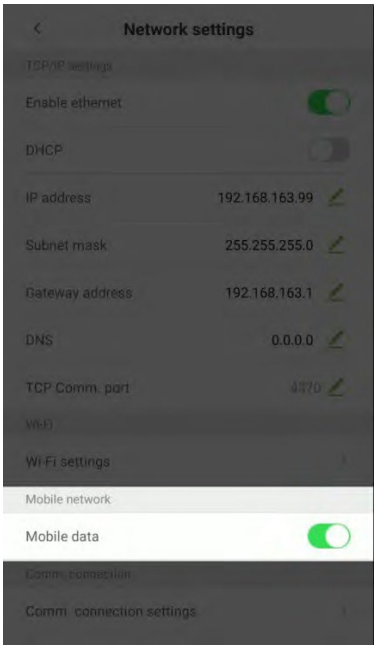
Quando o Wi-Fi é conectado com sucesso, a mensagem "Salvo com sucesso!" será exibida na lista de Wi-Fi, e a interface inicial exibirá o logotipo do Wi-Fi .

10.1.3 Configurações de Rede Móvel

Quando o dispositivo é aplicado a uma rede de discagem, certifique-se de que o dispositivo esteja dentro da área de cobertura do sinal do operador móvel (GPRS/4G).

Por favor, insira o cartão IOT no módulo 4G antes de habilitar. Em seguida, toque em **Dados móveis** para habilitar ou desabilitar a rede móvel na interface de **Configurações de Rede**.

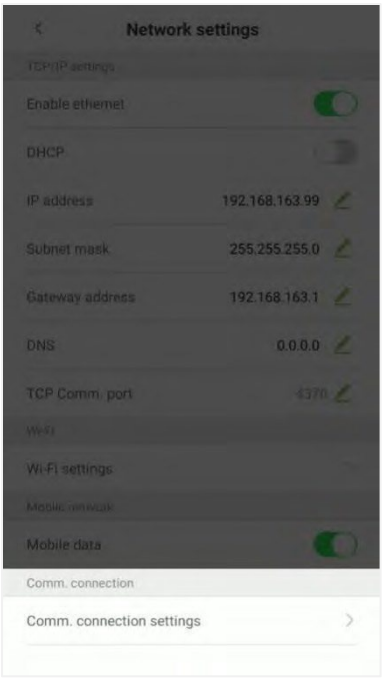
Uma vez ativado, o dispositivo é conectado automaticamente.

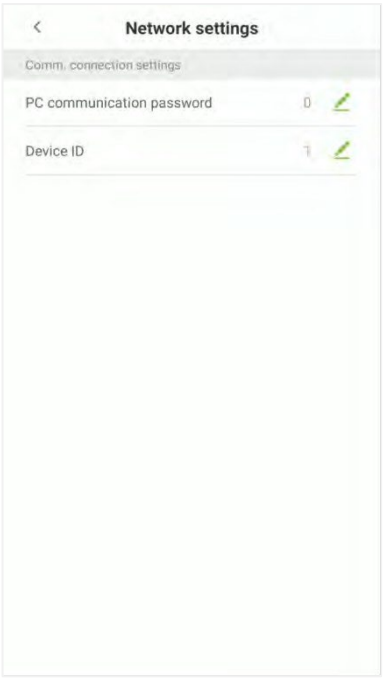


10.1.4 Configurações de Conexão de Comunicação

Para aumentar a segurança e a confidencialidade dos dados de acesso, é necessário definir uma senha de conexão. Para uma conexão bem-sucedida entre o software do PC e o dispositivo, a senha de conexão deve ser precisa.

Na interface de **Configurações de Rede**, toque em **Configurações de Conexão de Comunicação**.





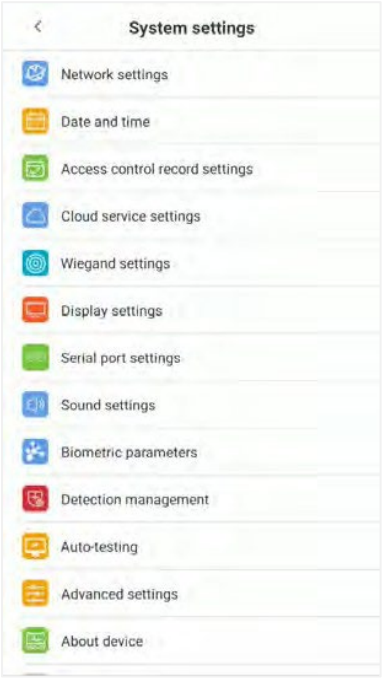
Descrição da Função

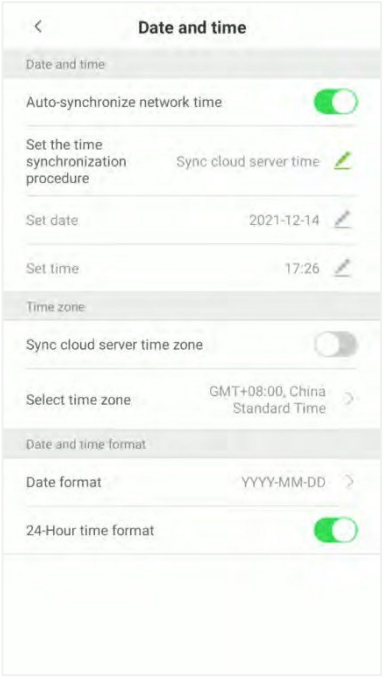
Função	Descrição
Senha de Comunicação com o PC	É usado para obter permissão de conexão ao usar a SDK offline ou a conexão SDK PULL. Se a senha não estiver correta, a conexão de comunicação não pode ser estabelecida. O valor varia de 0 a 999999. Quando o valor é 0, não há status de código.
ID do Dispositivo	O ID do dispositivo varia de 1 a 255. Se o sistema estiver usando o método de comunicação RS232/RS485, insira o ID do dispositivo durante a comunicação do software.

10.2 Data e Hora

10.2.1 Configurações de Data e Hora

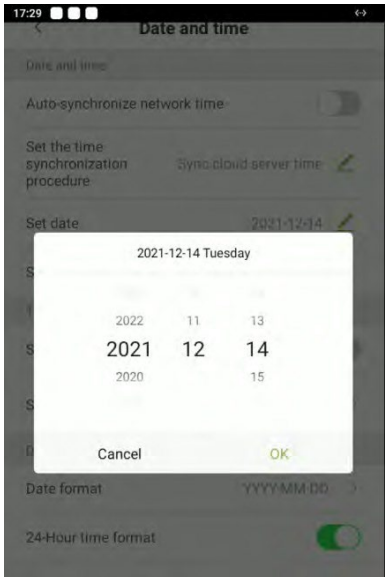
Na interface de configurações do sistema, toque em **Data e Hora** para entrar na interface de configurações de data e hora.





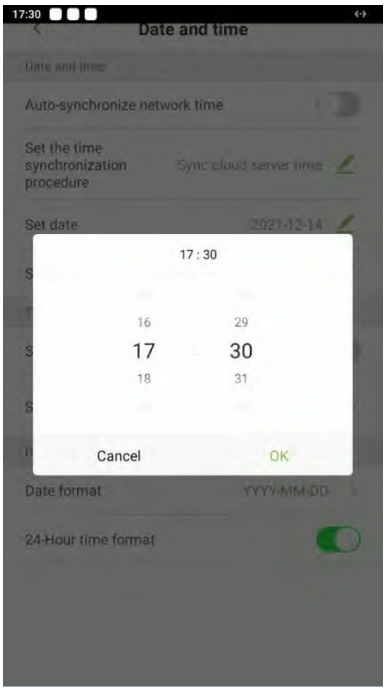
Toque em **Definir data** e deslize para cima e para baixo para definir o ano, mês e dia.

Após definir a data desejada, toque em **OK**.



Toque em **Definir hora** e deslize para cima e para baixo para definir a hora e o minuto.

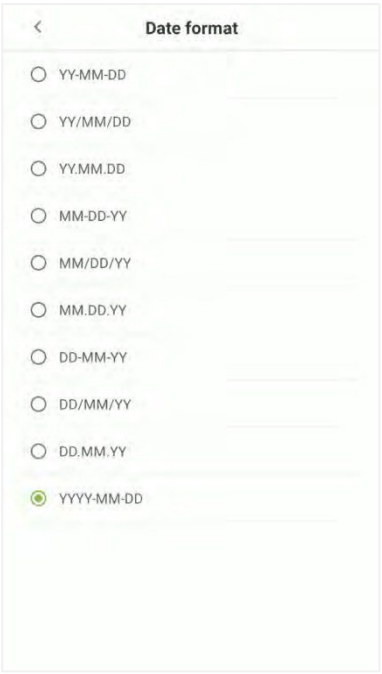
Após definir o horário, toque em **OK**.



10.2.2 Configurações de Formato de Data e Hora

Na interface de **Data e Hora**, toque em Formato de Data.

Na interface de **Formato de Data**, selecione o formato de data desejado.



Na interface de Data e Hora, toque na opção de **formato de hora de 24 horas** para habilitar essa função.

Descrições de Funções

Função	Descrição
Auto-sincronizar horário de rede	Está habilitado por padrão. Os usuários podem modificar a fonte de sincronização de tempo. Depois de desativado, os usuários podem modificar o procedimento de sincronização de tempo e configurar a data e a hora.
Sincronizar o tempo do servidor na nuvem	É usado para sincronizar o tempo entre o software e o servidor ao qual o dispositivo está conectado.
Sincronizar o tempo da rede	É usado para sincronizar o tempo real da internet.
Sincronizar o fuso horário do servidor na nuvem.	Essa opção está habilitada por padrão e é usada para sincronizar o fuso horário fornecido pelo software.
Selecionar fuso horário	O fuso horário padrão é GMT +8:00, Horário Padrão da China. Os usuários podem selecionar o fuso horário de acordo com suas necessidades.

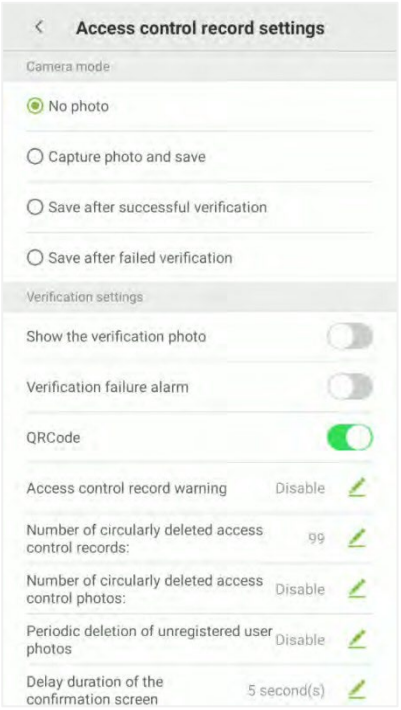
10.3 Configurações de Registro de Controle de Acesso

Na interface de **configurações do sistema**, toque em **Configurações de registro de controle de acesso** para acessar a interface de configurações de registro de acesso.

10.3.1 Modo de câmera

Essa função facilita a configuração das condições, como a necessidade de salvar as fotos e os registros de presença após o dispositivo capturar a foto da pessoa.

Toque no **modo de câmera** necessário que você gostaria de configurar:



Na interface do modo de câmera, os usuários podem definir se desejam tirar fotos e salvar fotos durante a verificação de acesso do usuário. As configurações são aplicáveis a todos os usuários.

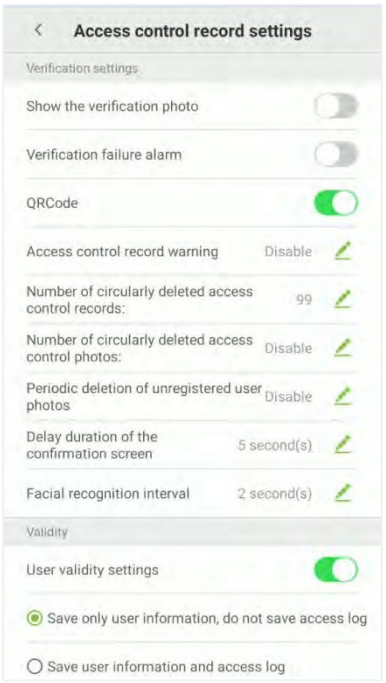
Descrições de Funções

Função	Descrição
Sem foto	Se esse modo for selecionado, o dispositivo não tira fotos durante a autenticação.
Capturar foto e salvar	Se esse modo for selecionado, o dispositivo captura fotos dos usuários e salva as fotos durante a autenticação.

Salvar após verificação bem-sucedida	Se esse modo for selecionado, quando o usuário passar pela verificação, a foto será tirada e, em seguida, a foto será salva.
Salvar após verificação falha	Se esse modo for selecionado, o dispositivo tira uma foto quando o usuário falha na verificação e a salva.

10.3.2 Configurações de Autenticação

As configurações de autenticação facilitam a configuração dos parâmetros de verificação de acesso.



Descrições de Funções

Função	Descrição
Mostrar a foto de verificação	Se estiver habilitado, a foto do usuário será exibida; caso contrário, a foto do usuário não será exibida.
Alarme de falha na verificação	O alarme irá tocar quando a verificação falhar. Os tempos do alarme de falha na verificação podem ser configurados de 3 a 100 segundos, e o intervalo de falha na verificação pode ser configurado de 8 a 60 segundos.
QRCode	Se estiver habilitado, a câmera pode reconhecer a imagem do código QR capturada pela lente.

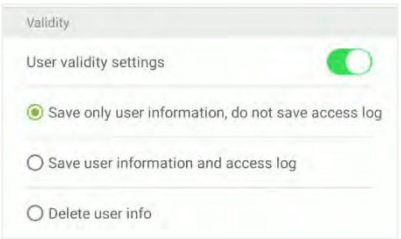
Aviso de espaço de registro de controle de acesso	Quando o espaço restante de registro de controle de acesso atinge um valor definido, o dispositivo exibirá automaticamente um aviso de memória de registro restante. Quando o valor for definido como 0, a função será desativada.
Número de registros de controle de acesso excluídos circularmente	Quando a memória de registro de acesso atinge a capacidade máxima, o dispositivo irá automaticamente excluir um valor definido de registros de acesso antigos. Quando o valor for definido como 0, a função será desativada.
Número de fotos de controle de acesso excluídas circularmente	Quando o espaço de armazenamento das fotos de controle de acesso atinge a capacidade máxima, o dispositivo irá automaticamente excluir um valor definido de fotos antigas de controle de acesso. Quando o valor for definido como 0, a função será desativada.
Exclusão periódica de fotos de usuários não registrados	Quando o espaço de armazenamento das fotos de usuários bloqueados atinge a capacidade máxima, o dispositivo irá automaticamente excluir um valor definido de fotos antigas de usuários bloqueados. Quando o valor for definido como 0, a função será desativada.
Duração do atraso da tela de confirmação	Essa é a duração de tempo em que as informações do usuário serão exibidas na tela do sistema após uma verificação bem-sucedida.
Intervalo de verificação facial	Este é o intervalo de tempo de correspondência do modelo facial que os usuários podem definir de 0 a 9 segundos.

10.3.3 Período de validade das informações do usuário

Isso é usado para determinar se os períodos de validade do usuário estão habilitados ou desabilitados ao registrar usuários.

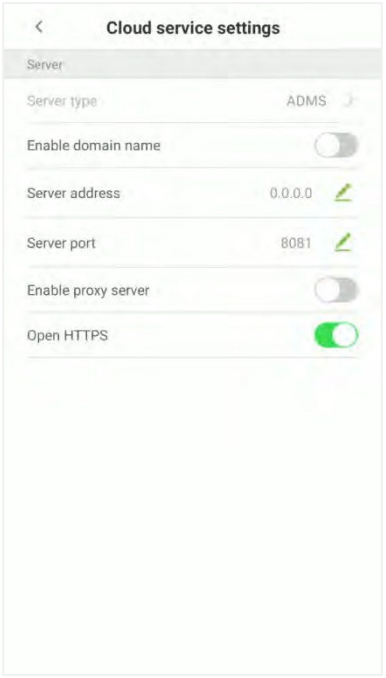
Toque em **Configurações de validade do usuário** para habilitar.

Quando as **Configurações de validade do usuário** estiverem habilitadas, a seguinte interface será exibida. Selecione a configuração que você deseja configurar.



10.4 Configurações do Servidor Nuvem

Na **interface de configurações do sistema**, toque em **Configurações de serviço em nuvem** para entrar na interface de configurações do serviço em nuvem.

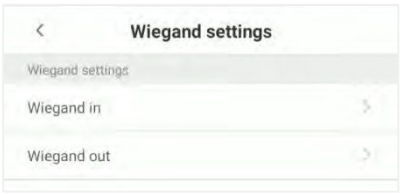


Descrições de Funções

Função		Descrição
Ativar nome de domínio	**Endereço do servidor**	Uma vez habilitada esta função, será utilizado o modo de nome de domínio "http://...", como http://www.XYZ.com, enquanto "XYZ" será o nome de domínio (quando este modo está **LIGADO**).
Endereço do servidor	**Endereço do servidor**	Endereço IP do servidor ADMS.
	Porta do servidor	Porta usada pelo servidor ADMS.
Ativar servidor proxy		Ao optar por habilitar o proxy, você precisa definir o endereço IP e o número da porta do servidor proxy.
HTTPS		Se estiver habilitado, é necessário reiniciar para ter efeito, e os dados são enviados para o terminal de push. O endereço é alterado de HTTP para HTTPS.

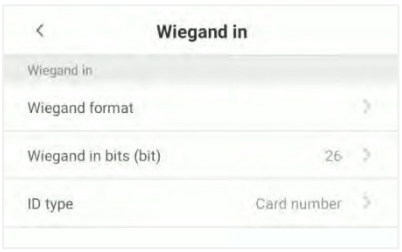
10.5 Configuração Wiegand

Na interface de **configurações do sistema**, toque em **Configurações Wiegand** para acessar a interface conforme mostrado abaixo.



10.5.1 Entrada Wiegand

Na interface de **Configurações Wiegand**, toque em **Entrada Wiegand** para abrir as configurações.



Descrições de Funções

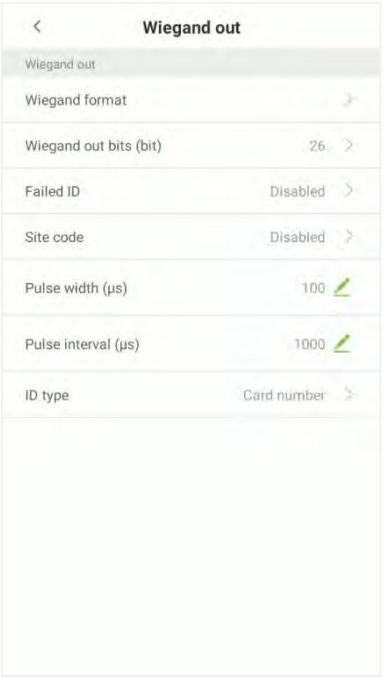
Função	Descrição
Formato Wiegand	O valor Wiegand pode ser de 26 bits, 34 bits, 36 bits, 37 bits ou 50 bits.
Número de bits Wiegand de entrada (bit)	Exibe o número de bits dos dados Wiegand. Após escolher o número de bits de entrada Wiegand, o dispositivo usará o número de bits configurado para encontrar o formato Wiegand adequado nas **Configurações de Formato Wiegand**.
Tipo de ID	O usuário pode inserir o **ID do usuário** ou o **número do cartão**.

Descrição dos formatos mais comuns de Wiegand:

Formato Wiegand	Descrição
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO Consiste em 26 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 13º bits, enquanto o 26º bit é o bit de paridade ímpar do 14º ao 25º bits. O 2º ao 25º bits são os números do cartão.
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO Consiste em 26 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 13º bits, enquanto o 26º bit é o bit de paridade ímpar do 14º ao 25º bits. Os 2º a 9º bits são os site code, enquanto os 10º a 25º bits são os números do cartão.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consiste em 34 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 17º bits, enquanto o 34º bit é o bit de paridade ímpar do 18º ao 33º bits. O 2º ao 25º bits são os números do cartão.
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consiste em 34 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 17º bits, enquanto o 34º bit é o bit de paridade ímpar do 18º ao 33º bits. Os 2º a 9º bits são o site code, enquanto os 10º a 25º bits são os números do cartão.
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consiste em 36 bits de código binário. O 1º bit é o bit de paridade ímpar do 2º ao 18º bits, enquanto o 36º bit é o bit de paridade par do 19º ao 35º bits. O 2º ao 17º bits são os códigos do dispositivo. Os bits 18 a 33 são os números do cartão e os bits 34 a 35 são os códigos do fabricante.
Wiegand36a	EFFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consiste em 36 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 18º bits, enquanto o 36º bit é o bit de paridade ímpar do 19º ao 35º bits. O 2º ao 19º bits são os códigos do dispositivo e os 20º ao 35º bits são os números do cartão.
Wiegand37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE Consiste em 37 bits de código binário. O 1º bit é o bit de paridade ímpar do 2º ao 18º bits, enquanto o 37º bit é o bit de paridade par do 19º ao 36º bits. O 2º ao 4º bits são os códigos do fabricante. O 5º ao 16º bits são os site code e os 21º ao 36º bits são os números do cartão.
Wiegand37a	EMMMFFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consiste em 37 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 18º bits, enquanto o 37º bit é o bit de paridade ímpar do 19º ao 36º bits. O 2º ao 4º bits são os códigos do fabricante. O 5º ao 14º bits são os códigos do dispositivo, e o 15º ao 20º bits são os site code e os 21º ao 36º bits são os números do cartão.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consiste em 50 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 25º bits, enquanto o 50º bit é o bit de paridade ímpar do 26º ao 49º bits. O 2º ao 17º bits são os site code e os 18º ao 49º bits são os números do cartão.
"**C**" Número do cartão; "**E**" paridade par; "**O**" paridade ímpar; "**F**" Código de instalação; "**M**" Código do fabricante; "**P**" Paridade e "**S**" site code.	

10.5.2 Saída Wiegand

Na interface de configurações Wiegand, toque em **Saída Wiegand** para abrir a interface de saída Wiegand.

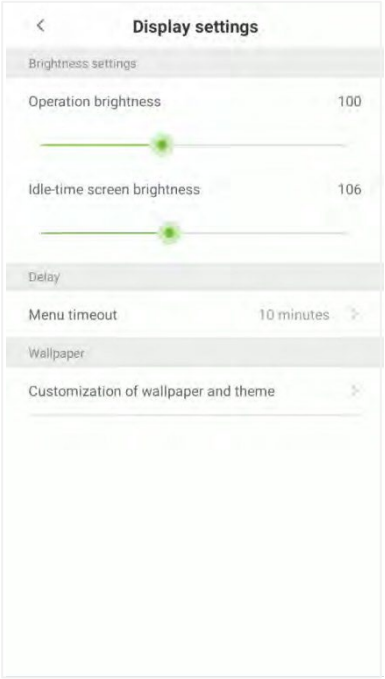


Descrições de Funções

Função	Descrição
Formato Wiegand	Os valores variam de 26 bits, 34 bits, 36 bits, 37 bits e 50 bits.
Número de bits Wiegand de saída (bit)	Depois de escolher o formato Wiegand, você pode selecionar um dos dígitos de saída correspondentes no formato Wiegand.
ID falhou	Se a verificação falhar, o sistema enviará o ID falhado para o dispositivo e substituirá o número do cartão ou o ID da pessoa pelos novos.
Site code	É semelhante ao ID do dispositivo, exceto que pode ser definido manualmente e repetido com dispositivos diferentes. O valor padrão varia de 0 a 256.
Largura de pulso (us)	A largura do pulso representa as mudanças na quantidade de carga elétrica com capacitância de alta frequência regularmente dentro de um tempo especificado.
Intervalo de pulso (us)	O intervalo de pulso é o tempo entre os pulsos.
Tipo de ID	Selecione o tipo de ID como ID do usuário ou Número do cartão.

10.6 Configurações de exibição

Na interface de configurações do sistema, toque em **Configurações de exibição** para entrar na interface de configurações de exibição.

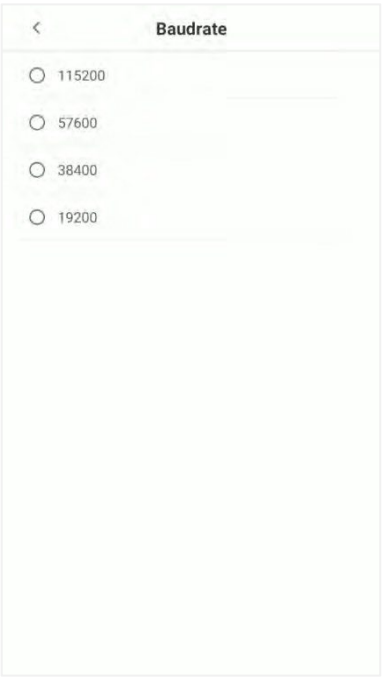


Descrições de Funções

Função		Descrição
Configuração de brilho	Brilho da operação	Defina o brilho de trabalho do dispositivo, como ao definir um parâmetro ou reconhecimento facial.
	Brilho da tela em modo de inatividade	Brilho da tela quando o dispositivo está no modo de espera.
Atraso	Tempo limite do menu	O tempo limite do menu ocorre quando nenhuma operação é realizada por um determinado período de tempo após o usuário entrar no menu, e o menu entra na tela de espera. As opções de parâmetro incluem: 1 minuto, 2 minutos, 5 minutos, 10 minutos. O menu (incluindo submenus) não será fechado automaticamente. Os usuários devem tocar em "Sair" para sair do menu.
Papel de parede	Personalização do papel de parede e tema	Escolha seu papel de parede favorito na interface de papéis de parede do tema.

10.7 Configurações da porta serial.

A função de Configurações da porta serial facilita o estabelecimento de comunicação com o dispositivo por meio de uma porta serial. Na interface de **configurações do sistema**, toque em **Configurações da porta serial** para entrar na interface de configurações da porta serial.



Descrições de Funções

Função	Descrição
Porta serial	Não utilizado: Não se comunica com o dispositivo através da porta serial.
Taxa de transmissão (Baudrate)	A taxa na qual os dados são comunicados com o PC, existem 4 opções de taxa de transmissão (baud rate): 115200, 57600, 38400 e 19200. Quanto maior a taxa de transmissão, maior é a velocidade de comunicação, mas também menor é a confiabilidade. Portanto, uma taxa de transmissão mais alta pode ser usada quando a distância de comunicação é curta; quando a distância de comunicação é longa, escolher uma taxa de transmissão mais baixa seria mais confiável.

10.8 Configurações de som

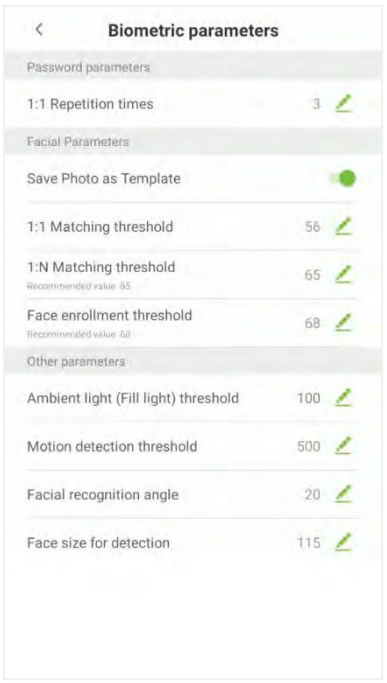
Na interface de **configurações do sistema**, toque em **Configurações de som** para entrar na interface de configurações de som.

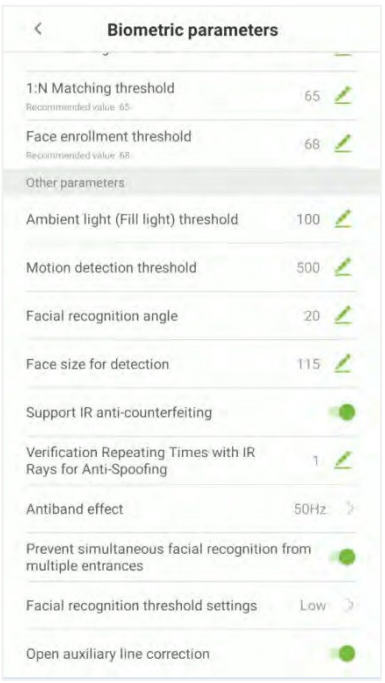
Descrições de Funções

Função	Descrição
Indicação de voz	Quando as indicações de voz estão habilitadas, os usuários receberão indicações de voz. As indicações de voz não serão recebidas quando essa configuração estiver desabilitada. Quando as indicações de voz estiverem desabilitadas e, em seguida, habilitadas novamente, o nível de volume será automaticamente ajustado para 1.
Prompt de toque	Este interruptor ativa/desativa o prompt de toque. Quando o prompt de toque está ativado, os usuários receberão indicações táteis. Quando o prompt de toque está desativado, nenhum prompt de toque será recebido.
Volume da voz	É usado para ajustar o volume. Isso só pode ser usado se as indicações de áudio estiverem habilitadas. Pode ser configurado de 0 a 15.

10.9 Parâmetros biométricos

Na interface de **configurações do sistema**, toque em **Parâmetros biométricos** para entrar na interface de parâmetros biométricos.





Descrições de Funções

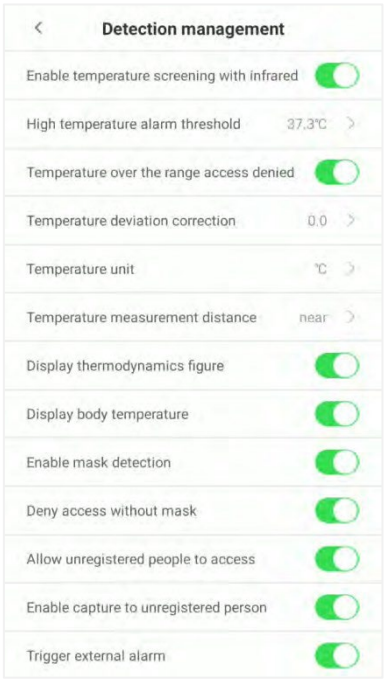
Função		Descrição
Parâmetros de senha	Número de repetições 1:1	O limite máximo de tentativas falhadas de verificação na verificação 1:1. Quando o número de tentativas falhadas de verificação atinge o valor definido, o sistema retornará à interface de espera.
Facial Parameters	Salvar foto como template	Selecione se deseja habilitar ou desabilitar.
	Limiar de correspondência 1:1.	Ao realizar a verificação facial 1:1, os dados faciais são coletados e comparados instantaneamente com os dados faciais usando um algoritmo 1:1. Isso é convertido em um valor que é então comparado a um valor definido. Se o valor da face escaneada exceder o valor definido, a verificação é aprovada. Caso contrário, a verificação falha. Quanto maior o limiar, mais precisa é a correspondência; quanto menor o limiar, maior é a taxa de sucesso da correspondência.

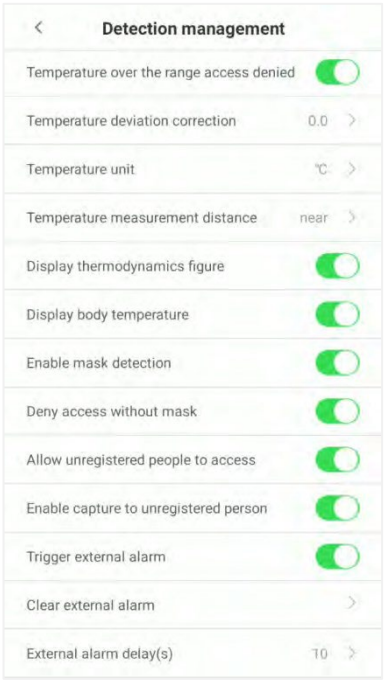
	Limiar de correspondência 1:N.	Ao realizar a verificação 1:N, os dados faciais são coletados e comparados instantaneamente com todos os modelos de rosto no sistema usando um algoritmo 1:N. Isso é convertido em um valor que é comparado a um valor definido. Se o valor da face escaneada exceder o valor definido, a verificação é aprovada. Caso contrário, a verificação falha. Quanto maior o limiar, mais precisa é a correspondência; quanto menor o limiar, maior é a taxa de sucesso da correspondência.
	Limiar de registro facial	No reconhecimento facial, quanto maior for o limiar definido, maior será a precisão do reconhecimento facial, o que pode levar a casos em que o reconhecimento não é realizado. Por outro lado, se o limiar for muito baixo, a precisão do reconhecimento facial será menor, o que pode levar a erros de julgamento e outros fenômenos. O valor padrão é 68.
Outros parâmetros	Limiar de luz ambiente (preenchimento de luz)	É usado para detectar a luminosidade da luz ambiente. Quando o brilho do ambiente circundante é inferior ao limiar, a luz complementar é ligada; quando o brilho é maior que o limiar, a luz complementar não é ligada. O valor padrão é 100.
	Limiar de detecção de movimento	É usado para detectar se há uma pessoa em movimento em frente ao dispositivo, a fim de determinar se a função de reconhecimento facial está habilitada. O valor padrão é 500.
	Ângulo de reconhecimento facial	Para limitar o ângulo do rosto no reconhecimento facial, o limite recomendado é de 20.
	Tamanho do rosto para detecção	O tamanho do rosto durante o reconhecimento facial. A faixa é de 65 a 320 cm. Quanto menor o valor, maior é a distância detectável, enquanto um valor maior indica uma distância mais próxima.
	Suporte a antifalsificação por infravermelho	Ele suporta a antifalsificação facial. Quando habilitado, ele pode realizar um reconhecimento de antifalsificação em fotos faciais para garantir a autenticidade do rosto.
	Tempo de repetição da verificação antifraude com raios infravermelhos	O limite máximo de tentativas de verificação falhadas durante a verificação facial, quando a IR Anti-counterfeiting está ativada, é de 1 a 6. Quando o número de tentativas de verificação falhadas atinge o valor definido, o sistema retornará à interface de espera.

	Efeito antirreflexo	Ao utilizar uma fonte de alimentação externa com energia CA, as imagens capturadas pelo dispositivo podem produzir ruído devido à variação da energia CA de ida e volta. De acordo com o uso específico da energia CA, ela pode ser ajustada para 50Hz ou 60Hz.
	Prevenir o reconhecimento facial simultâneo por várias entradas	Quando vários dispositivos estão instalados nas entradas lado a lado, por favor, habilite esta função para evitar o reconhecimento facial simultâneo por múltiplos dispositivos. Ajuste o limiar em três tipos: alto, médio e baixo. Quanto mais alto o limiar, mais estreita será a distância entre as diretrizes e menor será a faixa de reconhecimento facial na tela. Ao ajustar o limiar, é recomendado abrir a função de correção de linha auxiliar.
	Configurações de limiar de reconhecimento facial	Quando a função de Prevenir reconhecimento facial simultâneo por múltiplas entradas está habilitada, você pode definir o valor do limite facial como baixo, médio e alto.
	Abrir correção de linha auxiliar	Quando essa função está habilitada, o usuário é solicitado a posicionar o rosto no centro da tela do dispositivo para passar rapidamente pela autenticação.

10.10 Gerenciamento de detecção

Na interface de **configurações do sistema**, toque em **Gerenciamento de detecção** para entrar na interface de gerenciamento de detecção.
Essa interface é adicionada para habilitar a tela de temperatura com infravermelho e a detecção de máscara.





Descrições de Funções

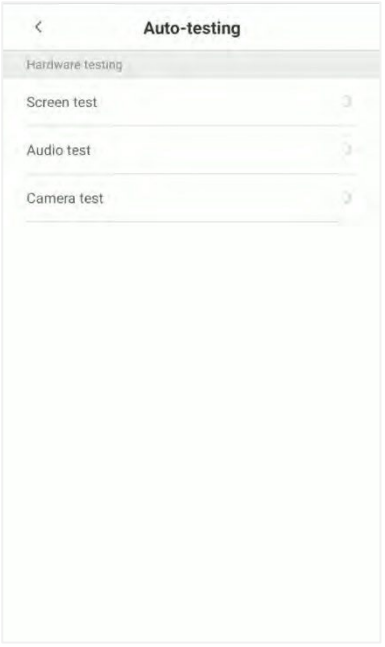
Função		Descrição
Triagem de temperatura com infravermelho	Habilitar triagem de temperatura com infravermelho	A tela de temperatura com módulo infravermelho pode ser configurada como **Desligada** ou **Ligada**.
	Limiar de alarme de temperatura alta	Definir o valor do limite de alarme para alta temperatura corporal. Quando a temperatura medida durante a verificação é maior que o valor definido, o dispositivo emitirá um aviso e um alarme sonoro. O limite de alarme padrão é de 37,30℃.
	Acesso negado quando a temperatura está acima do intervalo permitido	Quando habilitado, se a temperatura corporal medida do usuário estiver acima (ou abaixo) do limite de alarme, o acesso do usuário não será concedido, mesmo que sua identidade seja verificada. Quando desabilitado, o acesso é concedido ao usuário se sua identidade for verificada, independentemente de sua temperatura corporal.
	Correção de desvio de temperatura	Como o módulo de medição de temperatura lê uma pequena faixa de variação de um valor observado em ambientes incomuns (umidade, temperatura ambiente extrema, entre outros), os usuários podem definir aqui o valor de desvio para refletir a temperatura verdadeira da pessoa.

	Unidade de temperatura	The unit of body temperature can be toggled between Celsius (°C) and Fahrenheit (°F).
	Distância de medição de temperatura	Existem três modos ao medir a temperatura durante o processo de verificação, são eles: **Próximo**, **Médio** e **Distante**.
	Exibir figura termodinâmica	Habilitar ou desabilitar a exibição da imagem térmica de uma pessoa. Quando habilitada, a imagem térmica da pessoa será exibida no canto superior esquerdo do dispositivo durante o processo de detecção.
	Exibir temperatura corporal	Habilitar ou desabilitar a exibição da temperatura corporal. Quando habilitada, o dispositivo exibirá o valor da temperatura corporal do usuário durante o processo de verificação.
Detecção de máscara	Habilitar detecção de máscara	Habilitar ou desabilitar a função de detecção de máscara. Quando habilitada, o dispositivo identificará se o usuário está usando uma máscara durante a verificação.
	Negar acesso sem máscara	Habilitar ou desabilitar o acesso de uma pessoa sem máscara. Quando habilitado, o dispositivo negará o acesso de uma pessoa caso ela não esteja usando máscara.
	Permitir o acesso de pessoas não registradas	Habilitar ou desabilitar o acesso de pessoas não registradas. Quando habilitado, o dispositivo permite que a pessoa entre sem registro, desde que ela passe pela detecção.
	Acionar alarme externo	Quando habilitado, se a temperatura do usuário for superior ao valor limite definido ou a detecção de máscara estiver ativada, mas a máscara não estiver sendo usada pela pessoa, será acionado um alarme

	Limpar alarme externo	Isso limpa os registros de alarme acionados pelo dispositivo.
	Atraso do Alarme Externo (em segundos)	O tempo de atraso (em segundos) para acionar um alarme externo. Pode ser configurado em segundos. Os usuários podem desabilitar a função ou definir um valor entre 1 e 255.

10.11 Auto-teste

Na interface de **configurações do sistema**, toque em **Auto-teste** para entrar na interface de auto-teste.



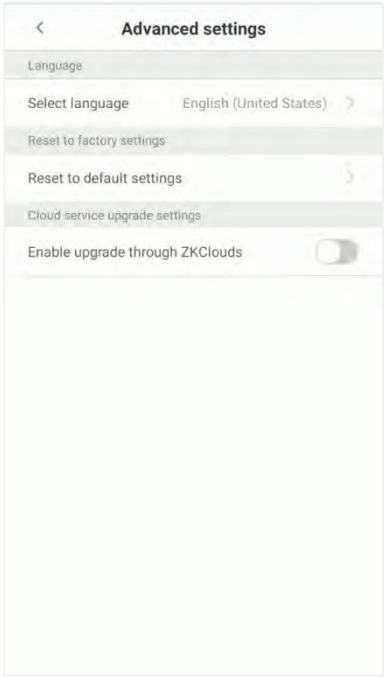
Descrições de Funções

Função	Descrição
Teste de tela	É usado para testar a exibição da tela. A tela exibirá testes nas cores vermelho, verde, azul, branco e preto. Verifique se a cor da tela está uniformemente correta em todas as áreas da tela. Toque em qualquer lugar da tela durante o teste para continuar o teste. Toque na tecla voltar para sair do teste.
Teste de áudio	O dispositivo realiza automaticamente testes de áudio reproduzindo arquivos de áudio armazenados nele. O teste de voz verifica principalmente se os arquivos de áudio do dispositivo estão completos e se os efeitos de áudio estão funcionando corretamente. Toque na tecla voltar para sair do teste.

Teste de câmera	É usado para testar se a câmera está funcionando corretamente. Verifique a imagem capturada para ver se a qualidade da imagem está nítida e utilizável.

10.12 Configurações avançadas

Na lista de **configurações do sistema**, toque em **Configurações avançadas** para entrar na interface de configurações avançadas.

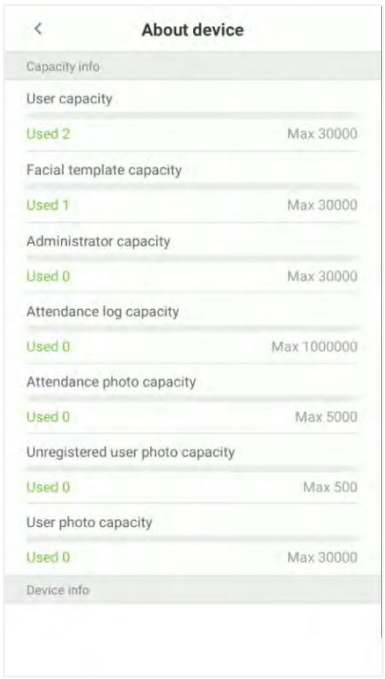


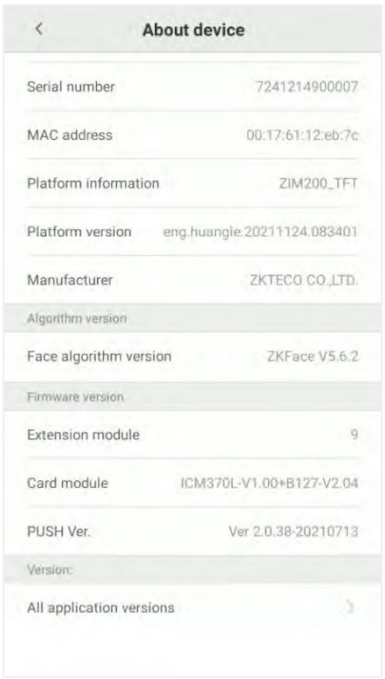
Descrições de Funções

Função	Descrição
Selecionar idioma	Selecione o idioma do dispositivo.
Redefinir para configurações de fábrica	Isso é usado para restaurar as configurações do dispositivo, incluindo as configurações de comunicação e as configurações do sistema, para as configurações de fábrica.
Configurações de atualização do serviço em nuvem	Se deseja habilitar a atualização do ZKClouds.

10.13 Sobre o dispositivo

Na interface de configurações do sistema, toque em **Sobre o dispositivo** para abrir a interface sobre o dispositivo.



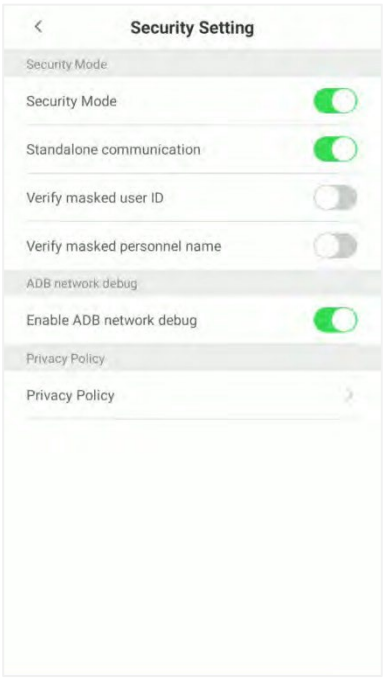


Descrições de Funções

Função	Descrição
Informações de capacidade	Ele exibe a capacidade atual do dispositivo em relação a usuários, modelos faciais, administradores, registros de controle de acesso, fotos de controle de acesso, fotos de usuários não registrados e fotos de usuários.
Informações do dispositivo	Ele exibe o nome do dispositivo, tipo de dispositivo, número de série, endereço MAC, versão do algoritmo, informações da plataforma e fabricante.
Versão do algoritmo	Ele exibe a versão do algoritmo facial do dispositivo
Versão do firmware	Ele exibe a versão de extensão do dispositivo, módulo de cartão e versão de push.
Versão	Ele exibe todas as versões de todos os aplicativos do sistema, como as configurações do sistema, gerenciamento de dados e outros aplicativos instalados.

10.14 Configuração de segurança

Na interface de **configurações do sistema**, toque em **Configuração de segurança** para abrir a interface de configuração de segurança.

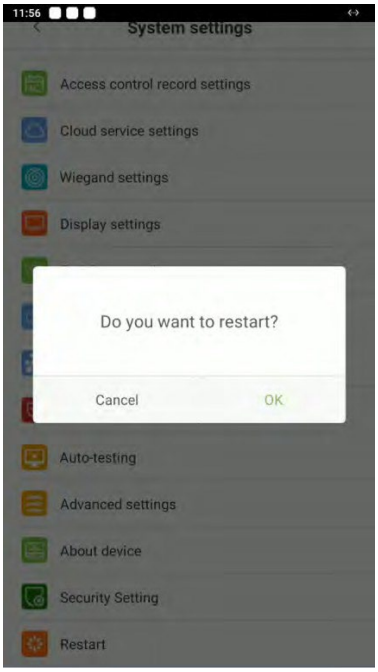


Descrições de Funções

Função	Descrição
Modo de segurança	Selecione se deseja habilitar o modo de segurança para proteger o dispositivo e as informações pessoais do usuário. Você pode configurar o dispositivo para funcionar offline e ocultar as informações pessoais do usuário para evitar vazamentos durante a verificação do usuário.
ADB network	Ele exibe o nome do dispositivo, o tipo de dispositivo, o número de série, o endereço MAC, a versão do algoritmo, as informações da plataforma e o fabricante.
Política de Privacidade	Exibir a política de privacidade do dispositivo.

10.15 Reiniciar

Na interface de **configurações do sistema**, toque em **Reiniciar**. O dispositivo apresentará uma janela pop-up, por favor, escolha se deseja reiniciar de acordo com suas necessidades.



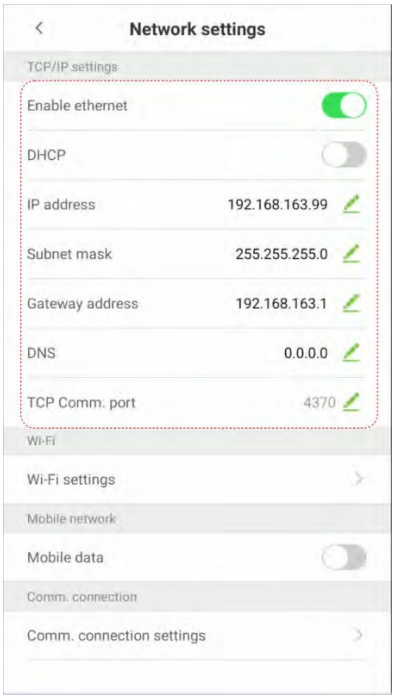
11 Conectar ao software ZKBioSecurity

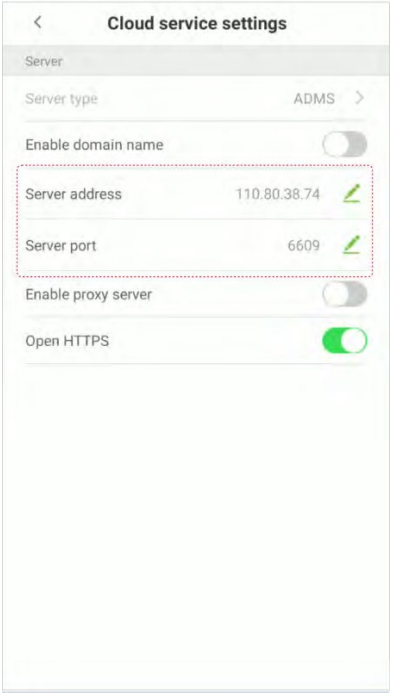
11.1 Configurar o endereço de comunicação

- **Lado do dispositivo**

1. Toque em **Configurações do sistema** > **Configurações de rede** > **Configurações TCP/IP** no menu principal para definir o endereço IP e o gateway do dispositivo.
   (**Observação:** O endereço IP deve ser capaz de se comunicar com o servidor ZKBioSecurity, preferencialmente na mesma segmento de rede que o endereço do servidor).

2. No menu principal, clique em **Configurações do sistema** > **Configurações do servidor de nuvem** para configurar o endereço do servidor e a porta do servidor.
   Endereço do servidor: Defina o endereço IP do servidor ZKBioSecurity.
   Porta do servidor: Defina a porta do servidor conforme o





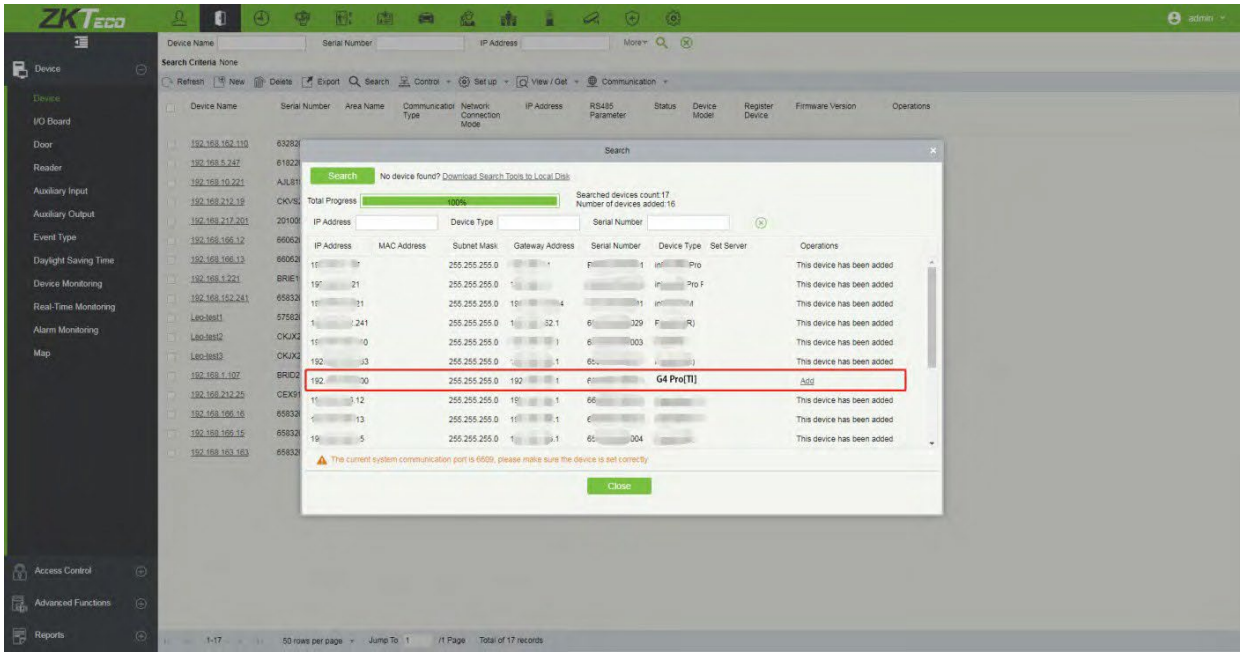
- **Lado do software**

Faça login no software ZKBioSecurity, clique em **Sistema > Comunicação > Monitor de comunicação** para configurar a porta do serviço ADMS, conforme mostrado na figura abaixo:

11.2 Adicionar dispositivo no software

Adicione o dispositivo fazendo uma pesquisa. O processo é o seguinte:

1. Clique em **Acesso > Dispositivo > Pesquisar** para abrir a interface de pesquisa no software.
2. Clique em **Pesquisar** e será exibida a mensagem [Procurando...].
3. Após a pesquisa, a lista e o número total de controladores de acesso serão exibidos.

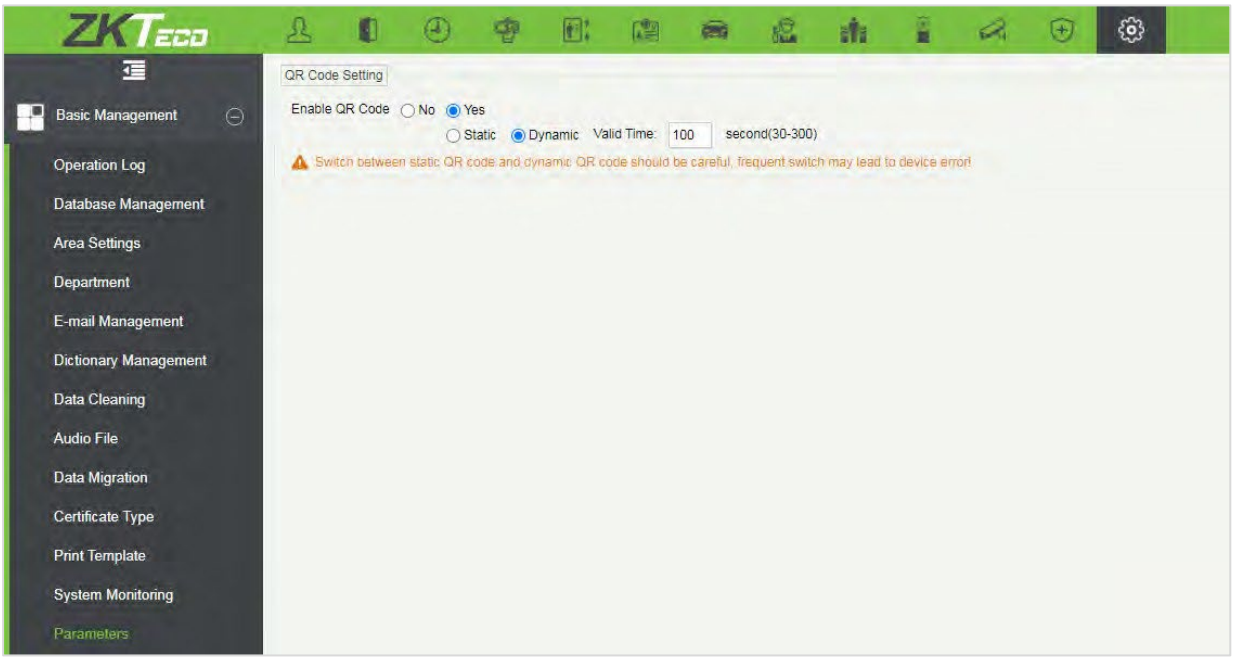


4. Clique em **[Adicionar]** na coluna de operação, uma nova janela será aberta. Selecione o tipo de ícone, área e nível a partir de cada menu suspenso e clique em **[OK]** para adicionar o dispositivo.

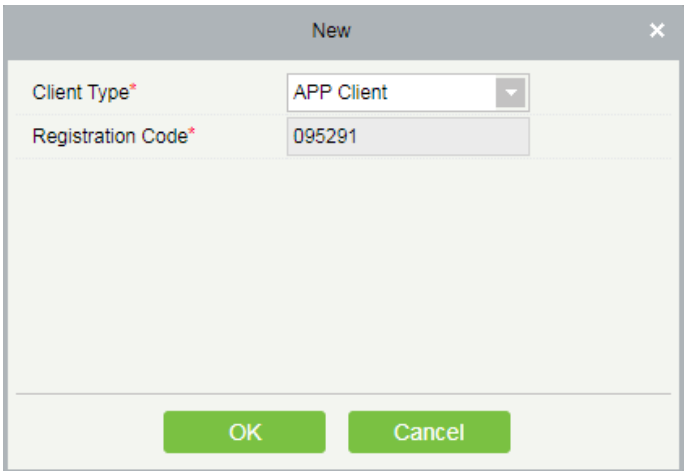
11.3 Credencial móvel

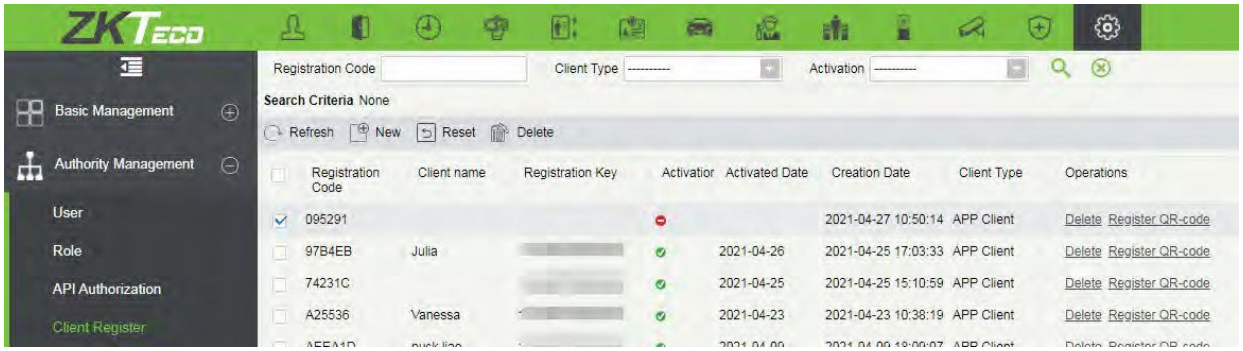
Após baixar e instalar o aplicativo, o usuário precisa configurar o servidor antes de fazer o login. Os passos são os seguintes:

1. Em **[Sistema] > [Gerenciamento Básico] > [Parâmetros]**, defina "Habilitar Código QR" para "Sim" e selecione 1. Em **[Sistema] > [Gerenciamento Básico] > [Parâmetros]**, defina "Habilitar Código QR" para "Sim" e selecione 1.



2. No servidor, escolha **[Sistema] > [Gerenciamento de Autoridade] > [Registro de Cliente]** para adicionar um cliente de aplicativo registrado.

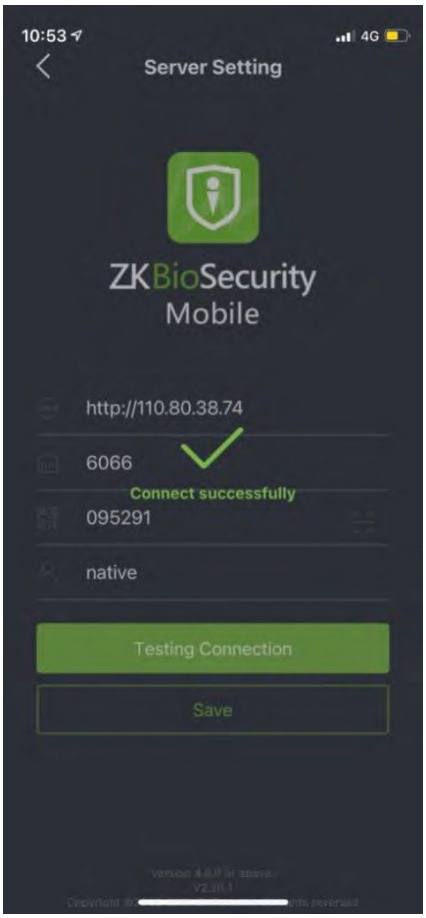




3. Abra o aplicativo no smartphone. Na tela de login, toque em **[Configuração do Servidor]** e digite o Endereço IP ou o Nome de Domínio do servidor, e sua Porta.

4. Toque no **ícone do QR Code** para escanear o QR Code do novo cliente do aplicativo. Após o cliente ser identificado com sucesso, defina o Nome do Cliente e toque em **[Teste de Conexão]**.

5. Após a conexão de rede ser estabelecida com sucesso, toque em **[Salvar]**.

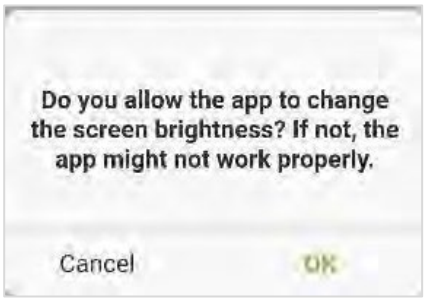


A função de Credencial Móvel só é válida ao fazer login como funcionário. Toque em "Funcionário" para alternar para a tela de login do funcionário. Insira o ID do funcionário e a senha (Padrão: 123456) para fazer login.

6. Toque em **[Credencial Móvel]** no aplicativo e um código QR será exibido, contendo as informações do ID do funcionário e o número do cartão (o código QR estático inclui apenas o número do cartão).

O código QR pode substituir um cartão físico em um dispositivo específico para realizar uma autenticação sem contato ao abrir a porta.

Ao usar esta função pela primeira vez, o aplicativo solicitará autorização para modificar as configurações de brilho da tela, conforme mostrado na figura:



O código QR é atualizado automaticamente a cada 30 segundos e também suporta atualização manual.

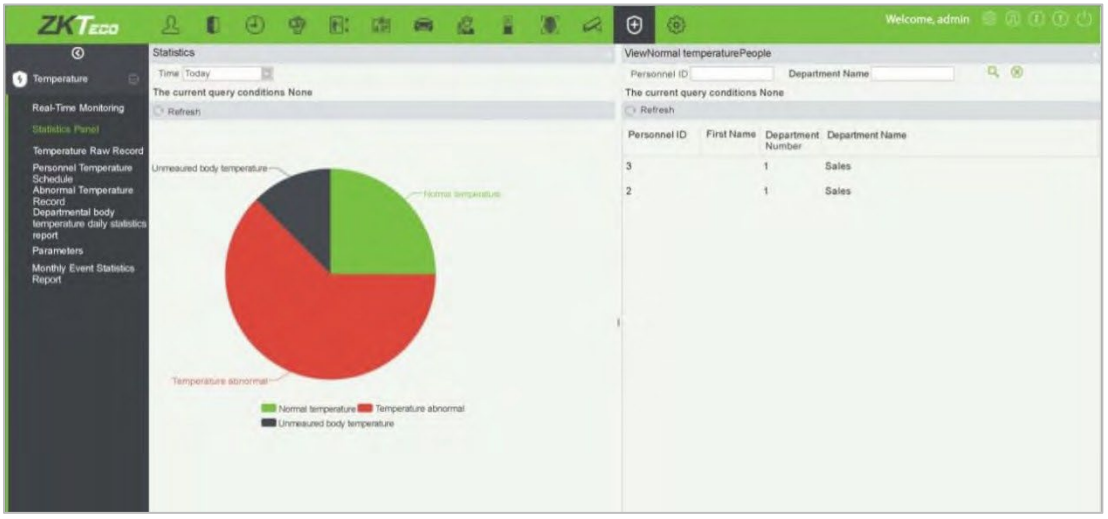
Observação: Para outras operações específicas, por favor, consulte o Manual do Usuário do Aplicativo Móvel ZKBioSecurity.

11.4 Monitoramento em tempo real no software ZKBioSecurity.

1. Clique em **Prevenção > Epidemia > Detecção de Temperatura > Monitoramento em tempo real** para visualizar todos os eventos das pessoas presentes nas categorias de Temperatura Anormal, Sem Máscaras e Registros Normais.

Os dados do usuário com temperatura corporal anormal são exibidos automaticamente na barra de informações de Temperatura Anormal de acordo com a configuração do Limite de Temperatura estabelecido.

2. Clique em **Epidemia > Gerenciamento de Temperatura > Painel de Estatísticas** para visualizar a análise dos dados estatísticos na forma de um gráfico de pizza e ver as pessoas com temperatura normal, temperatura anormal e temperatura não medida. Além disso, é possível ver informações detalhadas sobre a pessoa à direita, clicando na categoria específica no gráfico de pizza.

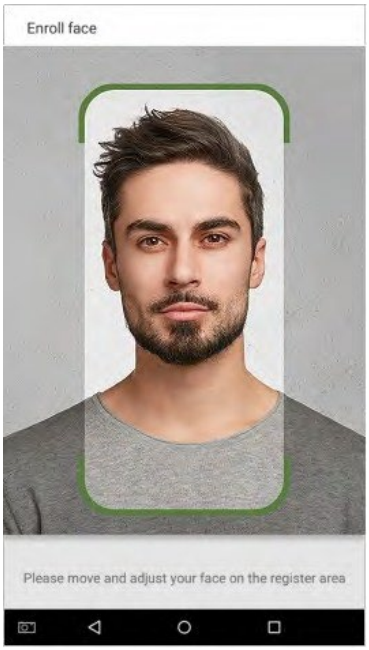


Observação: Para outras operações específicas, por favor, consulte o Manual do Usuário do ZKBioSecurity.

Apêndice 1

Requisitos para Cadastro no equipamento:

1) Recomenda-se realizar o cadastro em um ambiente interno com uma fonte de luz apropriada sem subexposição ou superexposição.
2) Não coloque o dispositivo em direção a fontes de luz externas, como portas ou janelas ou outras fontes de luz fortes.
3) Recomenda-se o manter sempre um bom contraste entre o tom de pele e a cor de fundo.
4) Exponha face e a testa adequadamente e não cubra a face e as sobrancelhas com o cabelo.
5) Recomenda-se mostrar uma expressão facial simples. (Um sorriso simples é aceitável, mas não feche os olhos ou incline a cabeça para qualquer orientação).
6) Duas imagens são necessárias para uma pessoa com óculos, uma imagem com óculos e outra sem os óculos.
7) Não use acessórios como cachecol ou máscara que possam cobrir a boca ou o queixo durante o cadastro.
8) Posicione a face na área de captura, conforme mostrado na imagem abaixo.
9) Não inclua mais de um face na área de captura.
10) Recomenda-se uma distância de 50 cm a 80 cm para capturar a imagem. (a distância é ajustável, dependendo da altura do corpo).



Requisitos para Upload de fotos no software

A foto deve ser reta, colorida, meio retratada com apenas uma pessoa e ela não deve possuir cadastro no sistema. As pessoas que usam óculos, devem permanecer de óculos para obter a captura foto via webcam ou upload da foto da pessoa usando óculos.

- **Distância dos olhos**

200 pixels ou mais são recomendados com não menos de 115 pixels de distância.

- **Expressão Facial**

Rosto neutro ou sorriso simples e olhos naturalmente abertos são recomendados.

- **Gesto e ângulo**

O ângulo de rotação horizontal não deve exceder ±10°, a elevação não deve exceder ±10° e o ângulo de depressão não deve exceder ±10°.

- **Acessórios**

Máscaras ou óculos coloridos não são permitidos durante o cadastro. A armação dos óculos não deve cobrir os olhos e não deve refletir a luz. Para pessoas com armação de óculos grossa, recomenda-se capturar duas imagens, uma com óculos e outra sem os óculos.

- **Face**

Rosto completo com contorno claro, escala real, luz uniformemente distribuída e sem sombra.

- **Formato de imagem**

Deve estar em BMP, JPG, ou JPEG.

- **Requisito de dados**

Deve seguir os requisitos:

1) Fundo branco com roupa de cor escura.
2) Modo de cor 24 bits.
3) Imagem compactada no formato JPG com tamanho não superior a 20kb.
4) A resolução deve estar entre 358 x 441 a 1080 x 1920.
5) A escala vertical da cabeça e do corpo deve estar na proporção de 2:1.
6) A foto deve incluir os ombros da pessoa capturada no mesmo nível horizontal.
7) Os olhos da pessoa capturada devem estar abertos e com a íris claramente visível.
8) Rosto ou sorriso simples são recomendados, sorriso excessivo mostrando os dentes não é recomendado.
9) A foto da pessoa capturada deve ser claramente visível, de cor natural, sem sombras fortes ou pontos de luz ou reflexos no rosto ou no fundo. O nível de contraste e luminosidade deve ser adequado.

Apêndice 2

Política de Privacidade

Aviso:

Para ajudá-lo(a) a utilizar melhor os produtos e serviços da ZKTeco (doravante referidos como "nós", "nosso" ou "nós"), um provedor de serviços inteligentes, coletamos consistentemente suas informações pessoais. Como entendemos a importância de suas informações pessoais, levamos sua privacidade a sério e formulamos esta política de privacidade para proteger suas informações pessoais. Listamos abaixo as políticas de privacidade para entender precisamente os dados e as medidas de proteção de privacidade relacionadas aos nossos produtos e serviços inteligentes.

Antes de utilizar nossos produtos e serviços, leia atentamente e entenda todas as regras e disposições desta Política de Privacidade. Se você não concordar com o contrato ou com qualquer um de seus termos, deverá parar de usar nossos produtos e serviços.

I. Informações coletadas

Para garantir o funcionamento normal do produto e ajudar na melhoria do serviço, coletaremos as informações fornecidas voluntariamente por você ou fornecidas conforme autorizado por você durante o registro e uso ou geradas como resultado do uso dos serviços.

1. **Informações de registro do usuário:** No seu primeiro registro, o modelo de recurso (Template de impressão digital/ de face/ de palma) será salvo no dispositivo de acordo com o tipo de dispositivo que você selecionou para verificar a semelhança exclusiva entre você e o ID do usuário que você tem registrado. Você pode opcionalmente inserir seu nome e código. As informações acima são necessárias para você usar nossos produtos. Se você não fornecer essas informações, não poderá usar alguns recursos do produto regularmente.
2. **Informações do produto:** De acordo com o modelo do produto e sua permissão concedida ao instalar e usar nossos serviços, as informações relacionadas ao produto no qual nossos serviços são usados serão coletadas quando o produto for conectado ao software, incluindo o modelo do produto, número da versão do firmware, número de série do produto e informações sobre a capacidade do produto. Ao conectar seu produto ao software, leia atentamente a política de privacidade do software específico.

II. Segurança e Gerenciamento do Produto

1. Ao usar nossos produtos pela primeira vez, você deve definir o privilégio de administrador antes de executar operações específicas. Caso contrário, você será frequentemente lembrado de definir o privilégio de administrador quando você entra na interface do menu principal. Se ainda não definir o privilégio de administrador após receber o prompt do sistema, você deve estar ciente do possível risco de segurança (por exemplo, os dados podem ser modificados manualmente).

2. Todas as funções de exibição de informações biométricas estão desativadas em nossos produtos por padrão. Você pode escolher Menu > Configurações do sistema para definir se deseja exibir as informações biométricas. Se você habilitar essas funções, assumimos que você está ciente dos riscos de segurança especificados na política de privacidade. 3. Apenas seu ID de usuário é exibido por padrão. Você pode definir se deseja exibir outras informações de verificação do usuário (como Nome, Departamento, Foto, etc.) sob o privilégio de Administrador.Todas as funções de exibição de informações biométricas estão desativadas em nossos produtos por padrão. Você pode escolher Menu > Configurações do sistema para definir se deseja exibir as informações biométricas. Se você habilitar essas funções, assumimos que você está ciente dos riscos de segurança especificados na política de privacidade.
3. Apenas seu ID de usuário é exibido por padrão. Você pode definir se deseja exibir outras informações de verificação do usuário (como Nome, Departamento, Foto, etc.) sob o privilégio de Administrador.
4. A função de câmera está desativada em nossos produtos por padrão. Se você deseja habilitar esta função para tirar fotos de si mesmo para registro de atendimento ou tirar fotos de estranhos para controle de acesso, o produto ativará o tom de alerta da câmera. Depois de habilitar esta função, presumimos que você esteja ciente dos possíveis riscos de segurança.
5. Todos os dados coletados por nossos produtos são criptografados usando o algoritmo AES 256. Todos os dados carregados pelo Administrador em nossos produtos são criptografados automaticamente usando o algoritmo AES 256 e armazenados com segurança. Se o administrador baixar dados de nossos produtos, presumimos que você precisa processar os dados e conhece o risco potencial de segurança. Nesse caso, você assumirá a responsabilidade pelo armazenamento dos dados. Você deve saber que alguns dados não podem ser baixados por questões de segurança de dados.
6. Todas as informações pessoais em nossos produtos podem ser consultadas, modificadas ou excluídas. Se você não usa mais nossos produtos, limpe seus dados pessoais.

III. Como tratamos informações pessoais de menores

Nossos produtos, site e serviços são principalmente projetados para adultos. Sem o consentimento dos pais ou responsáveis, os menores não devem criar sua própria conta. Se você é menor de idade, é recomendável que peça aos seus pais ou responsável para ler esta Política com atenção e só use nossos serviços ou informações fornecidas por nós com o consentimento dos seus pais ou responsável. Só usaremos ou divulgaremos informações pessoais de menores coletadas com o consentimento dos pais ou responsável se e na medida em que tal uso ou divulgação seja permitido por lei ou se tivermos obtido o consentimento explícito dos pais ou responsável, e tal uso ou divulgação for para a proteção de menores. Ao notar que coletamos informações pessoais de menores sem o consentimento prévio de pais verificáveis, excluiremos essas informações o mais rápido possível.

IV. Outros

Você pode visitar https://www.zkteco.com/cn/index/Index/privacy_protection.html para obter mais informações sobre como coletamos, usamos e armazenamos com segurança suas informações pessoais. Para acompanhar o rápido desenvolvimento da tecnologia, ajustar as operações comerciais e atender às necessidades dos clientes, iremos constantemente analisar e otimizar nossas medidas e políticas de proteção de privacidade. Fique à vontade para visitar nosso site oficial a qualquer momento para conhecer nossa política de privacidade mais recente.

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)	Mercury (Hg)	Cádmio (Cd)	Crómio hexavalente (Cr6+)	Bifenilos Polibromados (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.

NOTA: 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