Manual do Usuário

ProFace X (DS)

Data: Agosto de 2023

Versão do Documento: 1.0

Português

Obrigado por escolher o nosso produto. Por favor, leia atentamente as instruções antes da operação. Siga estas instruções para garantir que o produto esteja funcionando corretamente. As imagens mostradas neste manual são apenas para fins ilustrativos.

Para obter mais detalhes, por favor visite o site da nossa empresa http://www.zkteco.com.br.

Marca Registrada

ZKTeco é uma marca registrada da ZKTeco. Outras marcas comerciais envolvidas neste manual são propriedade 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 Rodovia MG-010, KM 26 - Loteamento 12 - Bairro
Angicos - Vespasiano - MG - CEP: 33.206-240.

Telefone +55 31 3055-3530
Para dúvidas relacionadas a negócios, escreva para nós em: comercial.brasil@zkteco.com
Para saber mais sobre nossas filiais globais, visite www.zkteco.com

Sobre a empresa

ZKTeco é um dos maiores fabricantes mundiais de leitores RFID e biométricos (impressões digitais, faciais, veias dos dedos). As ofertas de produtos incluem leitores e painéis de controle de acesso, câmeras de reconhecimento facial de alcance próximo e distante, controladores de acesso de elevador, catracas, controladores com reconhecimento de placa veicular (LPR) e produtos de consumo, incluindo fechaduras de impressão digital operadas por pilhas e leitores de face. Nossas soluções de segurança são multilíngues e disponibilizadas em mais de 18 idiomas diferentes. As instalações de fabricação ZKTeco são de última geração, com 700.000 pés quadrados e certificação ISO9001, controlamos a fabricação, o design do produto, a montagem dos componentes e a logística / transporte, tudo no mesmo local.

Os fundadores da ZKTeco foram determinados por pesquisa independente e desenvolvimento de procedimentos de verificação biométrica e a produção de SDK de verificação biométrica, que foi inicialmente e amplamente aplicado nos campos de segurança de PC e autenticação de identidade. Com o aprimoramento contínuo do desenvolvimento e muitos aplicativos de mercado, a equipe construiu gradualmente 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 soluções de verificações biométricas, a ZKTeco foi oficialmente estabelecida em 2007 e agora é uma das empresas líderes globais na indústria de soluções 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.

Padronização dos documentos

Os padrões usados neste manual estão listados abaixo:

Convenções de Interface Gráfica do Usuário:

Para Software	
Padrão	**Descrição**
Bold	Usado para identificar nomes de interface de software. Ex.: **OK**, **Confirmar**, **Cancelar**
>	Os menus de vários níveis são separados por esses colchetes. Ex.: Arquivo > Criar > Pasta.
Para Dispositivo	
Padrão	**Descrição**
< >	Nomes de botões ou chaves para dispositivos. Por exemplo, pressione <OK>
[ ]	Nomes de janelas, itens de menu, tabela 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 de encaminhamento. Por exemplo, [Arquivo / Criar / Pasta].

Símbolos

Padrão	Descrição
	Implica sobre o aviso ou para ter atenção, no manual
	Informações gerais que ajudam a realizar as operações mais rapidamente
	Informação que é significativa
	Cuidado para evitar perigos ou erros
	Declaração ou evento que avisa sobre algo ou que serve como um exemplo de advertência

Índice

1 Medidas de Segurança

As instruções abaixo têm a intenção de garantir que o usuário possa utilizar o produto corretamente para evitar perigos ou perdas de propriedade. As seguintes precauções visam manter os usuários seguros e prevenir qualquer dano. Por favor, leia atentamente antes da instalação.

⚠ O não cumprimento das instruções pode resultar em danos ao produto ou lesões físicas (podendo até mesmo causar a morte).

1. **Leia, siga e mantenha as instruções** - Todas as instruções de segurança e operação devem ser lidas e seguidas corretamente antes de colocar o dispositivo em funcionamento.
2. **Não ignore os avisos** - Adira a todos os avisos presentes no aparelho e nas instruções de operação.
3. **Acessórios** - Utilize apenas acessórios recomendados pelo fabricante ou vendidos com o produto. Por favor, não utilize outros componentes que não sejam os sugeridos pelo fabricante.
4. **Precauções para a instalação** - Não coloque este dispositivo em uma base ou suporte instável. Pode cair e causar lesões graves em pessoas e danos ao dispositivo.
5. **Serviço** - Não tente realizar o serviço deste aparelho por conta própria. Abrir ou remover capas pode expô-lo a voltagens perigosas ou outros riscos.
6. **Danos que necessitam de assistência -** Desconecte o sistema da fonte de energia CA ou CC e consulte pessoal de serviço nas seguintes condições:
   - Quando o cabo ou controle de conexão estiver afetado.
   - Quando líquidos forem derramados ou um objeto for inserido no sistema.
   - Se exposto à água ou devido a condições climáticas adversas (chuva, neve e similares).
   - Se exposto à água ou devido a condições climáticas adversas (chuva, neve e similares).

   Apenas altere os controles definidos nas instruções de operação. O ajuste inadequado dos controles pode resultar em danos e requerer a intervenção de um técnico qualificado para restaurar o funcionamento normal do dispositivo. E não conecte vários dispositivos a um único adaptador de energia, pois a sobrecarga do adaptador pode causar superaquecimento ou risco de incêndio.
7. **Peças de Reposição** - Quando forem necessárias peças de reposição, os técnicos de serviço devem usar somente peças de reposição fornecidas pelo fornecedor. Substituições não autorizadas podem resultar em queimaduras, choques elétricos ou outros riscos.
8. **Verificação de Segurança** - Ao concluir o serviço ou reparo no aparelho, peça ao técnico de serviço para realizar verificações de segurança a fim de garantir o funcionamento adequado do dispositivo.
9. **Fontes de** Energia - Opere o sistema apenas a partir da fonte de energia indicada na etiqueta. Se o tipo de adaptador CA a ser usado não estiver claro, entre em contato com o revendedor.
10. **Raios** - É possível instalar condutores externos de proteção contra raios para se precaver contra tempestades elétricas. Isso evita que descargas elétricas causem danos ao sistema. Recomenda-se instalar os dispositivos em áreas de acesso limitado.

Segurança Elétrica

- Antes de conectar um cabo externo ao dispositivo, realize o aterramento de maneira adequada e configure a proteção contra surtos; caso contrário, a eletricidade estática danificará a placa principal.
- Certifique-se de que a energia foi desconectada antes de realizar a fiação, instalação ou desmontagem do dispositivo.
- Garanta que o sinal conectado ao dispositivo seja um sinal de baixa corrente (interruptor); caso contrário, os componentes do dispositivo podem ser danificados.
- Assegure-se de que a voltagem padrão aplicável em seu país ou região seja utilizada. Se não tiver certeza sobre a voltagem padrão recomendada, consulte a sua empresa local de energia elétrica. A disparidade de energia pode causar curto-circuito ou danos ao dispositivo.
- Em caso de danos à fonte de energia, devolva o dispositivo a pessoal técnico profissional ou ao seu revendedor para resolução.
- Para evitar interferências, mantenha o dispositivo longe de dispositivos de alta radiação eletromagnética, como geradores (incluindo geradores elétricos), rádios, televisores (especialmente monitores de CRT) ou alto-falantes.

Segurança durante a Operação

- Se fumaça, odor ou ruído saírem do dispositivo, desligue imediatamente a energia e desconecte o cabo de alimentação e, em seguida, entre em contato com o centro de serviço.
- Transporte e outras causas imprevisíveis podem danificar o hardware do dispositivo. Verifique se o dispositivo possui danos intensos antes da instalação.
- Se o dispositivo apresentar defeitos graves que você não consegue resolver, entre em contato com o revendedor o mais rápido possível.
- Se o dispositivo apresentar defeitos graves que você não consegue resolver, entre em contato com o revendedor o mais rápido possível.
- Poeira, umidade e mudanças abruptas de temperatura podem afetar a vida útil do dispositivo. É aconselhável não manter o dispositivo sob tais condições.
- Não coloque o dispositivo em um local que vibra. Manuseie o dispositivo com cuidado. Não coloque objetos pesados em cima do dispositivo.

- Não aplique resina, álcool, benzeno, pesticidas e outras substâncias voláteis que possam danificar o invólucro do dispositivo. Limpe os acessórios do dispositivo com um pedaço de pano macio ou uma pequena quantidade de agente de limpeza.
- Se tiver alguma dúvida técnica sobre o uso, entre em contato com pessoal técnico certificado ou experiente.

Observação:

- Certifique-se se a polaridade positiva e negativa do adaptador CA de 12V CC está conectada corretamente. Uma conexão reversa pode danificar o dispositivo. Não é aconselhável conectar o adaptador CA de 24V à porta de entrada de CC de 12V.
- Certifique-se de conectar os fios seguindo a polaridade positiva e negativa indicada na placa de identificação do dispositivo.
- O serviço de garantia não cobre danos acidentais, danos causados por mau funcionamento e danos devido a instalação ou reparo independentes do produto pelo usuário.

2 Visão Geral

O ProFace X(DS) é uma versão recém-projetada da linha de produtos ProFace, desenvolvida para lidar com uma ampla gama de cenários. As tecnologias de Reconhecimento Facial de Dual Spectrum, Luz Escura e Luz Extremamente Forte (100.000 lux) permitem que o terminal reconheça faces em ambientes de luz extremamente forte e baixa luminosidade sem a necessidade de um flash LED, melhorando significativamente a experiência e a precisão do reconhecimento facial.

O ProFace X(DS) é alimentado pela CPU personalizada da ZKTeco, que executa um algoritmo de reconhecimento facial de engenharia intelectualizada e a mais recente tecnologia de visão computacional. Ele suporta verificação facial com grande capacidade e velocidade de reconhecimento rápida, além de suportar câmera facial com QR code via aplicativo móvel, aprimorando o desempenho de segurança em todos os aspectos.

Ele também contribui para a eliminação de preocupações com higiene, devido à sua tecnologia de reconhecimento sem contato, bem como novas capacidades, como identificação de pessoas usando máscara e detecção de máscara.

Características

- O Reconhecimento Facial em Luz Visível e o Reconhecimento Facial em Infravermelho Próximo são ambos suportados pela tecnologia de espectro duplo.
- Reconhecimento Facial em Luz Escura sem Flash LED
- Capacidade ultra grande de modelo facial; 1:N - 30.000 modelos faciais (padrão), 1:N - 50.000 modelos faciais (máximo) (opcional)
- Reconhecimento facial rápido em 0,35 segundos
- Algoritmo anti-fraude contra ataques de impressão (laser, fotos coloridas e em preto e branco), vídeo e máscaras 3D
- Padrão de proteção IP68 à prova de poeira e água e padrão de proteção IK04
- Câmera com sensor CMOS de 2MP com tecnologia "starlight" e função WDR, que permite ao terminal reconhecer rostos sob condições extremas de iluminação (0 a 100.000 lux)
- Detecção de máscara e verificação facial estão disponíveis ao usar máscaras.
- Suporta QR code estático e QR code dinâmico (opcional)
- Existem dois tipos de módulos de cartão disponíveis: cartão EM de 12,5 kHz e cartão IC de 13,56MHz (opcional)

Observação:

1) A FAR (Taxa de Falsas Aceitações) será aumentada pelo reconhecimento facial para pessoas de máscara.
2) O ProFace X (DS) vem de fábrica com hardware de intensidade de luz de 100.000 lux e suporta hardware opcional de intensidade de luz de 50.000 lux.

Especificações

Capacidade	Faces	30.000 (1: N) 50.000 (Opcional)
	Usuários / Cartões	50,000
	Transações	1.000.000 2.000.000 (Opcional)
	Fotos de Usuários	10.000
	Fotos de eventos	7.500
Compatibilidade	Caixa de Relé de Segurança, Leitor Escravo Wiegand/RS485 com Impressão Digital/RFID Impressora Externa RS232 Software ZKBio CVSecurity	
Funções Padrão	Níveis de Acesso, Grupos, Feriados, Horário de Verão, Modo de Coação (Senha), Anti-Passback, Consulta de Registros, Papel de Parede Personalizado, Protetor de Tela e Alarme de Interruptor de Violação	
Hardware	CPU Quad-core ARM Cortex-A7@ 1,2GHz, 1GB de RAM/8GB de Flash Tela de Toque LCD de 8" de Alto Brilho 125KHz EM/13.56MHz MF (Opcional) Câmera WDR de Baixa Luminosidade de 2MP, LED Ajustável de Brilho de Luz Voz Hi-Fi Sensibilidade do Receptor de Microfone Botão de Reset e Interruptor de Violação	
Interface de Controle de Acesso	Saída de Relé de Trava Saída de Alarme/Entrada Auxiliar Botão de Saída/Sensor de Porta	

Funções Especiais	IP68 e IK04 (Nível Opcional IK10) Verificação de Face em 0,3s Detecção de Rosto em Tempo Real Criptografia Https Opcional Snapshot de Evento
Comunicação	TCP/IP Entrada / Saída Wiegand Wi-Fi (Opcional) RS485/RS232
Informações Adicionais	Algoritmo Facial: ZKLiveFace5.95 Temperatura Operacional: -20°C a 55°C Umidade Operacional: ≤90% Temperatura de Armazenamento: -25°C a +65°C Umidade de Armazenamento: ≤93% Dimensões (ALP): 227 x 143 x 26mm
Alimentação	Tensão de Operação: 12V DC Consumo de Corrente: < 3.000mA

3 Instruções de Uso

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

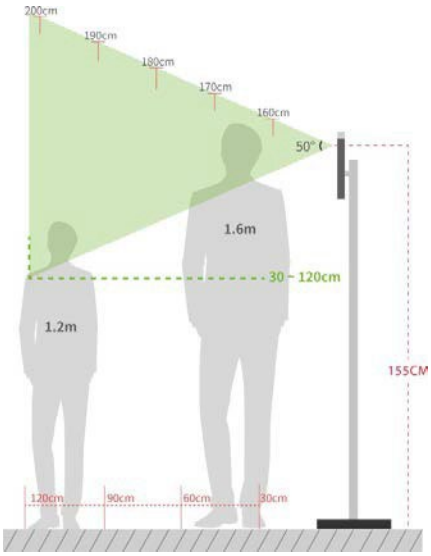
3.1 Como escanear o QR code?

Abra o aplicativo ZKBioSecurity, vá para o "Credenciamento Móvel" e alinhe a tela do telefone com o leitor de QR Code no dispositivo.

Observação: Coloque o seu telefone a uma distância de 15 a 50 cm do dispositivo (a distância varia dependendo do tamanho da tela do telefone) e evite bloquear o leitor de código QR do dispositivo e o código QR na tela do telefone.

3.2 Posição em Pé, Postura e Expressão Facial

- **A distância recomendada**



Recomenda-se que a distância entre o dispositivo e um usuário cuja altura esteja entre 1,55 m e 1,85 m seja de 0,3m a 2,5m. Os usuários podem se aproximar ou se afastar um pouco para melhorar a qualidade das imagens faciais capturadas.

- **Postura em pé e expressão facial recomendadas**

Postura em pé **Expressão Facial**

Observação: Mantenha sua expressão facial e postura natural durante o cadastro ou autenticação.

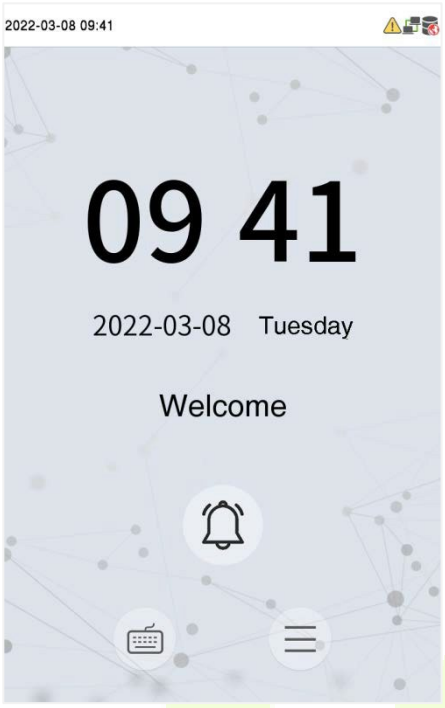
3.3 Cadastro de Face

Tente manter a face no centro da tela durante o cadastro. Olhe para a câmera e fique parado durante o cadastro da face. A tela deve ficar assim:

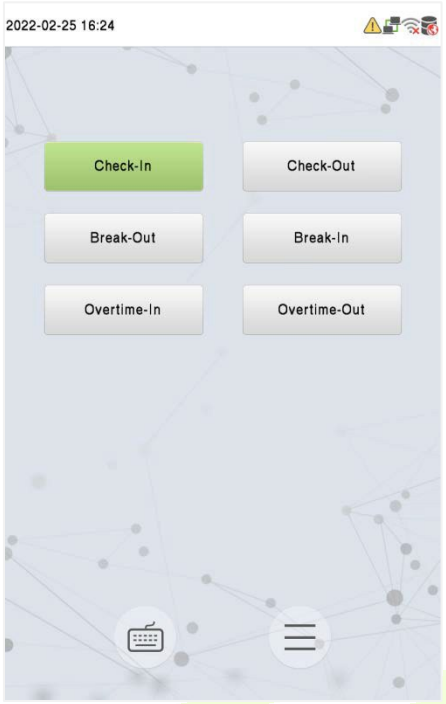
- **Modo correto de cadastro de face e método de autenticação**
  - Ao cadastrar uma face, mantenha uma distância de 40 cm a 80 cm entre o dispositivo e a face.
  - Tenha cuidado para não mudar sua expressão facial. (Ex.: sorriso, etc.)
  - Se você não seguir as instruções na tela, o cadastro de face pode demorar mais ou pode falhar.
  - Tenha cuidado para não cobrir os olhos ou as sobrancelhas.
  - Não use chapéus, bonés, máscaras, óculos de sol.
  - Tenha cuidado para não exibir duas faces na tela. Cadastre uma pessoa por vez.
  - Recomenda-se que usuários que usem óculos registrem tanto o rosto com óculos quanto o rosto sem óculos.
- **Recomendação para autenticar uma face**
  - Certifique-se de que a face apareça dentro da guia exibida na tela do dispositivo.
  - Se os óculos foram trocados, a autenticação pode falhar. Se a face sem óculos tiver sido cadastrada, autentique sem óculos. Se a face com óculos foi cadastrada, autentique com os óculos.
  - Se uma parte do rosto estiver coberta com um chapéu, boné, máscara, tapa-olho ou óculos de sol, a autenticação pode falhar. Não cubra a face, permita que o dispositivo veja as sobrancelhas e a face.

3.4 Tela principal

Após conectar a fonte de alimentação, a seguinte tela será exibida:



- Clique em para autenticar com ID do usuário.
- Quando não houver um super administrador cadastrado no dispositivo, clique em para ir ao menu
- Os visitantes tocam para fazer uma chamada e o telefone irá tocar.
- Após instalar o Super Administrador no dispositivo, ele deve ser verificado pelo Super Administrador antes de usar as funções do menu.
- As opções de status de registro também podem ser exibidas e usadas diretamente na interface de espera. Clique em qualquer lugar da tela, exceto nos ícones, e seis teclas de atalho aparecerão na tela, conforme mostrado na figura abaixo:

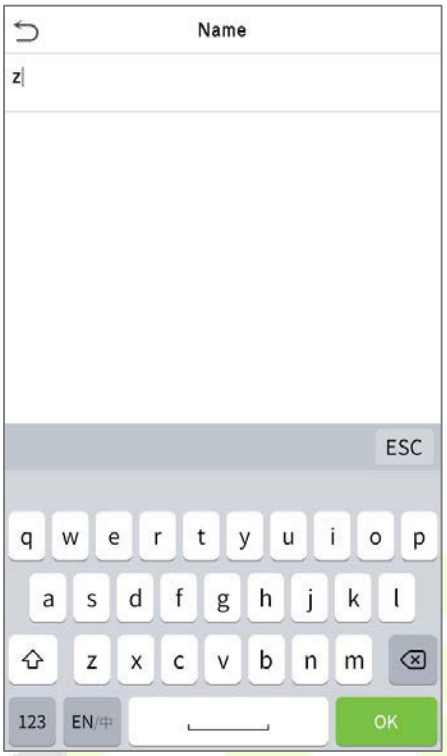


- Pressione a tecla correspondente ao estado de registro para selecionar o seu estado de registro atual, que é exibido em verde.

Observação:

1) Para a segurança do dispositivo, é recomendado registrar um super administrador na primeira vez que você utilizar o dispositivo.
2) As opções de estado de registro estão desligadas por padrão e devem ser configuradas para outra opção em "9.4 Opções de Estados de Registro" para que apareçam na tela de espera.

3.5 Teclado Virtual



Observação:

O dispositivo suporta a entrada em chinês, inglês, números e símbolos.

1) Clique em [En] para alternar para o teclado em inglês.
2) Pressione [123] para alternar para o teclado numérico e simbólico.
3) Clique em [ABC] para retornar ao teclado alfabético.
4) Clique na caixa de entrada para o teclado virtual ser exibido.
5) Clique em [ESC] para sair do teclado virtual

3.6 Modo de autenticação

3.6.1 Autenticação de QRCode

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

No aplicativo ZKBioSecurity, toque em [Credencial Móvel], e um código QR com o ID do funcionário e detalhes do número do cartão (o código QR estático inclui apenas o número do cartão) será exibido. Para realizar autenticação sem contato, um QR Code pode ser usado para substituir um cartão físico em um dispositivo específico.

3.6.2 Autenticação Facial

- **Autenticação facial 1:N (um para muitos)**

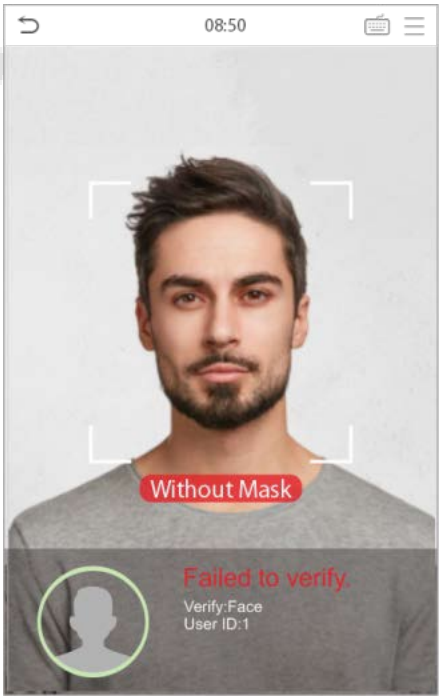
1. **Autenticação Convencional**

Nesse modo de verificação, o dispositivo compara as imagens faciais obtidas com todos os dados faciais do dispositivo. A seguir está o aviso pop-up para um resultado de comparação bem-sucedido.

2. Habilitar Detecção de Máscara

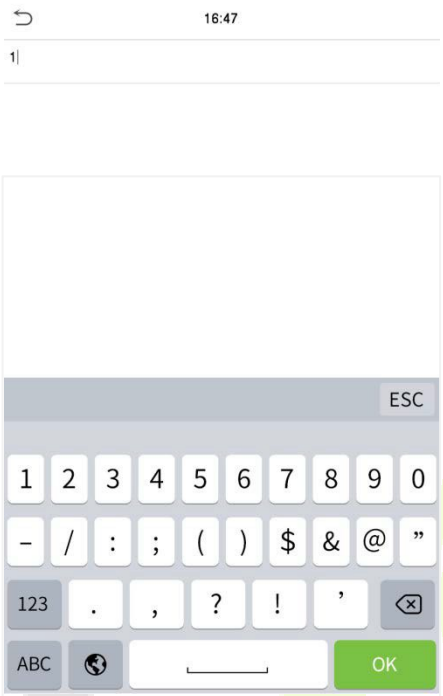
Quando o usuário habilita a função de Detecção de Máscara, o dispositivo identifica se o usuário está usando uma máscara durante a verificação ou não. As janelas pop-up da interface de resultado de comparação são listadas abaixo:

.

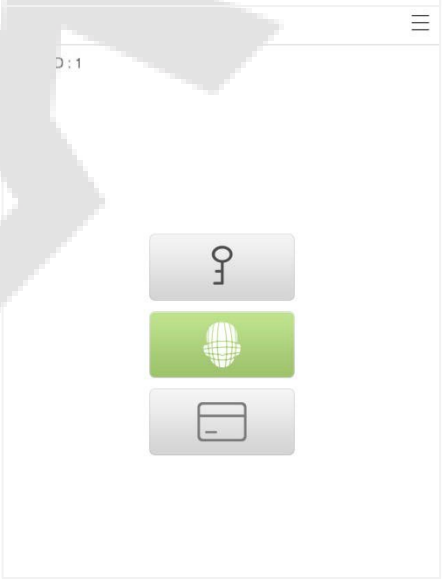


- **Autenticação facial 1:1**

Nesse modo de verificação, o dispositivo compara o rosto capturado pela câmera com o modelo facial associado ao ID do usuário inserido. Toque em e [OK] na interface principal após entrar no modo de verificação facial 1:1 e inserir o ID do usuário.



Se o usuário tiver registrado um cartão e senha além do rosto, e o método de verificação estiver configurado para verificação de Cartão/Senha/Rosto, a seguinte tela aparecerá. Selecione o ícone para entrar no modo de verificação facial.



Após a verificação bem-sucedida, a caixa de diálogo exibe **Verificação bem-sucedida**, como mostrado abaixo:

Se a verificação falhar, será exibida a mensagem "**Por favor, ajuste sua posição!**".

3.6.3 Autenticação de múltiplas faces

- **Autenticação 1: N**

1. **Verificação convencional**

Nesse modo de verificação, o dispositivo compara as imagens faciais obtidas de várias pessoas com todos os dados faciais armazenados nele. Ao mesmo tempo, o dispositivo pode verificar até quatro pessoas. O número de resultados de verificação exibidos no lado direito pode ser personalizado. A imagem abaixo ilustra o aviso de pop-up para um resultado de comparação bem-sucedido.

Toque em **Sistema > Rosto > Configurações de Identificação de Rosto > Modo de Identificação > Identificação de Múltiplos Rostos > Contagem a Exibir** para definir o número de resultados de verificação a serem exibidos.

Observação: A **Contagem a Exibir** pode ser definida entre 1 e 4.

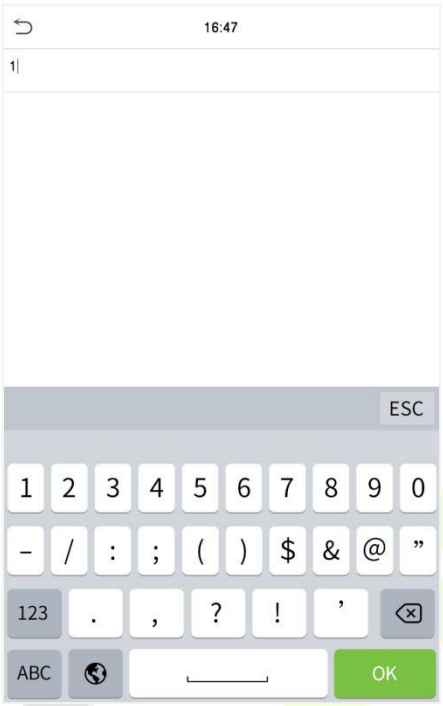
2. Habilitar Detecção de Máscara

Quando o usuário habilita a função de Detecção de Máscara, o dispositivo identifica se o usuário está usando uma máscara durante a verificação ou não. A seguir estão os pop-ups da interface de aviso de resultado de comparação.

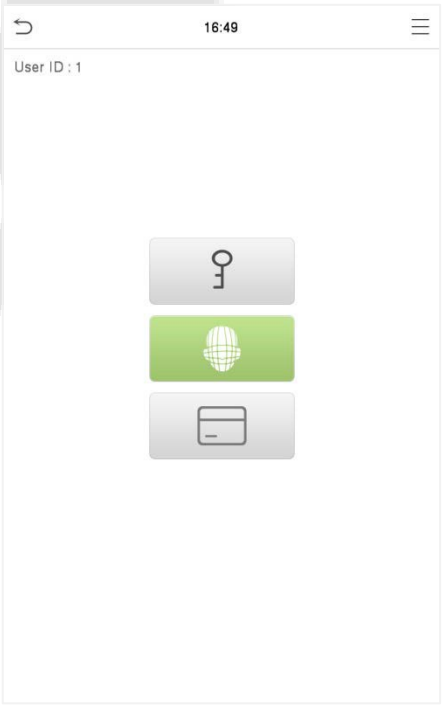
Observação: Não usar máscara é exibido como o ícone

- **Autenticação 1:1**

Nesse modo de verificação, o dispositivo compara o rosto capturado pela câmera com o modelo facial associado ao ID do usuário inserido. Pressione na interface principal, selecione o modo de verificação facial 1:1 e insira o ID do usuário e toque em [**OK**].



Se o usuário tiver registrado um cartão e senha, além do rosto, e o método de verificação estiver configurado para verificação de Cartão/Senha/Rosto, a seguinte tela aparecerá. Selecione o ícone para entrar no modo de verificação facial.

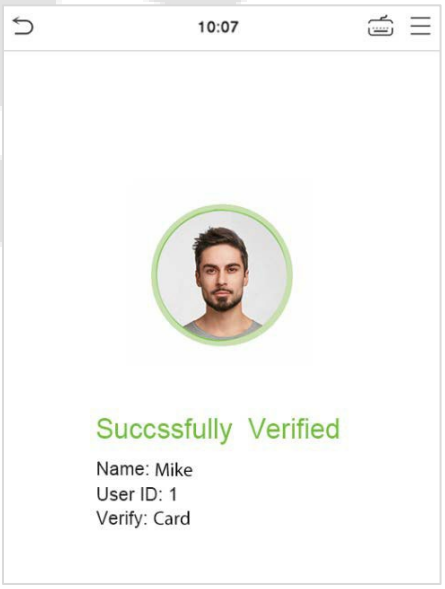


Após a verificação bem-sucedida, a caixa de diálogo exibirá o resultado da verificação, como mostrado na figura abaixo:

3.6.4 Autenticação de cartão

- **Autenticação de cartão 1:N**

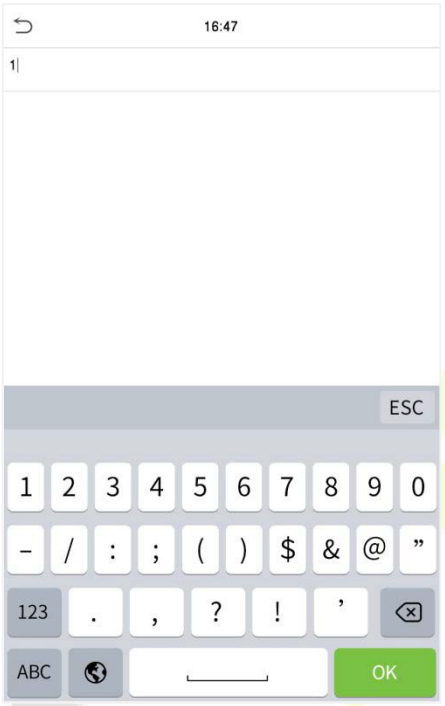
O modo de Verificação de Cartão 1: N compara o número do cartão na área de indução de cartão com todos os dados de número de cartão registrados no dispositivo. A seguir está a tela de verificação de cartão.



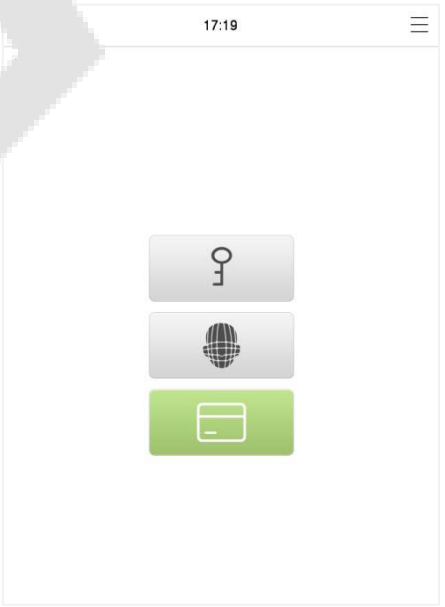
- **Verificação de Cartão 1:1**

O modo de Verificação de Cartão 1:1 compara o número do cartão na área de indução de cartão com o número associado ao ID do usuário do funcionário registrado no dispositivo.

Pressione na interface principal para abrir o modo de verificação de cartão 1:1. Insira o ID do usuário e clique em **[OK]**.



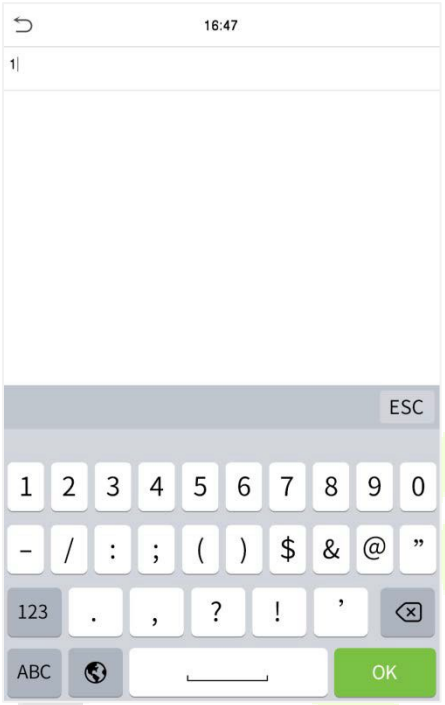
Se o usuário tiver registrado rosto e senha, além do cartão, e o método de verificação estiver configurado para verificação de Cartão/Senha/Rosto, a seguinte tela aparecerá. Selecione o ícone para entrar no modo de verificação de cartão.



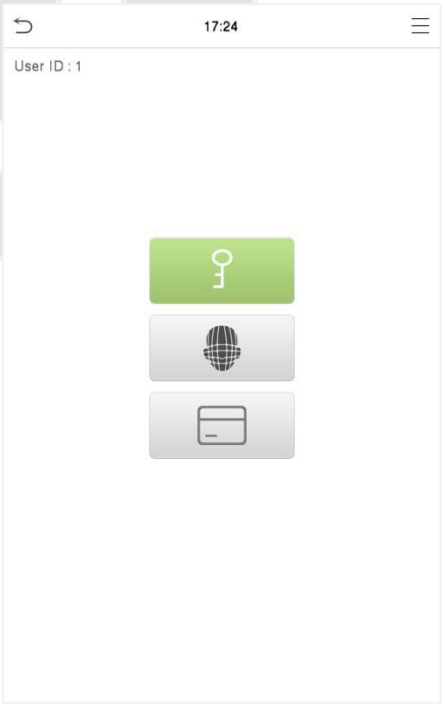
3.6.5 Autenticação de senha

O dispositivo compara a senha inserida com a senha registrada para o ID de usuário fornecido.

Toque o botão na tela principal para entrar no modo de verificação de senha 1:1. Em seguida, insira o ID do usuário e pressione **[OK]**.

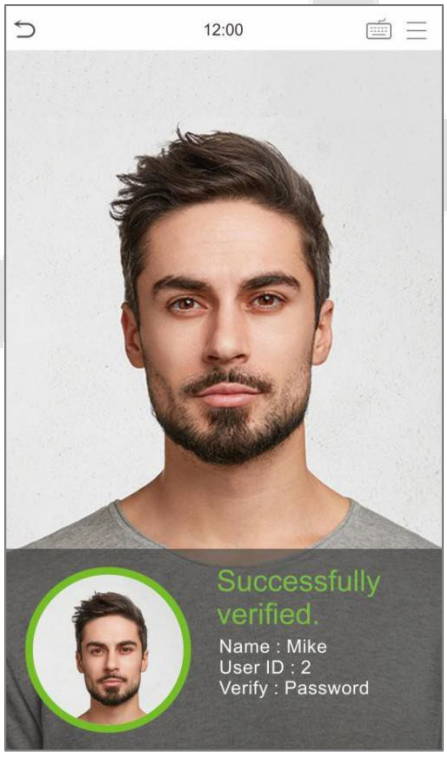


Se o usuário tiver registrado rosto e cartão, além de uma senha, e o método de verificação estiver configurado para verificação de Cartão/Senha/Rosto, a seguinte tela aparecerá. Selecione o ícone para entrar no modo de verificação de senha.

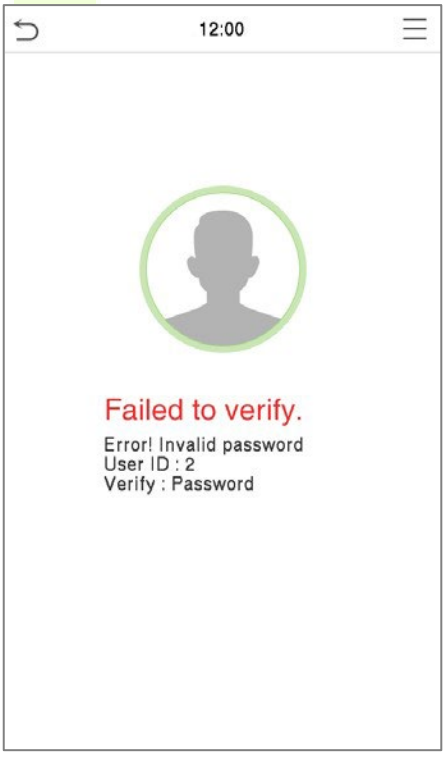


Digite a senha e pressione **[OK].**

Abaixo estão as telas de exibição após inserir uma senha correta e uma senha incorreta, respectivamente.



Autenticação bem sucedida



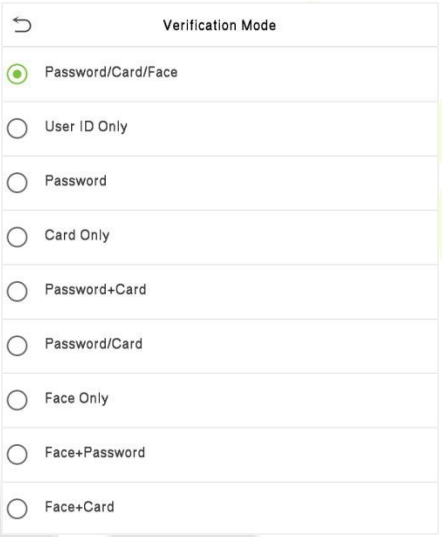
Falha na autenticação

3.6.6 Verificação Combinada

Este dispositivo permite que você utilize diversos métodos de verificação para aumentar a segurança. Existem um total de 9 combinações distintas de verificação que podem ser implementadas, conforme listado abaixo:

Definição dos Símbolos de Verificação Combinada

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 Verificação Combinada

- A verificação combinada requer que os funcionários registrem todos os diferentes métodos de verificação. Caso contrário, os funcionários não conseguirão completar com sucesso o processo de verificação combinada.
- Por exemplo, quando um funcionário registra apenas os dados faciais, mas o modo de verificação do Dispositivo está configurado como "Rosto + Senha", o funcionário não conseguirá completar com sucesso o processo de verificação.
- Isso ocorre porque o Dispositivo compara o modelo de rosto da pessoa com o modelo de verificação registrado (tanto o Rosto quanto a Senha) previamente armazenado para aquele ID de Pessoa no Dispositivo.
- Mas, como o funcionário registrou apenas o Rosto e não a Senha, a verificação não será concluída e o Dispositivo exibirá "Verificação Falhou".

4 Menu Principal

Pressione na interface de espera para entrar no **Menu Principal** e a seguinte tela será exibida:

Descrição da função

Menu	Descrição
Usuário Adm.	Para adicionar, editar, visualizar e excluir informações básicas de um usuário.
Priv. Usuário	Para definir o escopo de permissão da função personalizada e de cadastrador para os usuários, ou seja, os direitos para utilizar o sistema.
Conf. Com.	Para definir os parâmetros de rede, comunicação serial, conexão de PC, rede sem fio, servidor de nuvem, Wiegand e diagnóstico de rede.
Sistema	To set parameters related to the system, including Date & Time, Access Logs Setting, Face, Detection and Temperature Management, Device Type and Security Setting, and Reset.
Personalização	Isso inclui configurações de Interface do Usuário, Voz, Horários, Status de Registro e Teclas de Atalho.
Ger. Dados	Para deletar todos os dados relevantes no dispositivo.
Controle Acesso	Para configurar parâmetros relacionados ao sistema, incluindo Data e Hora, Configuração de Registros de Acesso, Rosto, Detecção e Gerenciamento de Temperatura, Tipo de Dispositivo e Configuração de Segurança, e Redefinição.
Busca de Frequência	Para consultar os logs, verificar fotos de frequência e fotos de frequência da lista de bloqueio.
Imprimir	Para configurar informações e funções de impressão (se a impressora estiver conectada ao dispositivo).
Autoteste	Para testar automaticamente se cada módulo funciona corretamente, incluindo a Tela LCD, Áudio, Câmera e Relógio em Tempo Real.
Informações do Sistema	Para visualizar a capacidade de dados, as informações do dispositivo e do firmware do dispositivo atual.

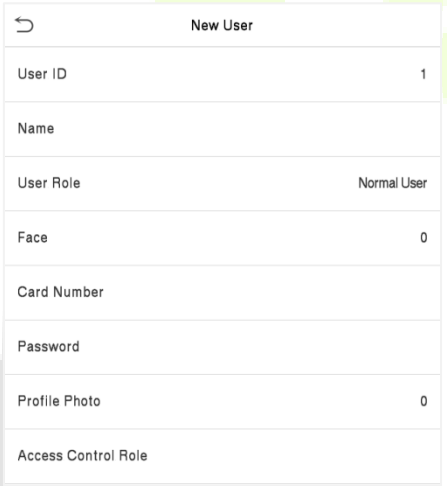
5 Gerenciamento de Usuários

5.1 Registro de Usuário.

Toque em **Gerenciamento de Usuários** no menu principal.

5.1.1 ID do Usuário e Nome

Toque em Novo Usuário e insira o ID de Usuário e o Nome.



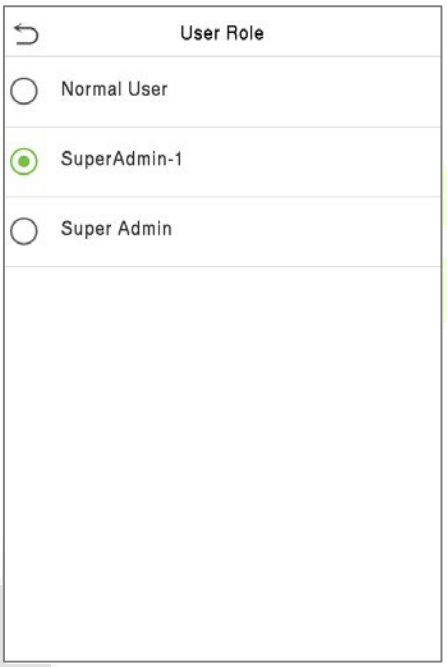
Observação:

1) Um nome pode ter até 34 caracteres.
2) O ID do usuário pode conter de 1 a 14 dígitos por padrão, suporta números e letras.
3) Durante o registro inicial, você pode modificar seu ID, mas não após o registro.
4) Se a mensagem "**Duplicado**!" aparecer, você deve escolher um ID de usuário diferente, pois o que você digitou já existe.

5.1.2 Privilégio do Usuário

Na interface de Novo Usuário, toque em Função do Usuário para definir a função do usuário como Usuário Normal ou Super Administrador.

- **Super Administrador:** O Super Administrador possui todos os privilégios de gerenciamento no Dispositivo.
- **Usuário Normal:** Se o Super Administrador já estiver registrado no dispositivo, os Usuários Normais não terão o privilégio de gerenciar o sistema e só poderão acessar verificações autênticas.
- **Funções Definidas pelo Usuário:** O Usuário Normal também pode ser atribuído a funções personalizadas com a Função Definida pelo Usuário. O usuário pode ser autorizado a acessar várias opções de menu conforme necessário.

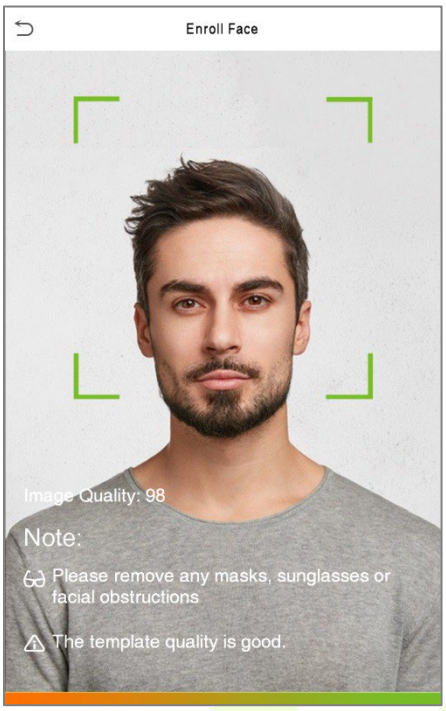


Observação: Se a função de usuário selecionada for a de Super Administrador, o usuário deverá passar pela autenticação de identidade para acessar o menu principal. A autenticação é baseada no(s) método(s) de autenticação que o super administrador registrou.

5.1.3 Face

Toque em **Face** na interface de **Novo Usuário** para acessar a página de registro de face.

- Por favor, vire-se para a câmera e posicione-se de modo que a imagem do seu rosto se encaixe dentro da caixa guia branca e permaneça imóvel durante o registro do rosto.
- Uma barra de progresso aparece durante o registro do rosto e, em seguida, a mensagem "Registrado com Sucesso" é exibida quando a barra de progresso é concluída.
- Se a face já estiver registrada, a mensagem "Face Duplicada" aparecerá. A interface de registro é a seguinte:

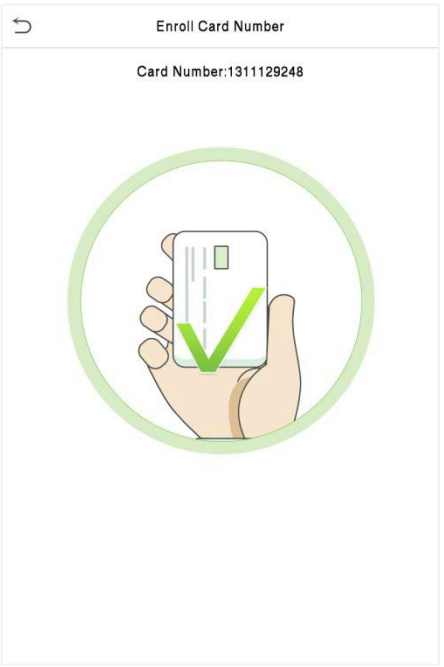


5.1.4 Cartão

- **Cadastrar Cartão**

Toque em **Cartão** na interface de **Novo Usuário** para entrar na página de registro de cartão.

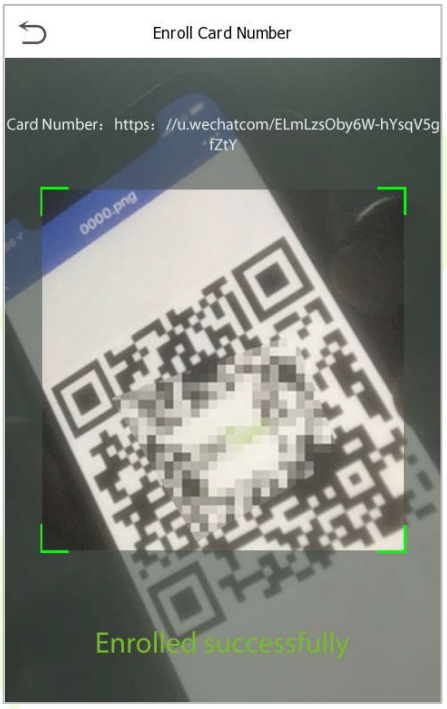
- Passe o cartão na área de leitura de cartões na interface de Cartão. O registro do cartão será bem-sucedido.
- Se o cartão já estiver registrado, a mensagem "Erro! Cartão já registrado" aparecerá. A interface de registro será semelhante a esta:



- **Registrar Código QR de Cartão**

Toque em Cartão na interface de Novo Usuário para acessar a página de registro de cartão.

- Na interface de Cartão, mostre o código QR na frente da câmera. O registro do código QR será bem-sucedido.
- Se o código QR já estiver registrado, a mensagem "Erro! Cartão já registrado" aparecerá. A interface de registro será semelhante a esta:



5.1.5 Senha

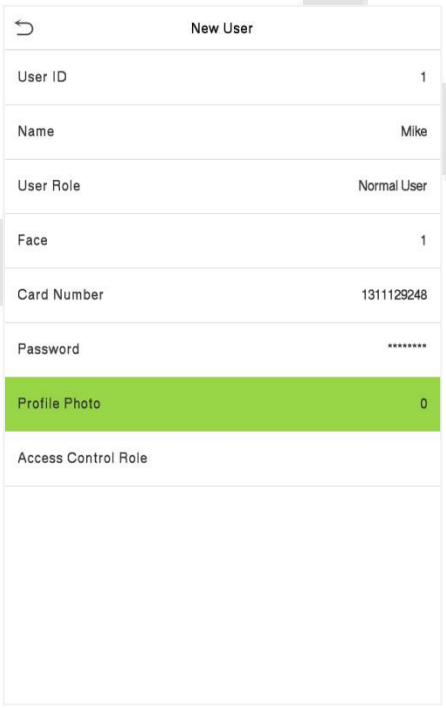
Toque em **Senha** na interface de **Novo Usuário** para acessar a página de registro de senha.

- Na interface de Senha, insira a senha necessária e digite novamente para confirmá-la. Depois, toque em **OK.**
- Se a senha digitada novamente for diferente da senha inserida inicialmente, o dispositivo exibirá a mensagem "Senha não coincide!" e o usuário precisará confirmar a senha novamente.

Observação: A senha pode conter de 1 a 8 dígitos por padrão.

5.1.6 Foto de Perfil

Toque em **Foto de Perfil** na interface de **Novo Usuário** para acessar a página de registro de Foto de Perfil.



- Quando um usuário registrado com uma foto é autenticado com sucesso, a foto registrada do usuário é exibida.
- Para tirar uma foto, toque em Foto de Perfil para abrir a câmera do dispositivo e, em seguida, toque no ícone da câmera. A foto capturada é exibida no canto superior esquerdo da tela e a câmera é aberta novamente para tirar outra foto, após a captura da foto inicial.

Observação: Ao registrar um rosto, o sistema captura automaticamente uma imagem como uma foto de perfil. Se você não tiver uma foto de perfil registrada, o sistema define automaticamente a imagem capturada durante o registro como a foto padrão.

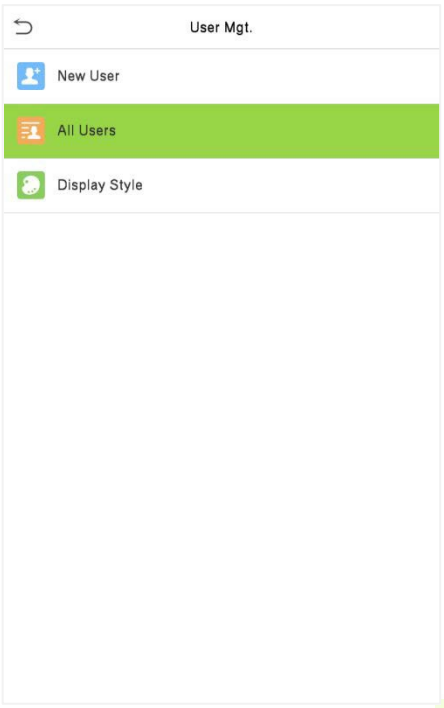
5.1.7 Função de Controle de Acesso

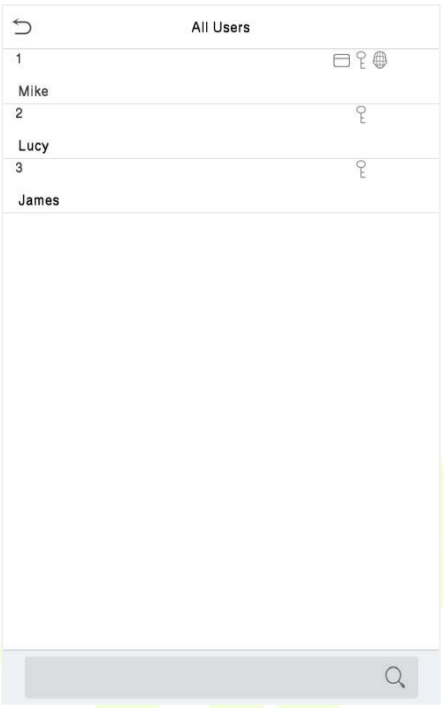
A Função de Controle de Acesso define os privilégios de acesso à porta para cada usuário. Isso inclui o grupo de acesso, o modo de verificação e facilita a configuração do período de tempo de acesso do grupo.

- Toque em **Função de Controle de Acesso > Grupo de Acesso** para atribuir os usuários registrados a diferentes grupos para um melhor gerenciamento. Novos usuários pertencem ao Grupo 1 por padrão e podem ser reatribuídos a outros grupos. O dispositivo suporta até 99 grupos de controle de acesso.
- Toque em **Período de Tempo** para selecionar o horário de uso.

5.2 Pesquisar Usuário

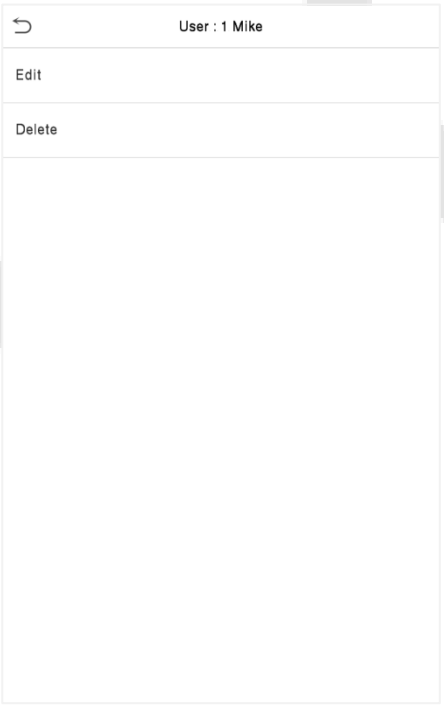
- No **Menu Principal**, toque em **Gerenciamento de Usuário** e, em seguida, toque em **Todos os Usuários** para pesquisar um usuário.
- Na interface **Todos os Usuários**, toque na barra de pesquisa na lista de usuários para inserir a palavra-chave de busca necessária (onde a palavra-chave pode ser o ID do usuário, sobrenome ou nome completo) e o sistema irá buscar as informações do usuário relacionado.

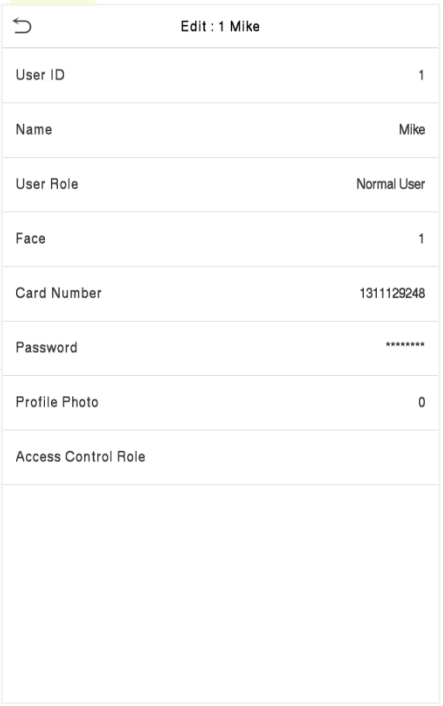




5.3 Editar Usuário

Na interface **Todos os Usuários**, toque no usuário necessário da lista e depois toque em **Editar** para editar as informações do usuário.





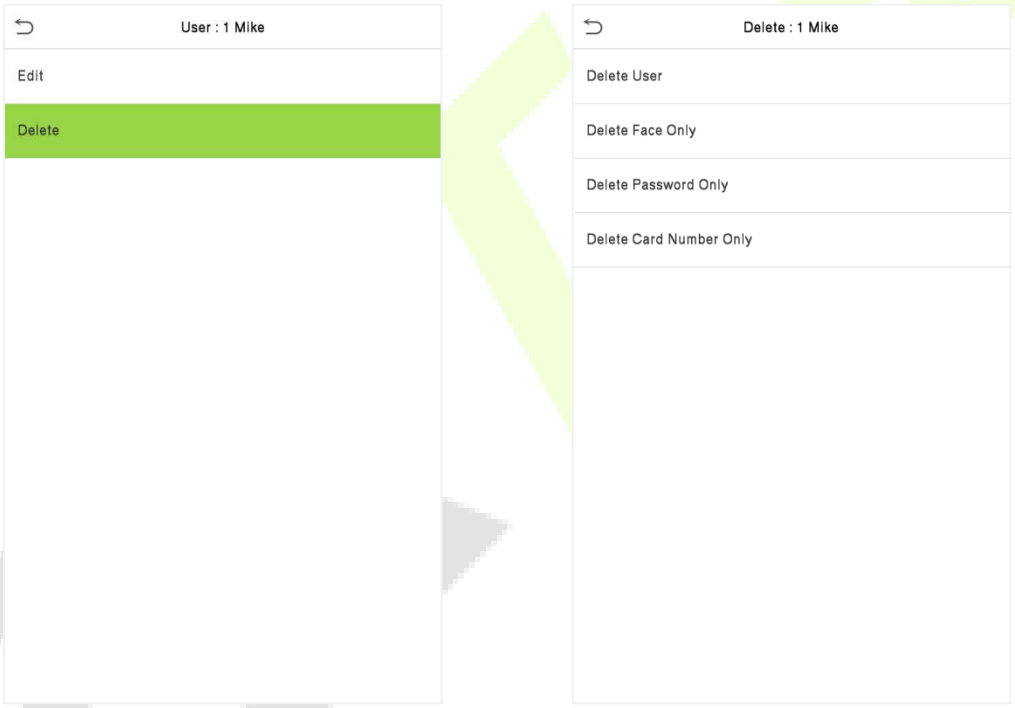
Observação: O processo de edição das informações do usuário é o mesmo que adicionar um novo usuário, exceto que o ID do usuário não pode ser modificado durante a edição de um usuário. O processo detalhado está descrito em "5.1 Registro de Usuário".

5.4 Excluir Usuário

Na interface **Todos os Usuários**, toque no usuário necessário da lista e depois toque em **Excluir** para deletar o usuário ou informações específicas do usuário do dispositivo. Na interface **Excluir**, toque na operação necessária e depois toque em **OK** para confirmar a exclusão.

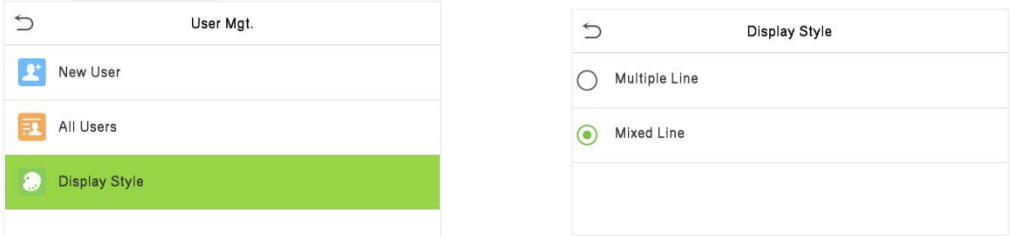
Operações de Exclusão

- **Excluir Usuário:** Deleta todas as informações do usuário (deleta o usuário selecionado como um todo) do Dispositivo.
- **Excluir apenas face:** Deleta as informações de face do usuário selecionado.
- **Excluir Apenas Senha:** Deleta as informações de senha do usuário selecionado.
- **Excluir Apenas Número do Cartão:** Deleta as informações do cartão do usuário selecionado.

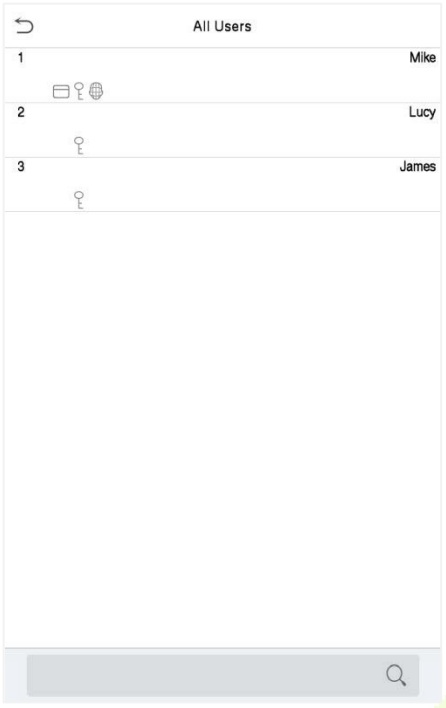


5.5 Estilo de Exibição

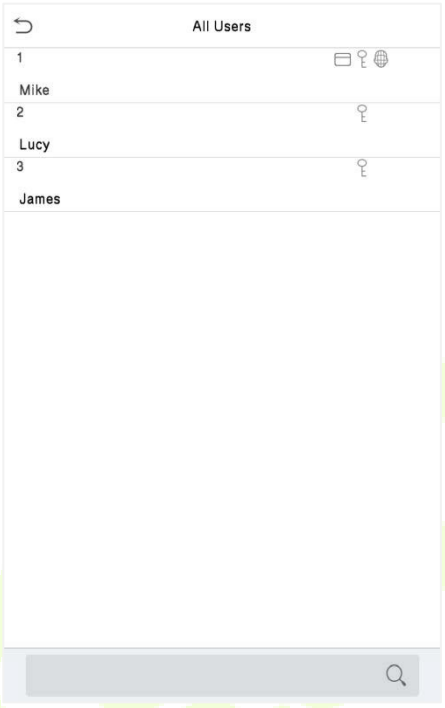
No **Menu Principal**, toque em **Gerenciamento de Usuário** e, em seguida, toque em **Estilo de Exibição** para acessar a interface de configuração do **Estilo de Exibição**.



Todos os Estilos de Exibição são mostrados como abaixo:



Múltiplas Linhas

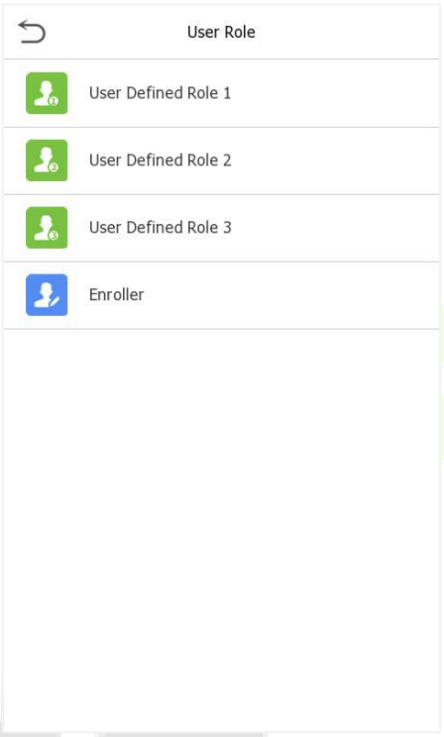


Linha Mista

6 Privilégio do Usuário

O **Privilégio do Usuário** facilita a atribuição de permissões específicas a determinados usuários, com base nos requisitos.

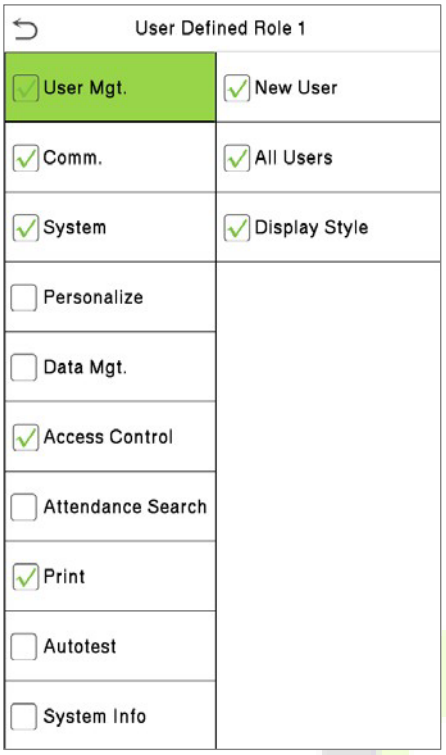
- No **menu principal**, toque em **Privilégio do Usuário** e, em seguida, toque na **Função Definida pelo Usuário** para definir as permissões definidas pelo usuário.
- O **escopo de permissão** da função personalizada pode ser configurado em 3 níveis, ou seja, o escopo operacional personalizado das funções do menu do usuário.

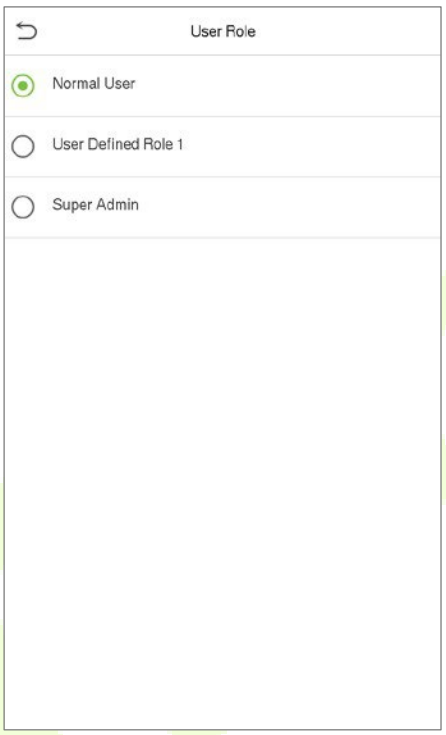


- Na interface de Função Definida pelo Usuário, alterne "Ativar Função Definida" para habilitar ou desabilitar a função definida pelo usuário.
- Toque no **Nome** e digite o nome da função personalizada.

- Em seguida, ao tocar em **Definir Função do Usuário**, selecione os privilégios necessários para a nova função e, em seguida, pressione o botão **Retornar**.
- Durante a atribuição de privilégios, os nomes das funções do menu principal serão exibidos à esquerda e seus submenus serão listados à direita.

- Primeiro, toque no nome da função do **Menu Principal** necessária e, em seguida, selecione seus submenus necessários na lista.



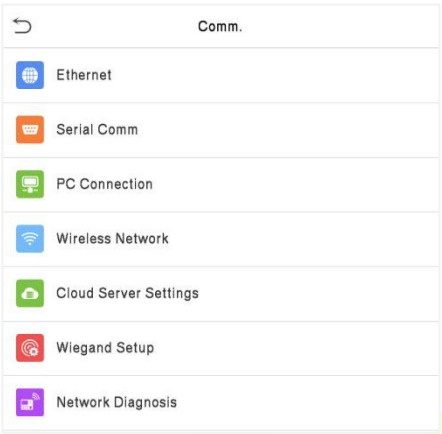


Observação: Se a Função do Usuário estiver habilitada para o Dispositivo, toque em **Gerenciamento de Usuário > Novo Usuário > Função do Usuário** para atribuir as funções criadas aos usuários necessários. No entanto, se não houver um superadministrador registrado no Dispositivo, então o dispositivo exibirá a mensagem "Por favor, cadastre primeiro um superadministrador!" ao habilitar a função de Função do Usuário.

7 Configurações de comunicação

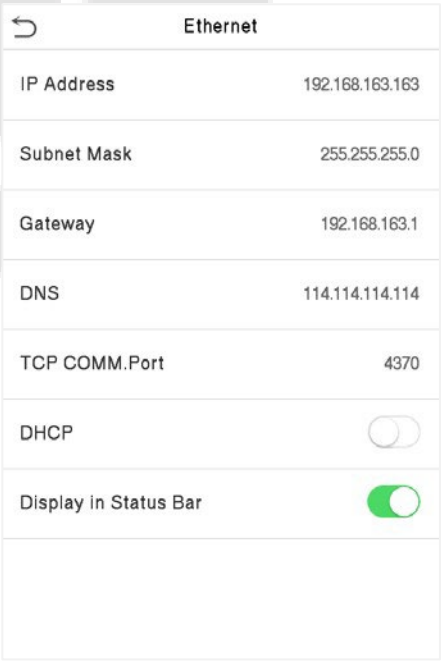
Toque em **Conf. Com.** no **Menu Principal** para definir a conexão com o PC, configuração da Nuvem e de Wiegand.

Toque em **COM.** no menu principal.



7.1 Configurações TCP/IP

Quando o dispositivo precisa se comunicar com um PC por TCP/IP, você precisará definir as configurações de rede e garantir que o dispositivo e o PC estejam se conectando no mesmo segmento de rede.
Toque em **TCP/IP** em **Conf. Com.** para definir as configurações.

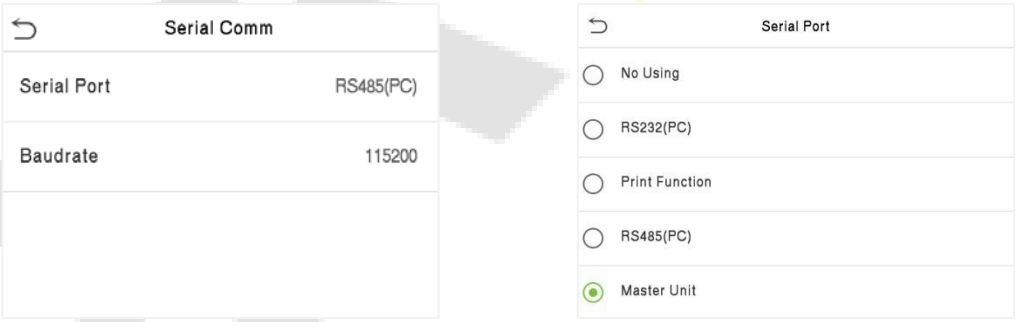


Nome da função	Descrição
TCP/IP	O valor de fábrica é 192.168.1.201 e pode ser editado;
Máscara de Rede	O valor de fábrica é 255.255.255.0 e pode ser editado;
Gateway	O valor de fábrica é 0.0.0.0 e pode ser editado;
DNS	O valor de fábrica é 0.0.0.0 e pode ser editado;
Porta de Comunicação TCP	O valor predefinido na fábrica é 4370 e pode ser editado;
DHCP	Ao habilitar esta função, o roteador será responsável por configurar todos os parâmetros de rede automaticamente.
Mostrar na barra status	Para definir se o ícone de rede será exibido na barra de status da tela inicial

7.2 Comunicação Serial

A função de Comunicação Serial estabelece a comunicação com o dispositivo por meio de uma porta serial (RS232/ Impressora/ RS485/ Unidade Mestra).

Toque em **Comunicação Serial** na interface de **Configurações de Comunicação**.



Descrição da Função

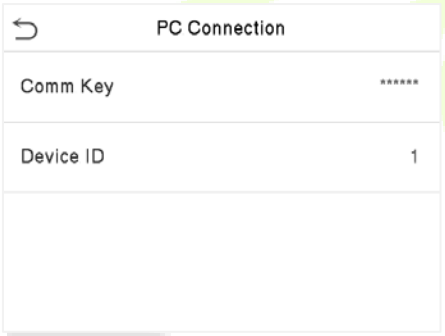
Nome da Função	Descrição
Porta Serial	**Não Usar:** Nenhuma comunicação com o dispositivo através da porta serial. **RS232(PC):** Comunicação com o dispositivo através da porta serial RS232. **RS485(PC):** Comunicação com o dispositivo através da porta serial RS485. **Função de Impressão:** O dispositivo pode ser conectado à impressora quando o RS485 habilita a função de impressão. **Unidade Mestra:** Quando o RS485 é utilizado como a função de "Unidade Mestra", ele pode ser conectado a um leitor de cartões.

Taxa de bauds	Existem 4 opções de taxa de bauds nas quais os dados se comunicam com o PC. São elas: 115200 (padrão), 57600, 38400 e 19200. Quanto maior a taxa de bauds, mais rápida é a velocidade de comunicação, porém também menos confiável. Portanto, uma taxa de bauds mais alta pode ser usada quando a distância de comunicação é curta; quando a distância de comunicação é longa, escolher uma taxa de bauds mais baixa é mais confiável.

7.3 Conexão do PC

A Senha de Comunicação aumenta a segurança na comunicação dos dados do dispositivo com o computador. Uma vez que a Senha de Comunicação for configurada no equipamento, ela deve ser fornecida ao software do PC para estabelecer uma conexão válida entre PC e dispositivo.

Toque em **Conexão do PC** na interface de configurações de comunicação para defini-las.



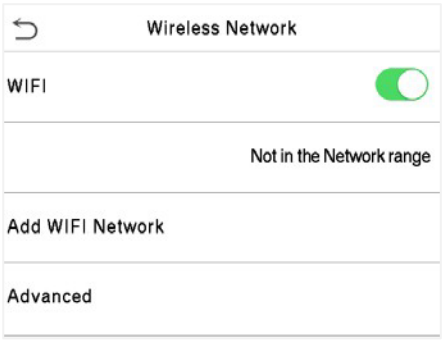
Nome da Função	Descrição
Senha de Comunicação	A senha padrão é 0, que pode ser alterada. A senha de comunicação pode conter de 1 a 6 dígitos.
ID do aparelho	Número de identificação do dispositivo na rede serial, que varia entre 1 e 254. Se o método de comunicação for RS232/RS485, você precisa inserir este ID do dispositivo na interface de comunicação do software.

7.4 Rede Sem Fio

O dispositivo fornece um módulo Wi-Fi, que pode ser integrado dentro do módulo do dispositivo ou conectado externamente.

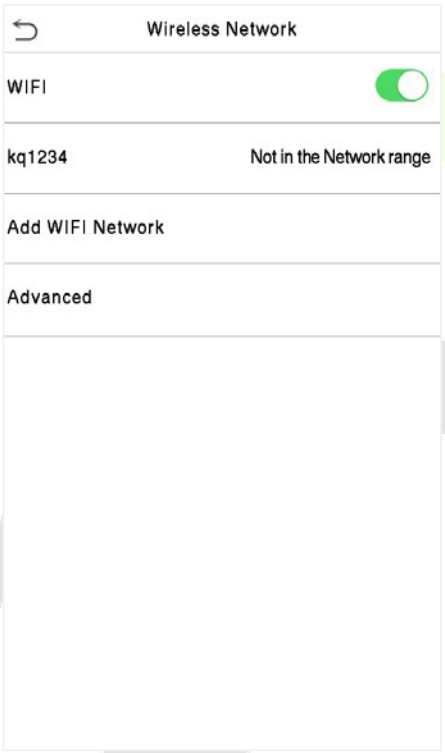
O módulo Wi-Fi possibilita a transmissão de dados via Wi-Fi (Wireless Fidelity) e estabelece um ambiente de rede sem fio. O Wi-Fi está habilitado por padrão no dispositivo. Se você não precisa usar a rede Wi-Fi, pode alternar o botão do Wi-Fi para desativá-lo.

Toque em **Rede Sem Fio** na interface de Configurações de Comunicação para configurar as configurações do Wi-Fi.

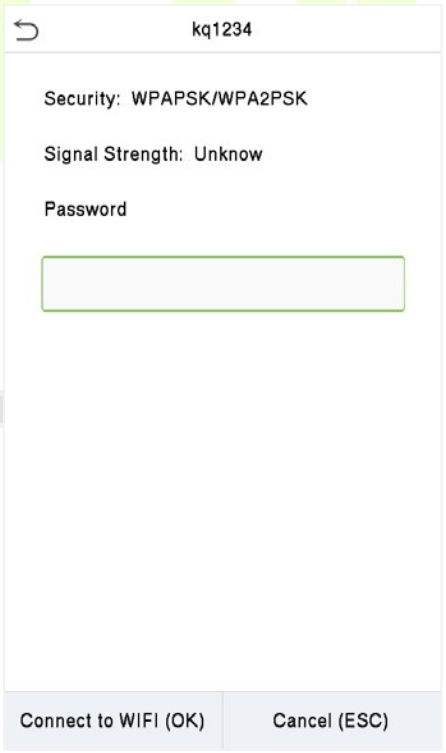


Procurando a Rede Wi-Fi

- O WIFI é ativado no dispositivo por padrão. Alternar o botão para ativar ou desativar o WIFI.
- Uma vez que o Wi-Fi é ativado, o dispositivo procurará pelas redes Wi-Fi disponíveis dentro do alcance da rede.
- Toque no nome do Wi-Fi desejado na lista disponível, insira a senha correta na interface de senha e, em seguida, toque em Conectar ao **WIFI (OK)**.



Wi-Fi Habilitado: Toque na rede desejada na lista de redes pesquisadas

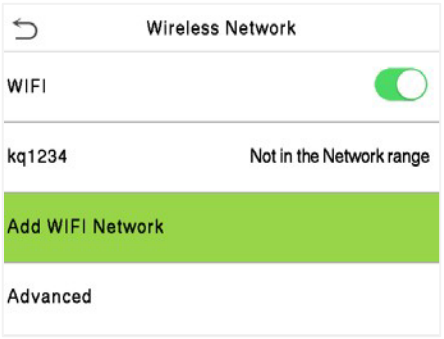


Toque no campo de senha para inserir a senha e toque em **Conectar ao WIFI (OK).**

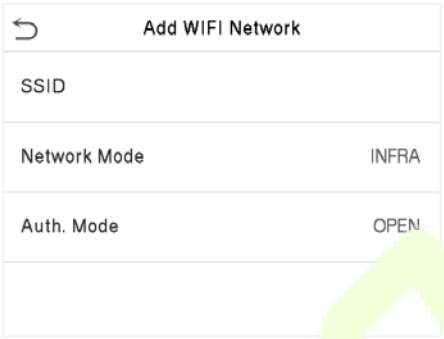
- Quando o WIFI for conectado com sucesso, a interface inicial exibirá o logotipo do Wi-Fi.

Adicionando Rede WIFI Manualmente

O WIFI também pode ser adicionado manualmente caso a rede WIFI desejada não apareça na lista.



Toque em **Adicionar Rede WIFI** para adicionar o WIFI manualmente.

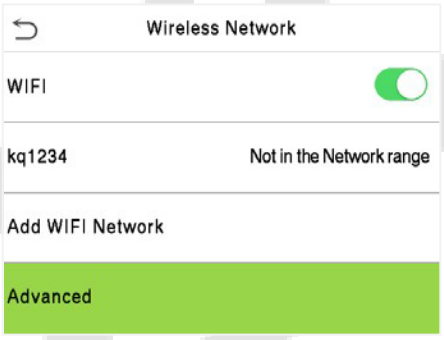


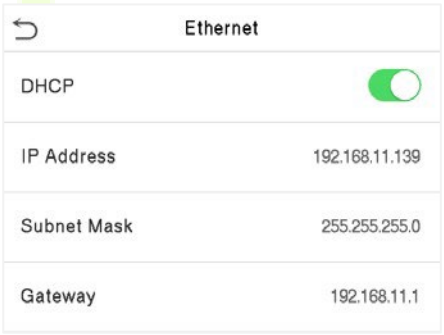
Nesta interface, insira os parâmetros da rede WIFI. (A rede adicionada deve existir.)

Note: Após adicionar o WIFI manualmente com sucesso, siga o mesmo processo para buscar pelo nome do WIFI adicionado. Clique aqui para visualizar o processo de busca da rede WIFI.

Configuração Avançada

Na interface da Rede Sem Fio, toque em Avançado para configurar os parâmetros relevantes conforme necessário.

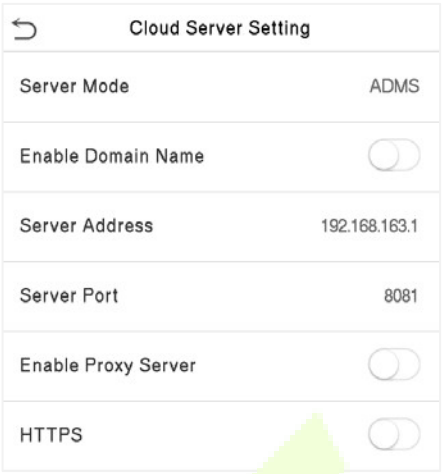




Nome da função	Descrição
DHCP	O Protocolo de Configuração Dinâmica de Hosts (DHCP) aloca dinamicamente endereços IP para os clientes da rede. Se o DHCP estiver habilitado, então o IP não pode ser configurado manualmente.
Endereço IP	O endereço IP para a rede WIFI é 0.0.0.0 por padrão. Pode ser modificado de acordo com a disponibilidade da rede.
Máscara de Sub-rede	A Máscara de Sub-rede padrão da rede WIFI é 255.255.255.0. Pode ser modificada de acordo com a disponibilidade da rede.
Gateway	O endereço de Gateway Padrão é 0.0.0.0. Pode ser modificado de acordo com a disponibilidade da rede.

7.5 Configurações do servidor de nuvem

Toque em **Configuração do Servidor de Nuvem** na Interface de **Configurações de Comunicação** para conexão com o servidor ADMS.



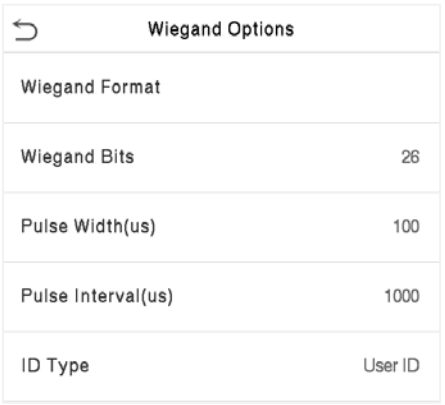
Função		Descrição
Ativar nome de domínio	**Endereço do servidor**	Uma vez habilitada esta função, será utilizado o modo de nome de domínio "http://...", como http://www.XYZ.com, enquanto "XYZ" será o nome de domínio (quando este modo está **LIGADO**).
Endereço do servidor	**Endereço do servidor**	Endereço 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		Baseado em HTTP, a criptografia da transmissão e a autenticação de identidade garantem a segurança do processo de transmissão.

7.6 Configuração de Wiegand

Para definir os parâmetros de entrada e saída Wiegand.

Toque em **Configuração Wiegand** na Interface de **Configurações de Comunicação** para definir os parâmetros de entrada e saída Wiegand.

7.6.1 Entrada Wiegand



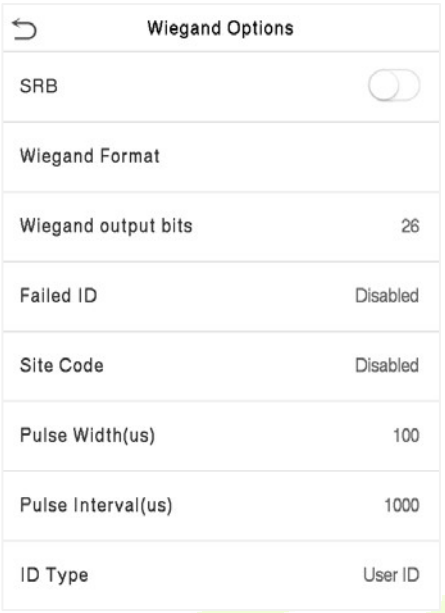
Nome da função	Descrição
Formato Wiegand	Os valores variam de 26 bits, 34 bits, 36 bits, 37 bits e 50 bits.
Bits de saída Wiegand	Após selecionar o formato Wiegand necessário, selecione os dígitos de bit de saída correspondentes do formato Wiegand.
Largura do pulso (us)	O valor da largura de pulso enviado pelo Wiegand é de 100 microssegundos por padrão, que pode ser ajustado dentro do intervalo de 20 a 400 microssegundos.
Intervalo de pulso (us)	O valor padrão é 1.000 microssegundos, que pode ser ajustado dentro do intervalo de 200 a 20.000 microssegundos.
Tipo de ID	Selecione entre ID do usuário e número do cartão.

Descrição dos formatos mais comuns de Wiegand:

Formato Wiegand	Descrição
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCO 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	ESSSSSSSSCCCCCCCCCCCCCCCO 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	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO 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	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO 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.0	

7.6.2 Saída Wiegand

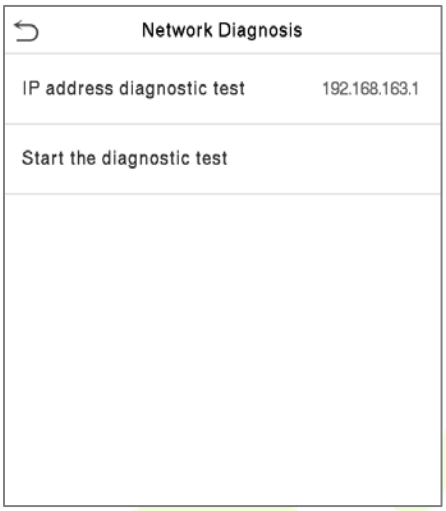


Função	Descrição
SRB	Quando o SRB está habilitado, a fechadura é acionada pelo SRB para evitar que a fechadura seja aberta com à remoção do dispositivo da parede
Formato Wiegand	Os valores variam de 26 bits, 34 bits, 36 bits, 37 bits e 50 bits.
Bits de saída Wiegand	Após selecionar o formato Wiegand necessário, selecione os dígitos de bit de saída correspondentes do formato Wiegand.
Código com Falha	Se a verificação falhar, o sistema enviará o ID com falha para o dispositivo ao invés do número do cartão ou ID.
Site code	É semelhante ao ID do dispositivo. A diferença é que um site code pode ser definido manualmente e pode ser repetido em um dispositivo diferente. O valor válido varia de 0 a 256 por padrão.
Largura do Pulso (µs)	A largura do tempo representa as mudanças na quantidade de carga elétrica com capacitância de alta frequência regular dentro de um tempo especificado.
Intervalo do Pulso	O intervalo de tempo entre pulsos.
Tipo de ID	Selecione entre ID do usuário e número do cartão.

7.7 Diagnóstico de Rede

Isso ajuda a configurar os parâmetros de diagnóstico de rede.

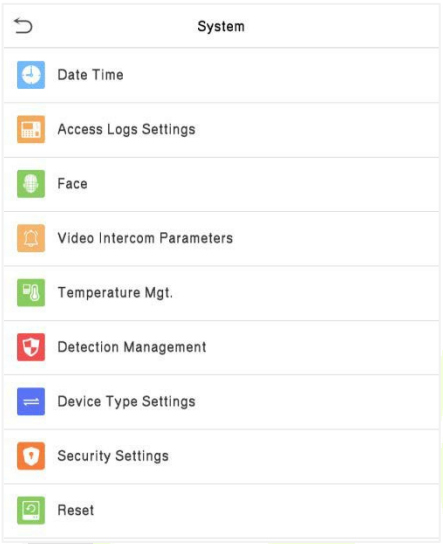
Toque em **Diagnóstico de Rede** na interface de **Configurações de Comunicação**. Insira o endereço IP que precisa ser diagnosticado e toque em Iniciar o teste de diagnóstico para verificar se a rede pode se conectar ao dispositivo.



8 Configurações do sistema

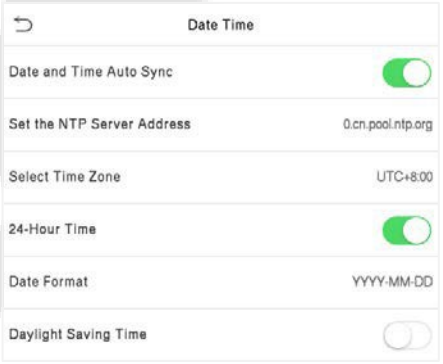
Defina os parâmetros do sistema para otimizar o desempenho do dispositivo.

Toque em **Sistema** na interface do **Menu Principal** para definir os parâmetros de sistema de forma a otimizar o desempenho do dispositivo



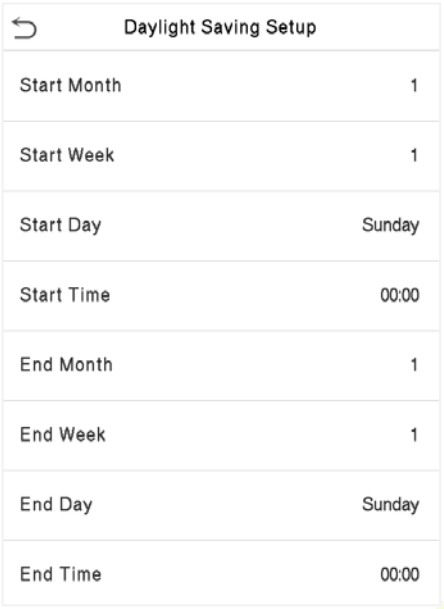
8.1 Data e hora

Toque em **Data e Hora** na interface do **Sistema** para definir a **Data e a Hora**.

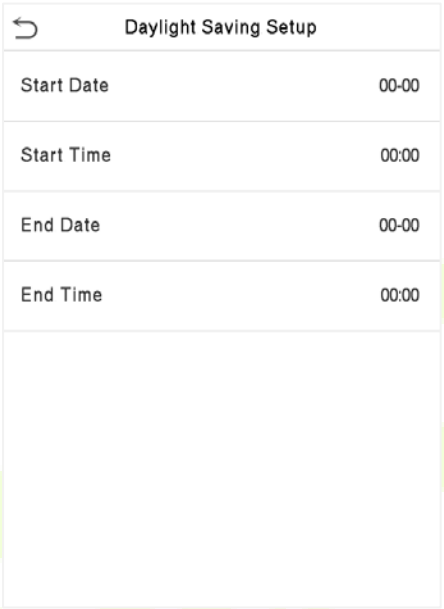


- Toque em **Sincronização Automática de Data e Hora** para habilitar a sincronização automática de tempo com base no endereço de serviço que você inserir.
- Toque em **Data e Hora Manual** para configurar manualmente a data e a hora e, em seguida, toque em **Confirmar para salvar**.
- Toque em **Selecionar Fuso Horário** para escolher manualmente o fuso horário onde o dispositivo está localizado.
- Habilite ou desabilite este formato tocando em **Horário de 24 Horas**. Se habilitado, selecione o **Formato de Data** para configurar a data.

- Toque em **Horário de Verão** para habilitar ou desabilitar a função. Se habilitado, toque em **Modo de Horário de Verão** para selecionar um modo de horário de verão e, em seguida, toque em **Configuração de Horário de Verão** para definir o horário do interruptor.



Modo de semana



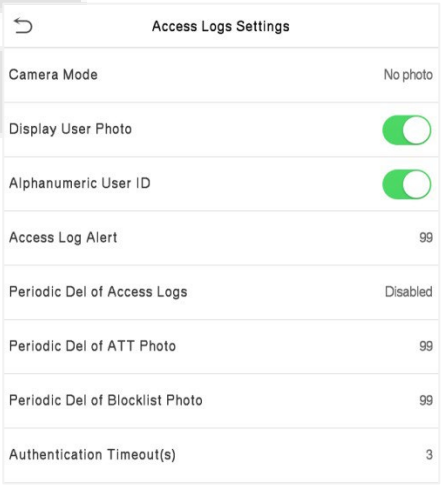
Modo de mês

- Ao restaurar as configurações de fábrica, o formato de hora (24 horas) e o formato de data (AAAA-MM-DD) podem ser restaurados, mas a data e a hora do dispositivo não podem ser restauradas.

Observação: Por exemplo, se um usuário configura o horário do dispositivo (18:35 do dia 15 de março de 2021) para 18:30 do dia 1 de janeiro de 2022. Após restaurar as configurações de fábrica, o horário do dispositivo permanecerá em 18:30 do dia 1 de janeiro de 2022.

8.2 Configuração de Registros de Acesso

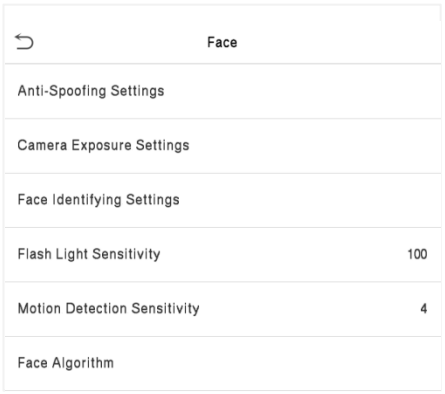
Toque em **Configuração de Registros de Acesso** na interface do Sistema.



Nome da função	Descrição
Modo de câmera	Para capturar e salvar a imagem durante a autenticação. Existem 5 modos: **Sem Foto**: Nenhuma foto é tirada durante a autenticação do usuário. **Tirar foto, não salvar**: a foto é tirada, mas não salva durante a autenticação. **Tirar foto e salvar**: a foto é tirada e salva durante a autenticação. **Salvar na verificação bem-sucedida**: a foto é tirada e salva para cada autenticação bem-sucedida. **Salvar na verificação com falha**: a foto será tirada e salva apenas para a autenticação com falha.
Exibir foto do usuário	Se a foto do usuário deve ser exibida quando o usuário for autenticado com sucesso.
ID de Usuário Alfanumérico	Habilitar/Desabilitar o alfanumérico como ID de Usuário.
Aviso de logs de acesso	Quando o espaço de registro do acesso atingir o valor limite máximo, o dispositivo exibirá automaticamente o aviso de espaço de memória. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 9999.
Exclusão cíclica dos registros de acesso	Quando os registros de acesso atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de registros de acesso antigos. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 999.
Excluir Fotos de frequência	Quando as fotos de frequência atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de fotos de ponto antigas. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 99.
Excluir fotos da lista de proibições	Quando as fotos da lista de proibições atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de fotos da lista negra antigas. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 99.
Atraso de tela (s)	A duração da mensagem de autenticação bem-sucedida é exibida. Valor válido: 1~9 segundos.

8.3 Parâmetros de Reconhecimento Facial

Toque em **Face** na interface do **Sistema** para acessar as configurações dos parâmetros de reconhecimento facial.



FRR	FAR	Limiares de Correspondência Recomendados	
		1: N	1:1
Alta	Baixa	85	80
Média	Média	82	75
Baixa	Alta	80	70

Descrição da função

Nome da Função	Descrição
Configurações de Antifalsificação	**Antifalsificação Monocular 2D**: Utiliza imagens de luz visível para detectar tentativas de falsificação e avaliar se a amostra biométrica fornecida é de uma pessoa real (ser humano vivo) ou uma representação falsa. **Limiar de Antifalsificação Monocular 2D:** Facilita a avaliação se a imagem visível capturada é de uma pessoa real (ser humano vivo). Quanto maior o valor, melhor o desempenho antifalsificação usando luz visível. **Antifalsificação Binocular 2D:** Utiliza imagens de espectros de infravermelho próximo para identificar e prevenir fotos falsas e ataques de vídeo. **Limiar de Antifalsificação Binocular 2D:** Facilita a avaliação se a imagem espectral de infravermelho próximo é uma foto ou vídeo falso. Quanto maior o valor, melhor o desempenho antifalsificação usando espectros de infravermelho próximo. **Nota:** O usuário deve habilitar tanto o Antifalsificação Monocular 2D quanto o Antifalsificação Binocular 2D nas configurações de Antifalsificação. Quando um dos interruptores é ligado, o outro é ativado ao mesmo tempo por padrão. Quando a opção é ligada ou desligada, o dispositivo reinicia automaticamente para executar a função.

Configurações de Exposição da Câmera	**AE:** No modo Face AE, quando o rosto está na frente da câmera, a luminosidade da área do rosto aumenta, enquanto outras áreas ficam mais escuras. **WDR:** Equilibra a luz e estende a visibilidade da imagem para vídeos de vigilância em cenas de iluminação de alto contraste, melhorando a identificação de objetos em ambientes claros e escuros. **Modo Anti-Flicker**: É usado quando o WDR está desligado. Ele ajuda a reduzir o flicker quando a tela do dispositivo pisca na mesma frequência que a luz.
Configurações de Identificação Facial	**Valor do Limiar 1:N** A verificação será bem-sucedida somente se a semelhança entre a imagem facial adquirida e todos os modelos faciais registrados for maior do que o valor definido no modo de verificação 1: N. O valor válido varia de 0 a 100. Quanto maior o limiar, menor a taxa de erro de julgamento e maior a taxa de rejeição, e vice-versa. Recomenda-se configurar o valor padrão de 75.
	Valor do Limiar 1:1 modo de verificação 1:1, a verificação só será bem-sucedida quando a semelhança entre a imagem facial adquirida e os modelos faciais do usuário inscritos no dispositivo for maior do que o valor definido. O valor válido varia de 0 a 100. Quanto maior o limiar, menor a taxa de erro de julgamento e maior a taxa de rejeição, e vice-versa. Recomenda-se configurar o valor padrão de 63.
	Limiar de Cadastro Facial: Durante o cadastro de face, a comparação 1: N é usada para determinar se o usuário já foi registrado anteriormente. Quando a semelhança entre a imagem facial adquirida e todos os modelos faciais registrados é maior do que o limiar definido, isso indica que o rosto já foi registrado
	Limiar de Correspondência 1: N para Pessoas com Máscara: A taxa de reconhecimento para pessoas usando máscara sob a configuração do modo de verificação 1:N. Quanto maior o limiar, menor é a taxa de erro de julgamento e maior é a taxa de rejeição, e vice-versa. Recomenda-se configurar o valor padrão de 68.
	Ângulo de Inclinação do Rosto: É a tolerância de ângulo de inclinação de um rosto para registro e comparação de modelos faciais. Se o ângulo de inclinação do rosto exceder o valor definido, ele será filtrado pelo algoritmo, ou seja, ignorado pelo terminal, e, portanto, nenhuma interface de registro e comparação será acionada.
	Ângulo de Rotação do Rosto: É a tolerância de ângulo de rotação de um rosto para registro e comparação de modelos faciais. Se o ângulo de rotação do rosto exceder o valor definido, ele será filtrado pelo algoritmo, ou seja, ignorado pelo terminal, e, portanto, nenhuma interface de registro e comparação será acionada.
	Qualidade da Imagem: É a qualidade da imagem para registro e comparação facial. Quanto maior o valor, mais clara a imagem é requerida.

<table>
<tr><td></td><td colspan="2">Tamanho Mínimo do Rosto: Define o tamanho mínimo de rosto necessário para registro e comparação facial. Se o tamanho mínimo da imagem capturada for menor que o valor definido, ela será filtrada e não reconhecida como um rosto. Esse valor também pode ser interpretado como a distância de comparação facial. Quanto mais distante o indivíduo estiver, menor será o rosto e menos pixels do rosto obtidos pelo algoritmo. Portanto, ajustar esse parâmetro pode ajustar a comparação mais distante de distância entre os rostos. Quando o valor é 0, a distância de comparação de rostos não é limitada.</td></tr>
<tr><td></td><td rowspan="2">Modo de Identificação</td><td>Identificação de Múltiplos Rostos: Quando ativado, o dispositivo pode identificar vários rostos ao mesmo tempo.

O Modo de Conteúdo a Ser Exibido e a Contagem a Ser Exibida podem ser configurados apenas se estiverem ativados.

Modo de Conteúdo a Ser Exibido: Você pode selecionar o conteúdo exibido abaixo da foto do usuário na interface após a verificação facial ser bem-sucedida. Por exemplo, exibir apenas o ID do usuário, exibir o nome, exibir o ID do usuário + nome, exibir carimbo de data e hora, exibir ID do usuário + carimbo de data e hora, exibir nome + carimbo de data e hora.
Contagem a Ser Exibida: Você pode escolher o número de resultados de verificação facial a serem exibidos na interface de uma vez, por exemplo, se definido como 3, a interface exibirá até 3 verificações de usuário bem-sucedidas de uma só vez.
Nota: A Contagem a Ser Exibida pode ser configurada de 1 a 4 usuários.</td></tr>
<tr><td>Identificação Discreta: O mesmo rosto só pode ser reconhecido uma vez. Para reconhecê-lo novamente, você deve sair da área de reconhecimento facial e entrar novamente antes que ele possa ser reconhecido novamente.</td></tr>
<tr><td></td><td colspan="2">Intervalo de Comparação Facial (s): Após clicar (selecionar) o intervalo de identificação, por exemplo, se o intervalo de comparação for configurado para 5 segundos, então o reconhecimento facial verificará o rosto a cada 5 segundos. Valor válido: 0 a 9 segundos. 0 significa identificação contínua, de 1 a 9 significa identificação em intervalos.</td></tr>
<tr><td></td><td colspan="2">Modo de Correspondência Híbrida de Luz Visível-Infravermelho: Reconhecimento de duplo modo em infravermelho próximo e luz visível. Aplicar reconhecimento em infravermelho próximo (NIR), reconhecimento em luz visível ou combinação de NIR e luz visível em reconhecimento de duplo modo automaticamente, de acordo com diferentes cenários de comparação.</td></tr>
<tr><td>Sensibilidade da Luz de Flash</td><td colspan="2">Este valor controla o ligar e desligar da luz LED. Quanto maior o valor, mais frequentemente a luz LED será ligada e desligada.</td></tr>
<tr><td>Sensibilidade de Detecção de Movimento</td><td colspan="2">Isso define o valor para a mudança no campo de visão da câmera conhecida como detecção potencial de movimento, que acorda o terminal do modo de espera para a interface de comparação.
Quanto maior o valor, mais sensível o sistema será, ou seja, se um valor maior for definido, a interface de comparação será ativada com mais facilidade e a detecção de movimento será acionada com mais frequência.</td></tr>
</table>

Algoritmo Facial	Ele contém informações relacionadas ao algoritmo facial e pausa a atualização do modelo facial.

Observação:

1) O ajuste inadequado dos parâmetros de exposição e qualidade pode afetar severamente o desempenho do dispositivo. Ajuste o parâmetro de exposição apenas sob a orientação dos profissionais de pós-venda de nossa empresa.
2) As opções Face AE e Identificação de Múltiplos Rostos são mutuamente exclusivas. Quando o interruptor da função de Identificação de Múltiplos Rostos é ativado, o interruptor de Face AE será automaticamente desligado. Se você ativar o Face AE neste momento, o modo de reconhecimento mudará para o modo de reconhecimento de um único rosto.
3) O intervalo de comparação facial e a Identificação de Rastreamento são opções mutuamente exclusivas. Se o interruptor de Identificação de Rastreamento for ativado, a função de intervalo de comparação facial nas Configurações de Identificação de Rosto será desativada, e vice-versa.Process to modify the Facial Recognition Accuracy

- Na interface do Sistema, toque em **Rosto > Antifalsificação** e ative as opções de **Antifalsificação Monocular 2D e Antifalsificação Binocular** 2D para configurar a antifalsificação.
- Em seguida, no **Menu Principal**, toque em **Auto-Teste** > **Teste de Face** e realize o teste facial.
- Toque três vezes nos escores no canto superior direito da tela e a caixa retangular vermelha aparecerá para começar a ajustar o modo.
- Mantenha uma distância de um braço entre o dispositivo e o rosto. É recomendado não mover o rosto em uma ampla gama.

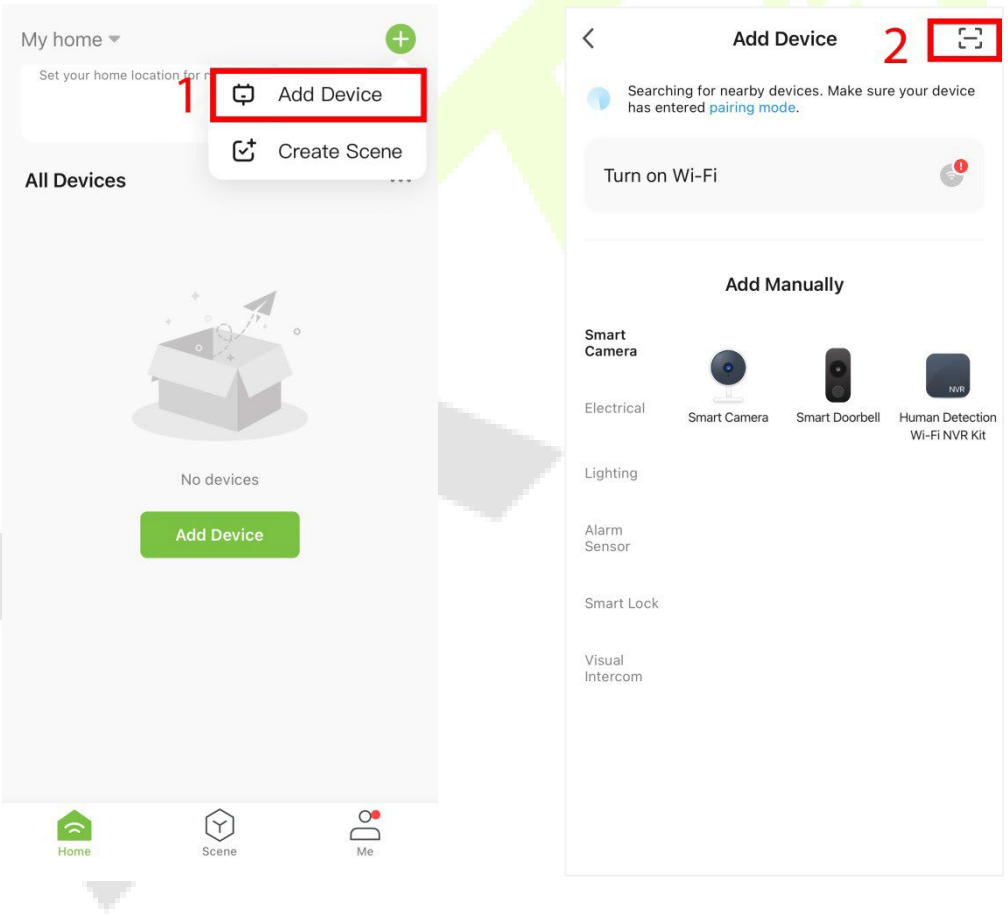
8.4 Parâmetros de Vídeo Interfone

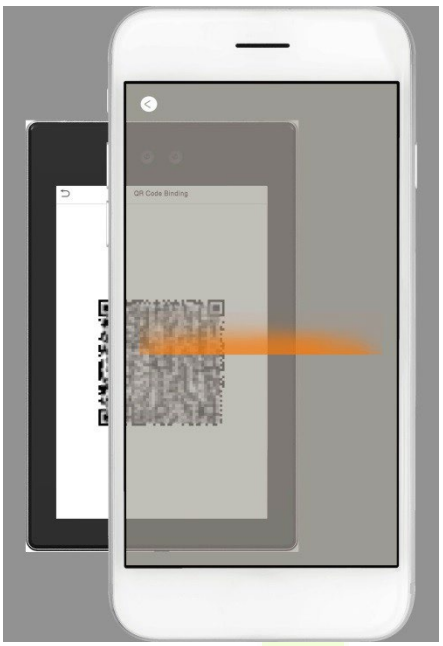
Toque em **Parâmetros de Vídeo Interfone** na interface do Sistema.

Após baixar e instalar o aplicativo ZSmart no telefone, abra-o e escaneie o código QR para adicionar o dispositivo para conectividade com o interfone de vídeo.

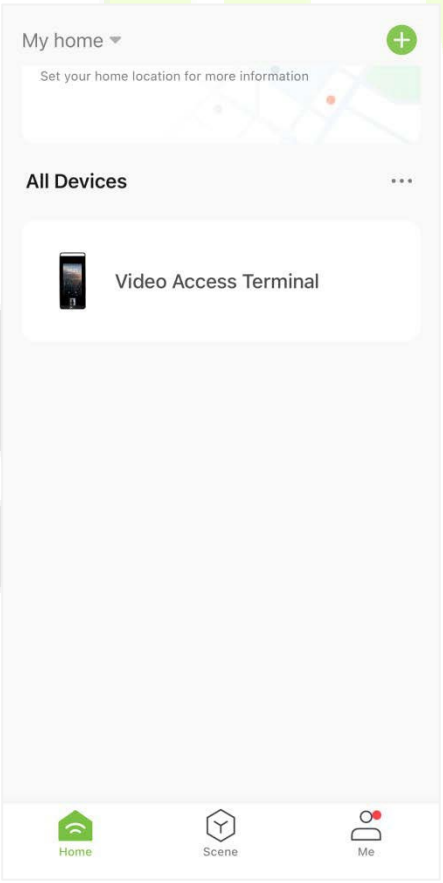
- **Conectar ao ZSmart APP**

Após baixar e instalar o aplicativo ZSmart em seu telefone, crie uma conta de usuário inicialmente com o seu endereço de e-mail. Depois de criar a conta de usuário, faça login no aplicativo e clique ⊕ para adicionar o dispositivo. O processo é o seguinte:





Você pode adicionar o dispositivo **escaneando um código**. Após a adição ser bem-sucedida, o dispositivo é exibido na página do terminal.



- **Conexão de Vídeo Porteiro**

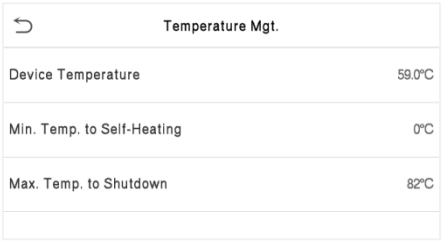
Os visitantes tocam em  para fazer uma ligação e o telefone irá tocar. O usuário pode aceitar ou recusar a chamada. Após o usuário aceitar a chamada, a interface do interfone de vídeo será aberta. Digite a senha para destrancar a porta..

Item	Descrição
Captura de Tela	Clique para tirar uma captura de tela.
Falar	O ícone ficará **azul** quando você clicar nele e você pode falar com o dispositivo nesse momento.
Gravar	Clique para gravar um vídeo.
Álbum de Fotos	Visualize e exclua capturas de tela e os vídeos gravados.
Destrancar	Clique para abrir a porta remotamente. O registro de destrancamento é salvo em Eu > Centro de Mensagens.

8.5 Gerenciamento de Temperatura

O dispositivo possui um sensor de temperatura integrado e, quando a temperatura do ambiente está muito baixa ou muito alta, ele acionará o autoaquecimento ou desligará.

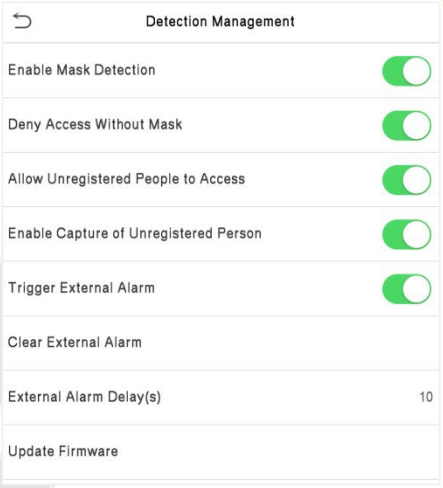
Clique em **Gerenciamento de Temperatura** na interface do **Sistema**.



Nome da função	Descrição
Temperatura do Dispositivo	Esta coluna mostra a temperatura em tempo real do dispositivo.
Temperatura Mínima para Autoaquecimento	Quando a temperatura do dispositivo estiver abaixo do valor definido, o dispositivo iniciará o autoaquecimento, com uma faixa de 0 a 10 (°C).
Temperatura Máxima para Desligamento	Quando a temperatura do dispositivo estiver acima do valor definido, ele será desligado automaticamente para proteger o hardware, com uma faixa de 70 a 90 (°C).

8.6 Gerenciamento de Detecção

Toque em **Gerenciamento de Detecção** na interface do **Sistema** para configurar as configurações de Gerenciamento de Detecção.

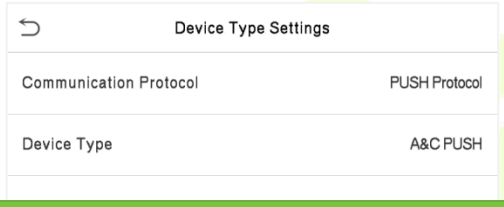


Nome da função	Descrição
Ativar Detecção de Máscara	Isso ativa ou desativa a função de detecção de máscara. Quando ativada, o dispositivo identifica se o usuário está usando uma máscara durante a verificação.
Negar Acesso Sem Máscara	Isso ativa ou desativa o acesso de uma pessoa sem máscara. Quando ativado, o dispositivo nega o acesso de uma pessoa se ela não estiver usando máscara.
Permitir Acesso de Pessoas Não Registradas	Isso ativa ou desativa o acesso de pessoas não registradas. Quando ativado, o dispositivo permite que a pessoa entre sem registro.

Ativar Captura de Pessoa Não Registrada	Para ativar ou desativar a captura da pessoa não registrada. Quando ativado, o dispositivo capturará automaticamente a foto da pessoa não registrada. Habilitar esse recurso requer a ativação de Permitir Acesso de Pessoas Não Registradas.
Acionar Alarme Externo	Quando ativado, se o usuário não estiver usando máscara, o sistema acionará um alarme.
Limpar Alarme Externo	Isso limpa os registros de alarmes acionados do dispositivo.
Atraso do Alarme Externo (s)	É o tempo de atraso (em segundos) para acionar um alarme externo. Pode ser configurado em segundos. Os usuários podem desativar a função ou definir um valor entre 1 e 255.
Atualizar Firmware	Atualizar a versão do firmware de detecção.

8.7 Configuração do Tipo de Dispositivo

Toque em **Configuração do Tipo de Dispositivo** na interface do **Sistema** para configurar as configurações de Configuração do Tipo de Dispositivo.

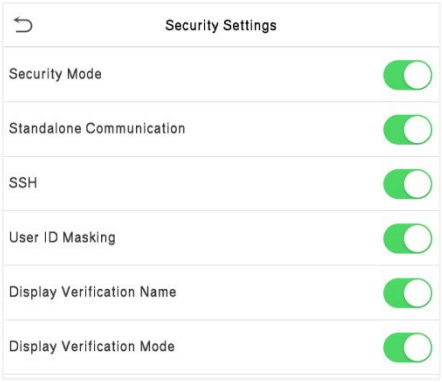


Nome da função	Descrição
Terminal de Controle de Presença	Defina o dispositivo como um terminal de controle de presença.
Terminal de Controle de Acesso	Defina o dispositivo como um terminal de controle de acesso.

Observação: Após alterar o tipo de dispositivo, o dispositivo irá apagar todos os dados e reiniciar, e algumas funções serão ajustadas de acordo.

8.8 Configurações de Segurança

Toque em **Configurações de Segurança** na **interface do Sistema** para acessar as configurações de segurança.

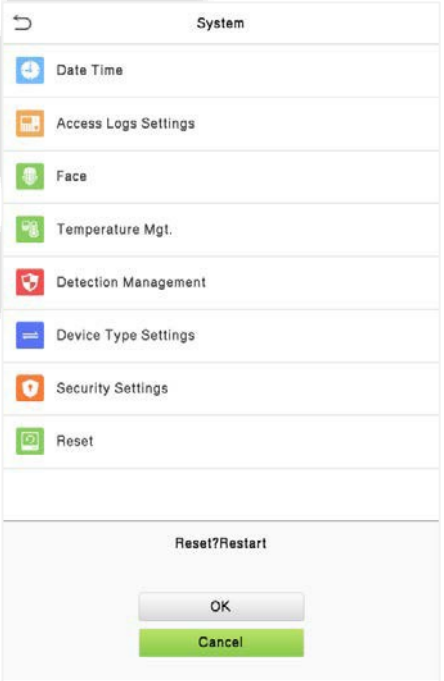


Nome da função	Descrição
Modo de Segurança	Selecione se deseja habilitar o modo de segurança para proteger o dispositivo e as informações pessoais do usuário. Você pode configurar o dispositivo para funcionar offline e ocultar as informações pessoais do usuário para evitar vazamentos durante a verificação do usuário.
Comunicação Standalone	Para evitar não conseguir usar quando o dispositivo está offline, você pode baixar o software C/S (como o ZKAccess 3.5) em seu computador com antecedência para uso offline.
SSH	SSH é usado para entrar no modo de manutenção do dispositivo.
Mascaramento de ID do Usuário	Quando ativado e o usuário é comparado e verificado com sucesso, o ID do usuário no resultado de verificação exibido será substituído por um * para alcançar a proteção segura de informações privadas sensíveis.
Exibir Nome de Verificação	Defina se deseja exibir o nome de usuário na interface de resultado de verificação.
Exibir Modo de Verificação	Defina se deseja exibir o modo de verificação na interface de resultado de verificação.

8.9 Restauração dos padrões de fábrica

A função de Restauração de Fábrica restaura as configurações do dispositivo, como configurações de comunicação e configurações do sistema, para as configurações de fábrica padrão (esta função não apaga os dados de usuário registrados).

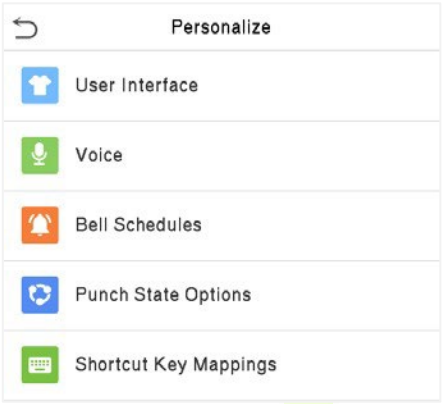
Toque em **Resetar** na interface do **Sistema** e depois toque em **OK** para restaurar as configurações padrão de fábrica.



9 Configurações de Personalização

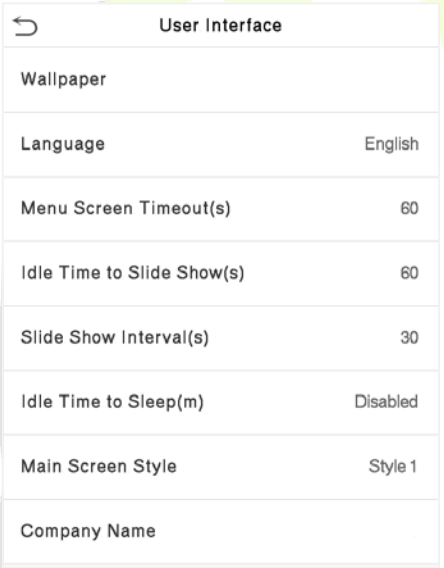
Toque em **Personalizar** a interface do **Menu Principal** para personalizar as configurações da interface, voz, sino, opções de estado de ponto e mapeamento de teclas de atalho.

.



9.1 Configurações de Exibição

Toque em **Interface do Usuário** na **interface Personalização** para personalizar o estilo de exibição

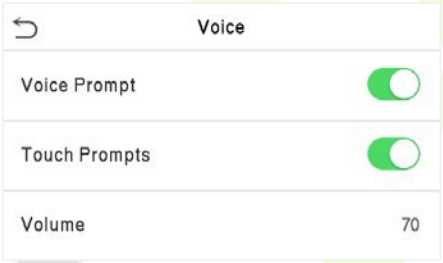


Nome da função	Descrição
Papel de parede	O papel de parede da tela principal pode ser selecionado de acordo com a preferência do usuário.
Idioma	Selecione o idioma do dispositivo.
Tempo limite da tela do menu (s)	Quando não há utilização e o tempo excede o valor definido, o dispositivo retornará automaticamente à tela inicial. A função pode ser desativada ou definir o valor necessário entre 60 e 99999 segundos.

Tempo de espera (s)	Quando não houver operação e o tempo exceder o valor definido, uma apresentação de slides será reproduzida. A função pode ser desativada ou você pode definir o valor entre 3 e 999 segundos.
Intervalo de apresentações (s)	É o intervalo de tempo para alternar entre diferentes fotos de apresentação de slides. A função pode ser desativada ou você pode definir o intervalo entre 3 e 999 segundos.
Tempo de inatividade (m)	Se o modo de inatividade estiver ativado e não houver utilização do dispositivo, ele entrará no modo de espera. Toque em qualquer lugar da tela para retomar o modo de trabalho normal. Esta função pode ser desativada ou definir um valor dentro de 1-999 minutos.
Estilo da tela principal	O estilo da tela principal pode ser selecionado de acordo com a preferência do usuário.
Nome da Empresa	Digite o nome da empresa aqui. O nome da empresa é impresso quando a opção de nome da empresa nas configurações de informações de impressão está habilitada.

9.2 Configurações de voz

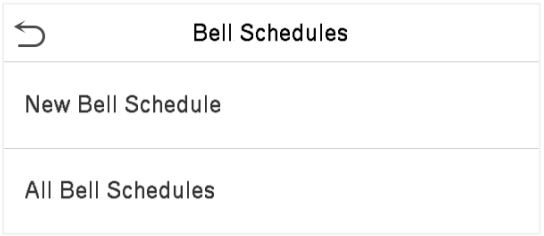
Toque em **Opções de Voz** na interface **Personalização** para definir as configurações de voz.



Nome da Função	Descrição
Voz	Alterne para ativar ou desativar os comandos de voz durante as operações de funções.
Confi. de toque	Alterne para ativar ou desativar os sons do teclado.
Volume	Ajuste o volume do dispositivo que pode ser definido entre 0-100.

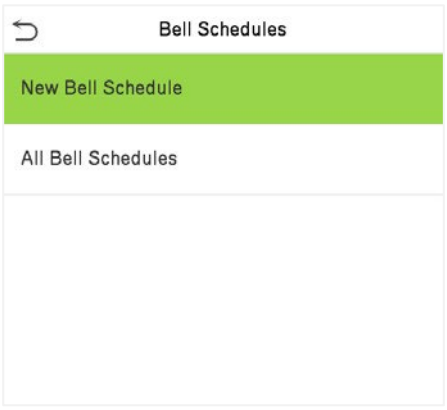
9.3 Horários

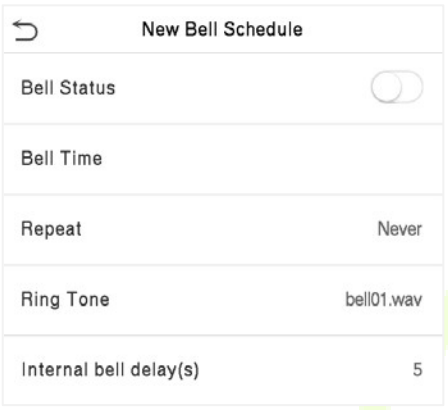
Toque em **Horários** na interface **Personalização** para definir as configurações de Horários.



Novo Horário

Toque em **Novo Horário** na interface **Horário** para adicionar uma nova programação de horário.





Nome da função	Descrição
Status da campainha	Alterne para ativar ou desativar o status da campainha.
Horário campainha	Uma vez definido o tempo necessário, o dispositivo acionará automaticamente para tocar a campainha durante esse tempo.
Repetir	Defina o número necessário de contagens para repetir a campainha programada.
Toque	Selecione um som de campainha.
Intervalo campainha (s)	Defina o tempo de reprodução da campainha. Os valores válidos variam de 1 a 999 segundos.

Todos os horários de campainha

Assim que a campainha estiver agendada, na interface de **Horários**, toque em **Todos os Horários** para visualizar o que foi agendado.

Edite a campainha agendada

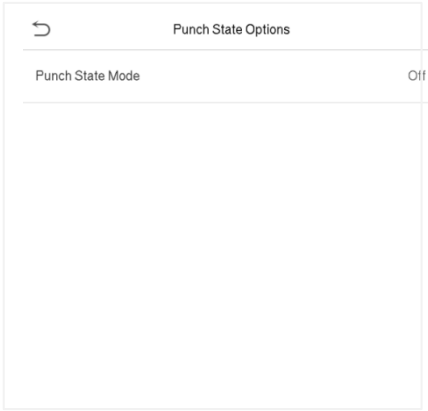
Na interface **Todos os Horários**, toque na programação de campainha e toque em **Editar** para editar a programação de campainha selecionada. O método de edição é o mesmo que as operações de adição de uma nova programação de campainha.

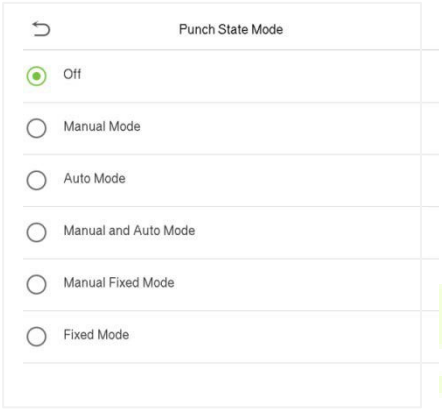
Deletar um horário

Na interface **Todos os Horários** de campainha, toque na programação de campainha e toque em **Excluir**, em seguida, toque em **Sim** para excluir a campainha selecionada.

9.4 Configurações de status de registro de presença

Toque em Opções de Status de Registro de Presença na interface de Personalização para configurar as configurações de Status de Registro de Presença.



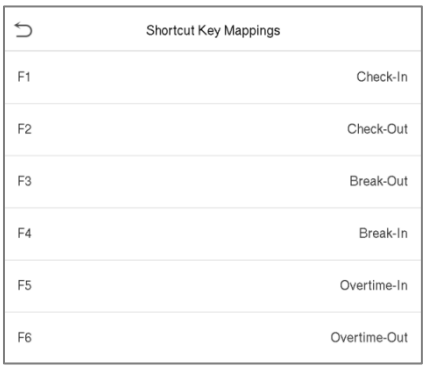


Nome da função	Descrição
Modo de status de registro de presença	Selecione um Modo de Status de Registro de Presença: **Off:** Isso desabilita a função de registro de presença. E a tecla de registro de presença definida no menu de **Mapeamento de Teclas de Atalho** se torna inválida. **Modo Manual:** Altere manualmente a tecla de registro de presença, e ela desaparecerá após o **Tempo Limite do Estado de Registro de Presença.** **Modo Automático:** A tecla de registro de presença alternará automaticamente para um status de registro de presença específico de acordo com o cronograma predefinido, que pode ser configurado no Mapeamento de Teclas de Atalho. **Modo Manual e Automático:** A interface principal exibirá a tecla de registro de presença de alternância automática. No entanto, os usuários ainda poderão selecionar uma alternativa que é o status de presença manual. Após o tempo limite, a tecla de registro de presença de alternância manual se tornará uma tecla de registro de presença de alternância automática. **Modo Fixo Manual:** Depois que a tecla de registro de presença for configurada manualmente para um status de registro de presença específico, a função permanecerá inalterada até que seja alterada manualmente novamente. **Modo Fixo:** Somente a tecla de registro de presença definida manualmente

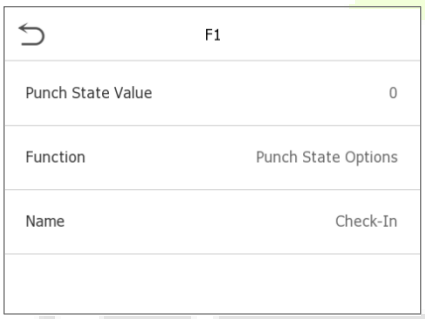
9.5 Mapeamentos de teclas de atalhos

Os usuários podem definir teclas de atalho para status de ponto que serão exibidas na interface principal. Assim, na interface principal, quando as teclas de atalho são pressionadas, o status de ponto ou a interface de funções serão exibidas.

Toque em **Mapa de atalhos** na interface **Personalização** para definir as teclas de atalho necessárias.



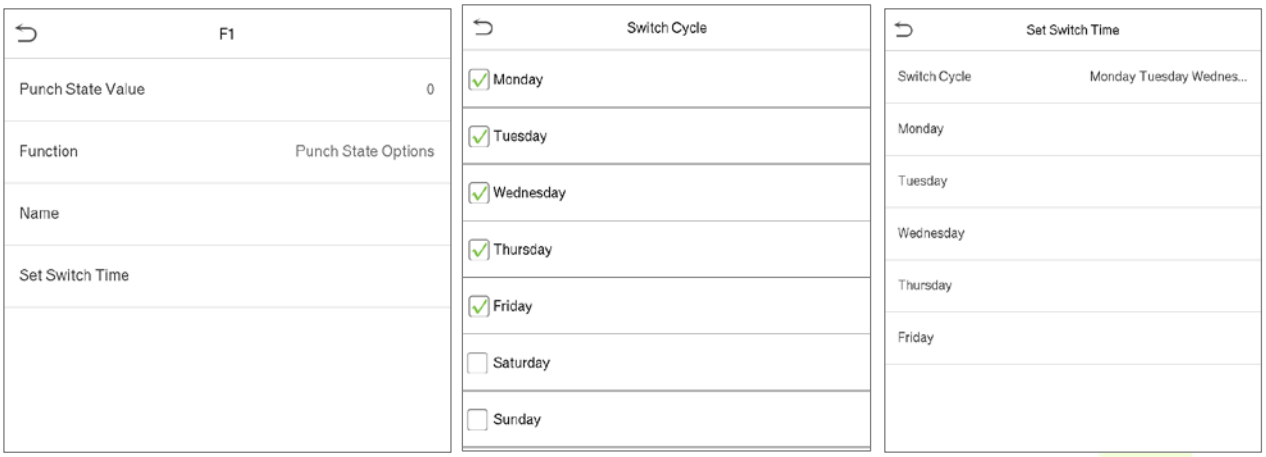
- Na interface de Mapeamento de Teclas de Atalho, toque na tecla de atalho necessária para configurar as configurações da tecla de atalho.
- Na interface da Tecla de Atalho (por exemplo, "F1"), toque na função para definir o processo funcional da tecla de atalho, seja como uma tecla de estado de ponto ou uma tecla de função.
- Se a tecla de atalho for definida como uma tecla de função (como Novo usuário, Todos os usuários, etc.), a configuração é concluída como mostrado na imagem abaixo.



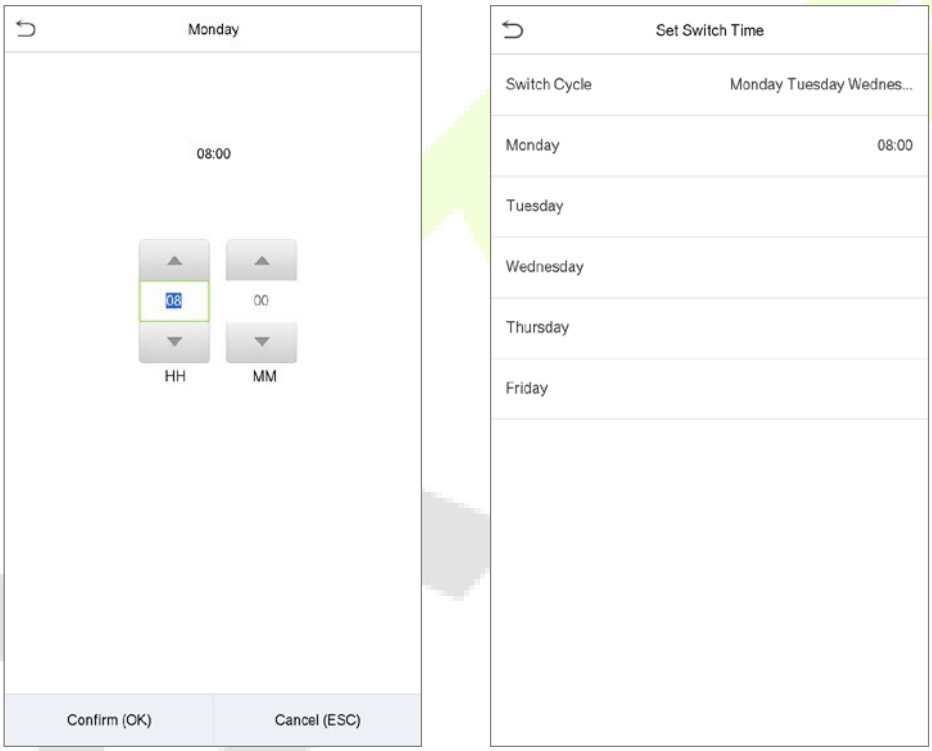
- Se a tecla de atalho for definida como uma tecla de status de presença (como entrada, saída, etc.), então é necessário definir o valor do status (valor válido de 0 a 250) e o nome.

Defina o horário de comutação

- O horário de comutação é definido de acordo com as opções de status de presença.
- Quando o Modo de Status de Presença estiver definido como Modo Automático, o horário de comutação deve ser configurado.
- Na interface de Tecla de Atalho, toque em Definir Horário de Comutação para configurar o horário de comutação.
- Na interface de Ciclo de Comutação, selecione o ciclo de comutação (segunda-feira, terça-feira, etc.), conforme mostrado na imagem abaixo.



- Uma vez que o ciclo de comutação é selecionado, defina o horário de comutação para cada dia e toque em OK para confirmar, como mostrado na imagem abaixo.



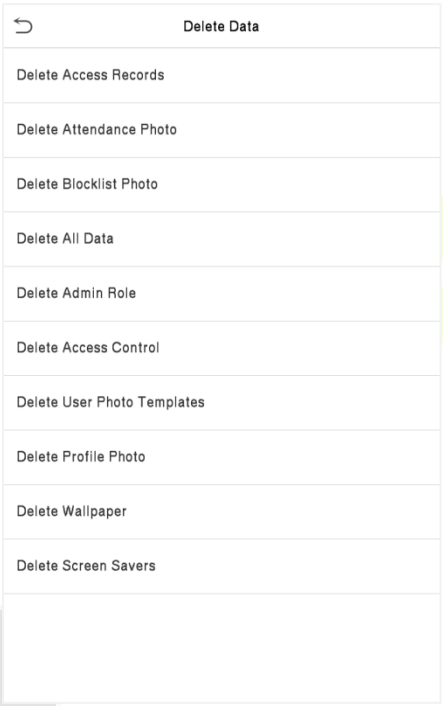
Observação: Quando a função estiver definida como indefinida, o dispositivo não habilitará a tecla de estado de presença.

10 Gerenciamento de dados

No **Menu Principal**, toque em **Gerenciamento de Dados** para excluir os dados do dispositivo.

10.1 Excluir dados

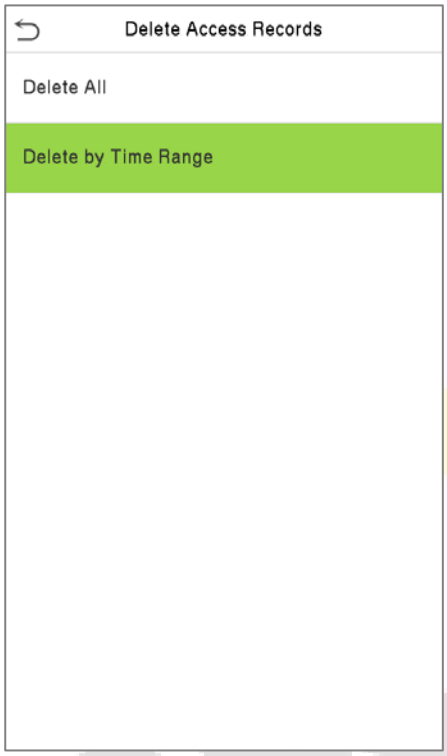
Toque em **Excluir Dados** na interface de **Gerenciamento de dados**



Menu	Descrição
Apagar reg. de acesso	Para apagar dados de frequência/registros de acesso.
Apagar foto de presença	Para apagar fotos de presença registradas.
Apagar foto lista bloqueio	Para apagar as fotos tiradas durante verificações com falha.
Apagar todos os dados	Para apagar informações e registros de presença/registros de acesso de todos os usuários registrados.
Apagar privilégios de administrador	Para remover todos os privilégios de administrador. (não apagar usuários)
Apagar dados de acesso	Para apagar todos os dados de acesso.
Excluir Templates de Fotos de Usuários	Para excluir todos os templates de fotos de usuários no dispositivo.

Apagar foto do usuário	Para apagar todas as fotos do usuário no dispositivo.
Apagar papel de parede	Para apagar todos os papéis de parede no dispositivo.
Apagar proteção de tela	Para apagar os protetores de tela no dispositivo.

O usuário poderá selecionar **Apagar Tudo** ou **Apagar por Faixa de Horário** quando quiser apagar os registros de acesso, fotos de ponto ou fotos listas de bloqueio. Selecionando **Apagar por intervalo de tempo**, você precisa definir um intervalo de tempo específico para apagar todos os dados dentro de um período específico.

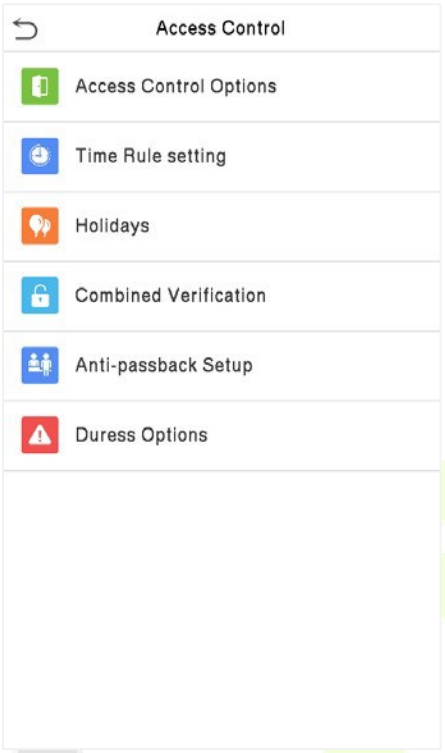


Selecione Excluir por Intervalo de Tempo.

Configure o intervalo de tempo e toque em OK.

11 Controle de acesso

No **Menu Principal**, toque em **Controle de Acesso** você poderá definir o tempo de abertura de portas, controle de fechaduras e configurar outros parâmetros relacionados ao controle de acesso.

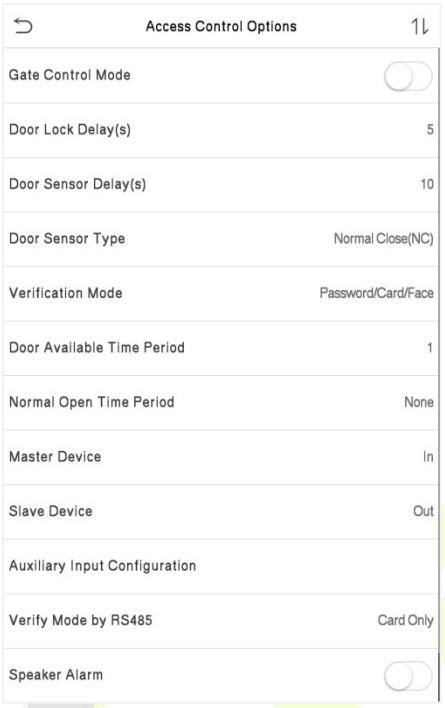


Para ter uma autenticação válida, o usuário cadastrado deve atender às seguintes condições:

- O tempo atual de desbloqueio da porta deve estar dentro de qualquer fuso horário válido do período de tempo do usuário.
- O grupo do usuário já deve estar definido na combinação de desbloqueio da porta (e se houver outros grupos, sendo configurados na mesma regra de acesso, também é necessária a verificação dos membros desse grupo para destravar a porta).
- Na configuração padrão, os novos usuários são alocados no primeiro grupo com o fuso horário do grupo padrão, onde a regra de acesso é "1" e é definida no estado de desbloqueio por padrão.

11.1 Opções de controle de acesso

Acesse as **Opções de Controle de Acesso** na interface de **Controle de Acesso** para definir os parâmetros do bloqueio de controle do terminal e equipamentos relacionados.



Função	Descrição
Modo de controle de portão/catraca	Alterne entre ON ou OFF para entrar no modo de controle do portão ou não. Quando definido como LIGADO, nesta interface removerá as opções de relé de trava de porta, sensor de porta e tipo de sensor de porta.
Tempo de trava (s)	Tempo de acionamento do relé após uma autenticação válida. Valor válido: 1~10 segundos; 0 segundo representa função desativada.
Atraso do sensor da porta (s)	Se a porta não estiver travada e for deixada aberta por um determinado período (Atraso do sensor da porta), um alarme será acionado. O valor válido do Atraso do Sensor da Porta varia de 1 a 255 segundos.
Tipo de sensor de porta	Existem três opções de Sensores: **Nenhum, Normal Aberto** e **Normal Fechado.** **Nenhum**: significa que o sensor da porta não está em uso. **Normal Aberta**: Com a porta fechada, o equipamento espera um sinal aberto. **Normal Fechado**: Com a porta fechada, o equipamento espera um sinal fechado.

Modo de verificação	Os modos de verificação suportados incluem Senha/Cartão/Rosto, Somente ID do Usuário, Somente Senha, Somente Cartão, Senha + Cartão, Senha/Cartão, Somente Rosto, Rosto + Senha e Rosto + Cartão.
Tempo de acionamento da porta	Para definir o período de tempo para a porta, para que a porta esteja disponível apenas durante esse período.
Período de tempo normalmente aberto	Período de tempo programado para o modo "Normal Aberto", para que a porta fique sempre aberta 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.
Dispositivo auxiliar	Ao configurar o equipamento auxiliar, 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	Define o período de tempo de destravamento da porta e o tipo de saída auxiliar do dispositivo terminal auxiliar. Os tipos de saída auxiliar incluem "Nenhum", "Acionamento da porta", "Acionamento de alarme" e "Acionamento de porta e alarme".
Modo de Verificação por RS485	Esse modo de verificação é utilizado quando o dispositivo é usado tanto como hospedeiro quanto como auxiliar. Tal modo de verificação inclui Apenas Cartão e Cartão + Senha.
Alarme	Emite um alarme sonoro. Quando a porta estiver fechada ou a verificação for bem-sucedida, o sistema cancelará o alarme do local.
Redefinir Configurações de Acesso	Os parâmetros de redefinição do controle de acesso incluem atraso na fechadura da porta, atraso do sensor da porta, tipo de sensor da porta, modo de verificação, período de disponibilidade da porta, período de abertura normal, dispositivo principal e alarme. No entanto, os dados do controle de acesso apagados no Gerenciamento de Dados estão excluídos.

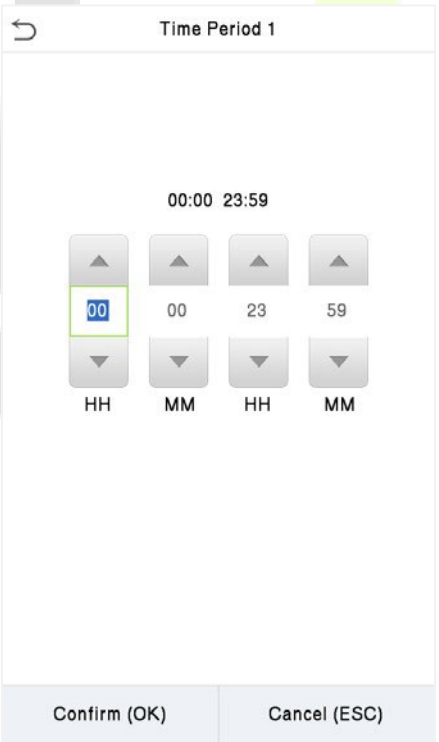
11.2 Configuração de regra de tempo

Toque em **Configuração de Regra de Tempo** na interface de controle de acesso para definir as configurações de tempo.

- O equipamento permite definir até 50 períodos de tempo.
- Cada período de tempo representa 10 faixas horárias, ou seja, 1 semana e 3 feriados, e cada faixa horária possui um período padrão de 24 horas por dia. O usuário só pode verificar dentro do período de tempo válido.
- Pode-se definir um máximo de 3 períodos de tempo para cada faixa horária. A relação entre esses períodos de tempo é "OU". Assim, quando o tempo de verificação cair em qualquer um desses períodos de tempo, a verificação é válida.
- O formato de faixa horária de cada período de tempo: HH MM-HH MM, de acordo com o relógio de 24 horas.

Toque na caixa cinza para pesquisar a faixa horária e especifique o número da faixa horária (Limite: até 50 faixas).

Na interface do número da faixa horária selecionada, toque no dia desejado (segunda-feira, terça-feira, etc.) para definir a hora.



Especifique a hora de início e de término e toque em **OK**.

Observação:

1) Quando o horário de término é anterior ao horário de início (como 23:57~23:56), indica que o acesso está proibido o dia todo.
2) Quando a hora de término for posterior à hora de início (como 00:00~23:59), isso indica que o intervalo é válido.
3) O período de tempo efetivo para manter a porta desbloqueada ou aberta o dia todo é (00:00~23:59) ou também quando a hora de término é posterior à hora de início (como 08:00~23:59) .
4) A faixa horária padrão 1 indica que a porta está aberta o dia todo.

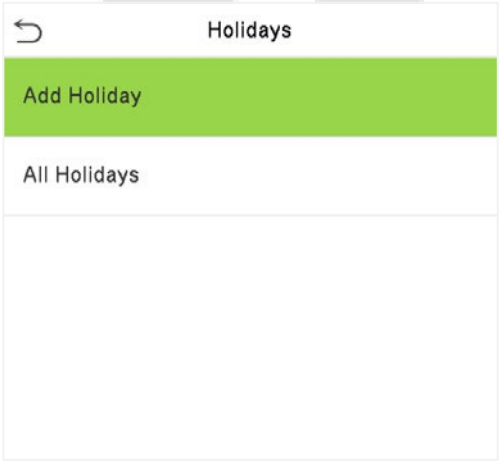
11.3 Feriados

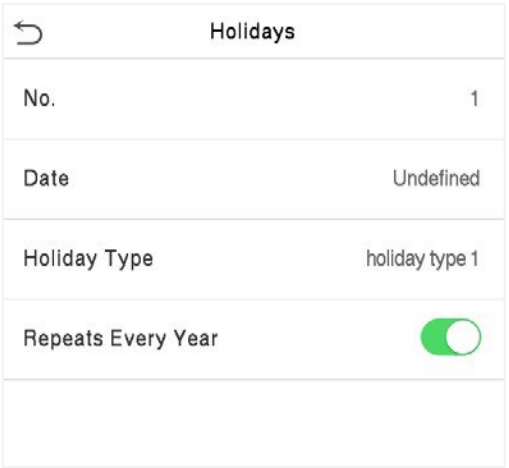
Sempre que houver feriado, poderá necessitar de um horário de acesso especial; mas alterar o horário de acesso de todos um por um é extremamente complicado, então você pode definir um horário de acesso de feriado que seja aplicável a todos os funcionários, e o usuário poderá abrir a porta durante os feriados.

Toque em **Feriados** na interface de **Controle de Acesso** para definir o acesso em Feriados

- **Adicionar um novo feriado**

Toque em **Adicionar Feriado** na interface de **Feriados** e defina os parâmetros.





- **Editar um feriado**

  Na interface **Feriados**, selecione um item de feriado a ser modificado. Toque em **Editar** para modificar os parâmetros de feriados.

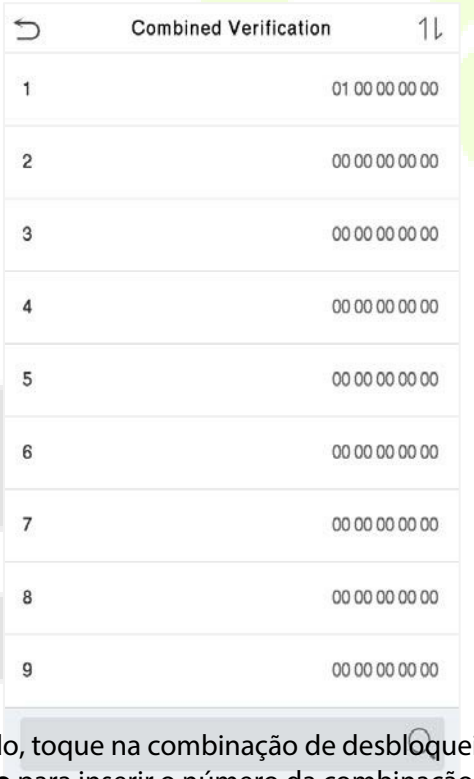
- **Excluir um feriado**

  Na interface de **Feriados**, selecione um item de feriado a ser excluído e toque em **Apagar**. Pressione **OK** para confirmar a exclusão. Após a exclusão, este feriado não é mais exibido na interface Todos os feriados.

11.4 Acesso combinado

Os grupos de acesso são organizados em diferentes combinações de desbloqueio de portas para obter várias verificações e aumentar a segurança. Em uma combinação de destravamento de porta, a faixa do número combinado N é: 0 ≤ N ≤ 5, o número de membros N pode pertencer a um grupo de acesso ou pode pertencer a cinco grupos de acesso diferentes.

Toque em Acesso combinado na interface de Controle de Acesso para definir a configuração.



Na interface de acesso combinado, toque na combinação de desbloqueio da porta a ser definida e toque no botão **para cima** e **para baixo** para inserir o número da combinação e pressione **OK**.

Por exemplo:

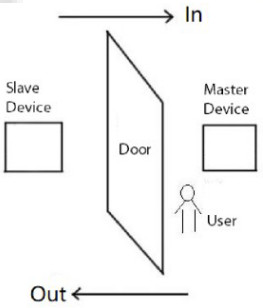
- A combinação de destravamento da porta 1 é definida como (01 03 05 06 08), indicando que a combinação de desbloqueio 1 é composta por 5 pessoas, e os 5 indivíduos são de 5 grupos. Grupo de Controle de Acesso 1, grupo AC 1, Grupo AC 3, grupo AC 5, grupo AC 6 e grupo AC 8, respectivamente.
- A combinação de destravamento da porta 2 é configurada como (02 02 04 04 07), indicando que a combinação de destravamento 2 é composta por 5 pessoas; os dois primeiros são do grupo AC 2, os dois seguintes são do grupo AC 4 e a última pessoa é do grupo AC 7.
- A combinação de destravamento da porta 3 é configurada como (09 09 09 09 09), indicando que há 5 pessoas nesta combinação; todos são do grupo AC 9.
- A combinação de destravamento da porta 4 é definida como (03 05 08 00 00), indicando que a combinação de destravamento 4 é composta por apenas três pessoas. A primeira pessoa é do grupo AC 3, a segunda pessoa é do grupo AC 5 e a terceira pessoa é do grupo AC 8.

Observação: Defina todas as combinações de desbloqueio de porta para 0 se desejar excluir combinações de desbloqueio de porta.

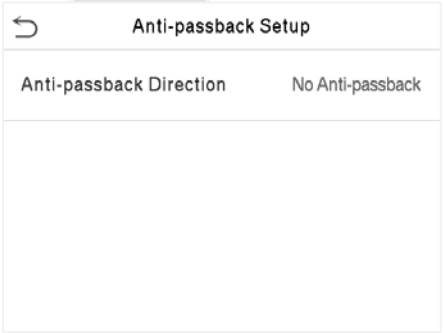
11.5 Anti-Passback

É possível que os usuários sejam seguidos por algumas pessoas para entrar na porta sem verificação, resultando em uma violação de segurança. Assim, para evitar tal situação, foi desenvolvida a opção Anti-Passback. Uma vez habilitado, o registro de check-in deve coincidir com o registro de check-out para abrir a porta.

Esta função requer que dois dispositivos funcionem juntos: um é instalado dentro da porta (dispositivo mestre) e o outro é instalado fora da porta (dispositivo escravo). Os dois dispositivos se comunicam através do sinal Wiegand. O formato Wiegand e o tipo de saída (ID do usuário / número do cartão) adotados pelo dispositivo mestre e pelo dispositivo escravo devem ser iguais.



Toque em **Configuração de Anti-Passback** na interface de **Controle de Acesso**.

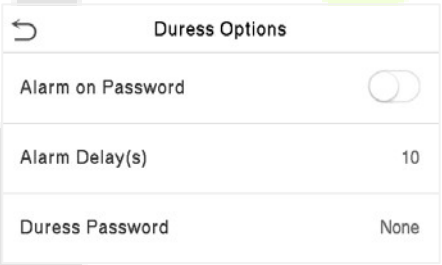


Função	Descrição
Direção anti-passback	**Sem Anti-Passback:** A função de Anti-Passback está desativada, o que significa que a verificação bem-sucedida através do dispositivo principal ou dispositivo escravo pode destrancar a porta. O estado de presença não é salvo nessa opção. **Anti-passback de saída:** O usuário só pode fazer o check-out se o último registro for um registro de check-in; caso contrário, um alarme é acionado. No entanto, o usuário pode fazer o check-in livremente. **Anti-passback de entrada:** O usuário só pode fazer o check-in novamente se o último registro for um registro de check-out; caso contrário, um alarme é acionado. No entanto, o usuário pode fazer o check-out livremente. **Anti-passback de entrada/saída:** Nesse caso, um usuário só pode fazer o check-in se o último registro for um check-out, ou o usuário só pode fazer o check-out se o último registro for um check-in; caso contrário, o alarme é acionado.

11.6 Opções de Coação

Uma vez que um usuário ativar a função de verificação por coação com método(s) de autenticação específico(s), e quando ele estiver sob coação e se autenticar usando verificação de coação, o dispositivo irá destravar a porta normalmente, mas ao mesmo tempo, um sinal será enviado para acionar o alarme.

Na interface de **controle de acesso**, toque em **Opções de Coação** para definir as configurações de coação.

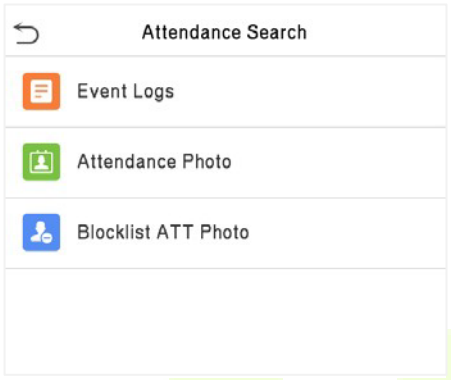


Nome da função	Descrição
Senha de alarme	Quando um usuário usa o método de verificação de senha, um sinal de alarme será gerado somente quando a verificação de senha for bem-sucedida, caso contrário não haverá sinal de alarme.
Atraso do Alarme (s)	O sinal de alarme não será transmitido até que o tempo de atraso do alarme tenha decorrido. O valor varia de 1 a 999 segundos.
Senha de coação	Defina a senha de coação de 6 dígitos. Quando o usuário digitar essa senha de coação para verificação, um sinal de alarme será gerado.

12 Procurar registros

Assim que a autenticação de um usuário for validada, os logs de eventos serão salvos no dispositivo. Esta função permite que os usuários verifiquem seus registros de acesso.

Clique em **Procurar registros** na interface do **Menu Principal** para pesquisar o registro de Acesso/Presença necessário.

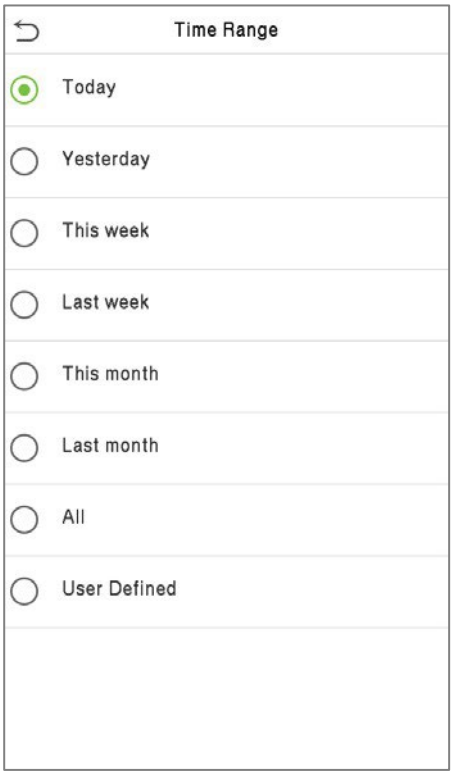


O processo de pesquisa de fotos de presença e lista de bloqueio é semelhante ao da pesquisa de logs de eventos. Veja a seguir um exemplo de pesquisa de logs de eventos.

Na interface de **Reg. acesso**, toque em **Logs de eventos** para pesquisar o registro necessário.

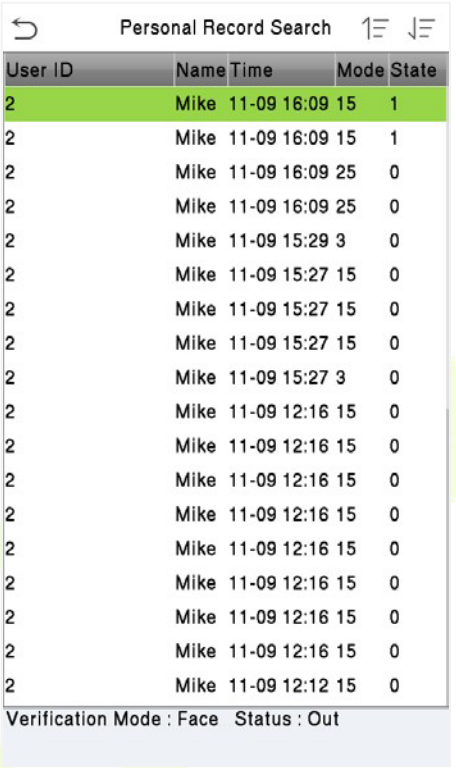
1. Insira o ID do usuário a ser pesquisado e clique em OK. Se desejar pesquisar logs de todos os usuários, clique em OK sem inserir nenhum ID de usuário.

2. Selecione o intervalo de tempo em que os logs precisam ser pesquisados.



3. Depois que a pesquisa de log for bem-sucedida. Toque no registro destacado em verde para visualizar seus detalhes.

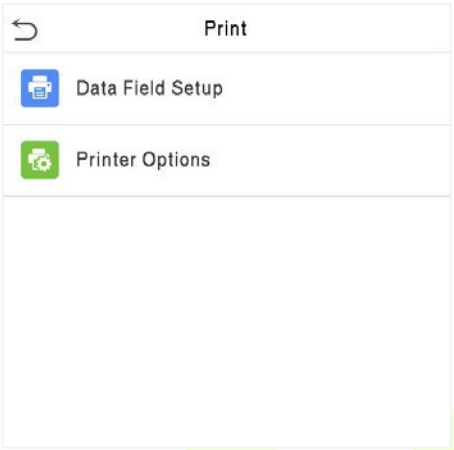
4. A figura abaixo mostra os detalhes do log selecionado.



13 Configurações de Impressão

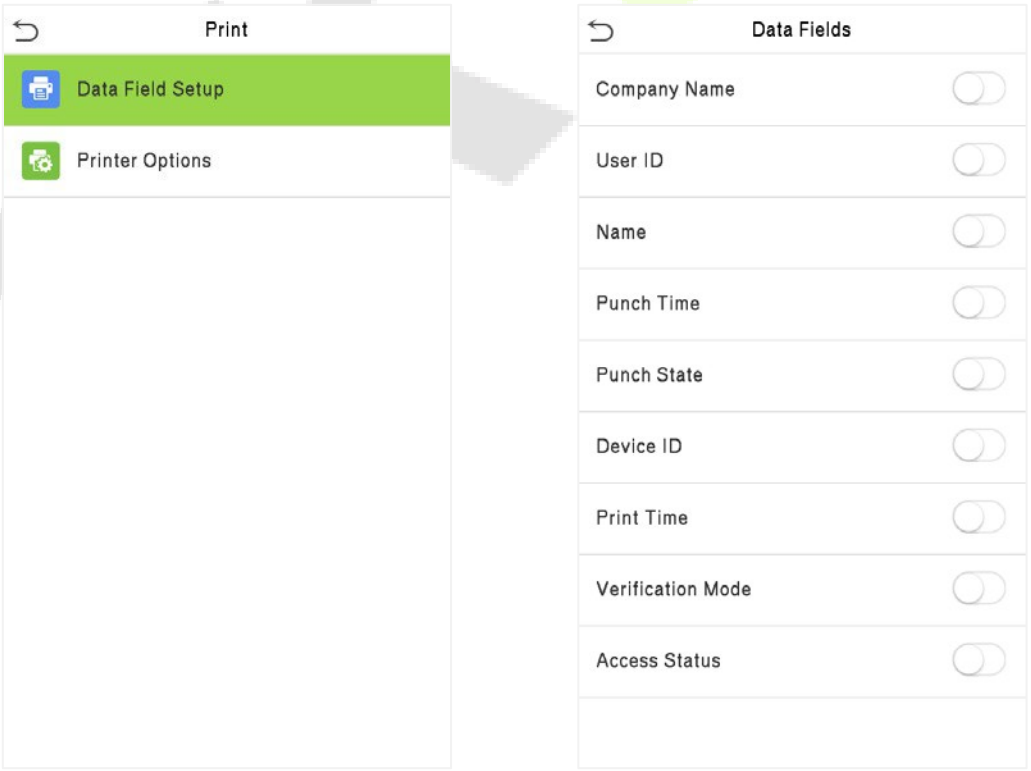
Dispositivos com função de impressão podem imprimir registros de presença quando uma impressora está conectada (essa função é opcional e implementada apenas em alguns produtos).

Toque em **Imprimir** na interface do **Menu Principal**.



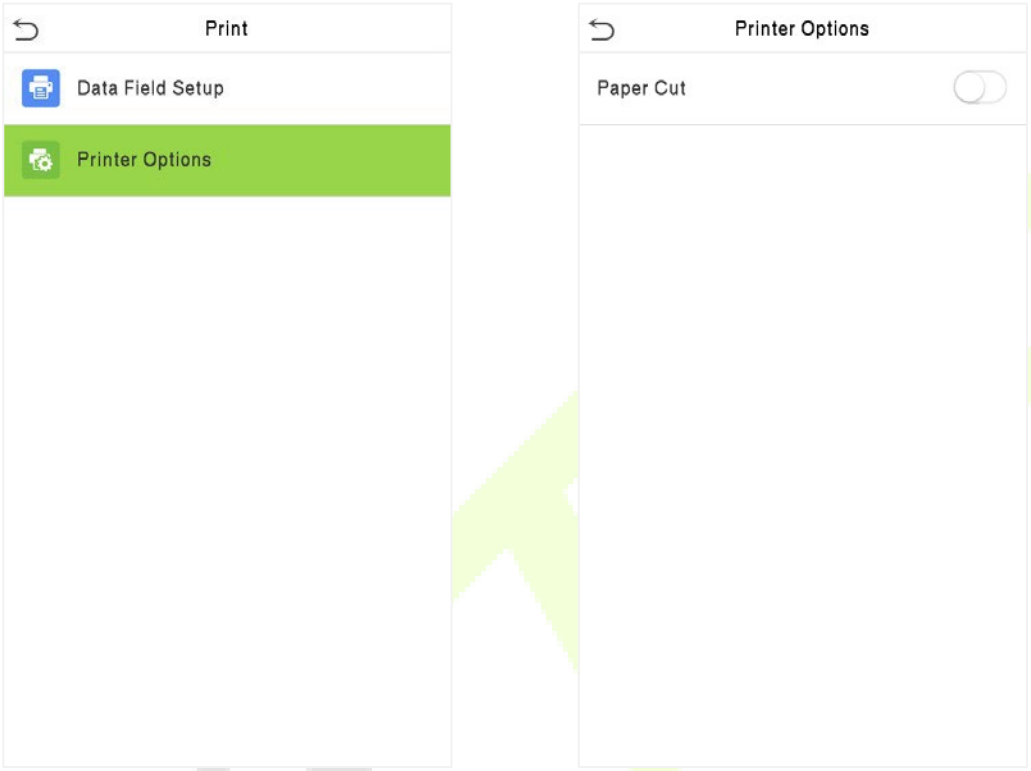
13.1 Configurações de Campos de Dados para Impressão

Selecione **Configuração de Campos de Dados** na interface de **impressão**. Alterne o botão para ligar/desligar os campos que requerem impressão.



13.2 Configurações de Opções de Impressão

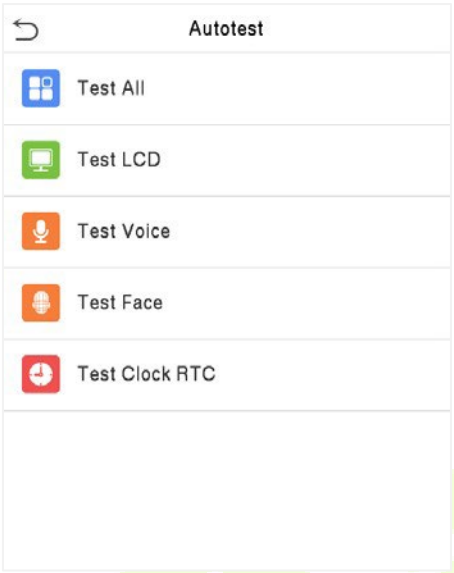
Selecione **Opções da Impressora** na interface de impressão. Alterne o botão para habilitar ou desabilitar a função de Corte de Papel.



Observações: Para ativar a função de Corte de Papel, é necessário conectar o dispositivo a uma impressora com função de corte de papel, para que a impressora corte os papéis de acordo com as informações de impressão selecionadas durante a impressão.

14 Auto teste

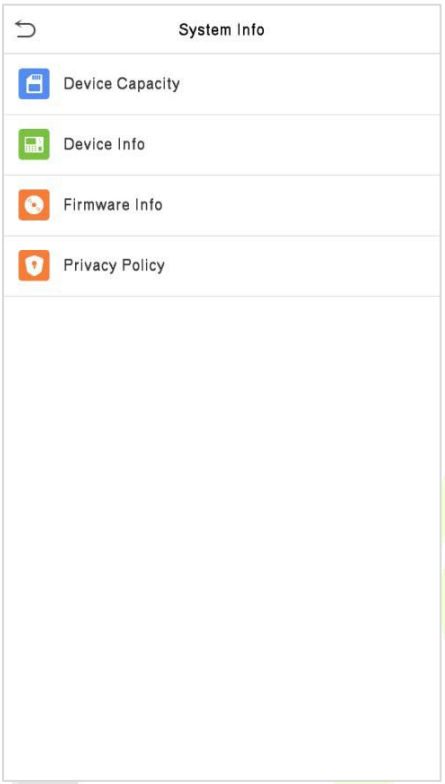
No **Menu Principal**, toque em **Auto teste** para testar automaticamente se todos os módulos do dispositivo funcionam corretamente, incluindo LCD, áudio, câmera e relógio em tempo real (RTC).



Menu	Descrição
Testar tudo	Para testar automaticamente se o LCD, áudio, câmera e relógio em tempo real (RTC) estão normais.
Testar LCD	Para testar automaticamente a tela LCD exibindo cores, diferentes para verificar se a tela exibe as cores normalmente.
Testar áudio	Para testar automaticamente se os arquivos de áudio armazenados no dispositivo estão completos e se a qualidade da voz é boa.
Testar de câmera	Para testar se a câmera funciona corretamente, verificando as fotos tiradas estão claras o suficiente.
Testar relógio	Para testar o RTC. O dispositivo testa se o relógio funciona normalmente e com precisão com um cronômetro. Toque na tela para começar a contar e pressione-o novamente para parar de contar.

15 Informação do sistema

No **Menu Principal**, toque em **Informações do Sistema** para visualizar o status do armazenamento, as informações da versão do dispositivo e as informações do firmware.



Nome da função	Descrição
Capacidade do dispositivo	Exibe o armazenamento atual do usuário do dispositivo, armazenamento de cartões, senhas e rostos, administradores, registros, fotos de presença e lista de bloqueio, e fotos de perfil.
Informação do dispositivo	Exibe o nome do dispositivo, número de série, endereço MAC, algoritmo de reconhecimento facial, informações da plataforma, versão do MCU, fabricante e data de fabricação.
Informações de firmware	Exibe a versão do firmware e outras informações de versão do dispositivo.
Política de Privacidade	Exibe a política de privacidade do dispositivo.

16 Conectar ao Software ZKBioSecurity

16.1 Configurar o Endereço de Comunicação

- **Lado do Dispositivo**

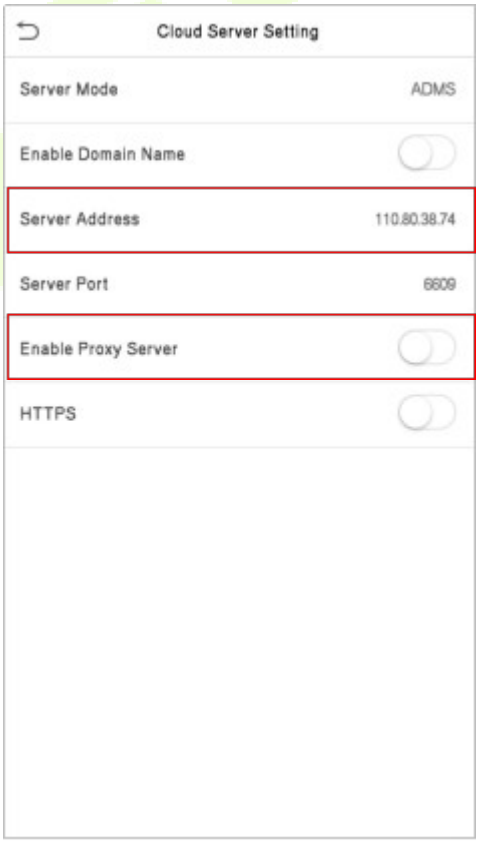
1. Toque em **Configurações do Sistema** > **Configurações de Rede** > **Configurações TCP/IP** no menu principal para definir o endereço IP e o gateway do dispositivo.

   (**OBSERVAÇÃO**: O endereço IP deve ser capaz de se comunicar com o servidor ZKBioSecurity, preferencialmente no mesmo segmento de rede do endereço do servidor.)

2. No menu principal, clique em **Configurações do Sistema > Configurações do Servidor Cloud** para definir 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 ZKBioSecurity (O padrão é 6609).



- **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:

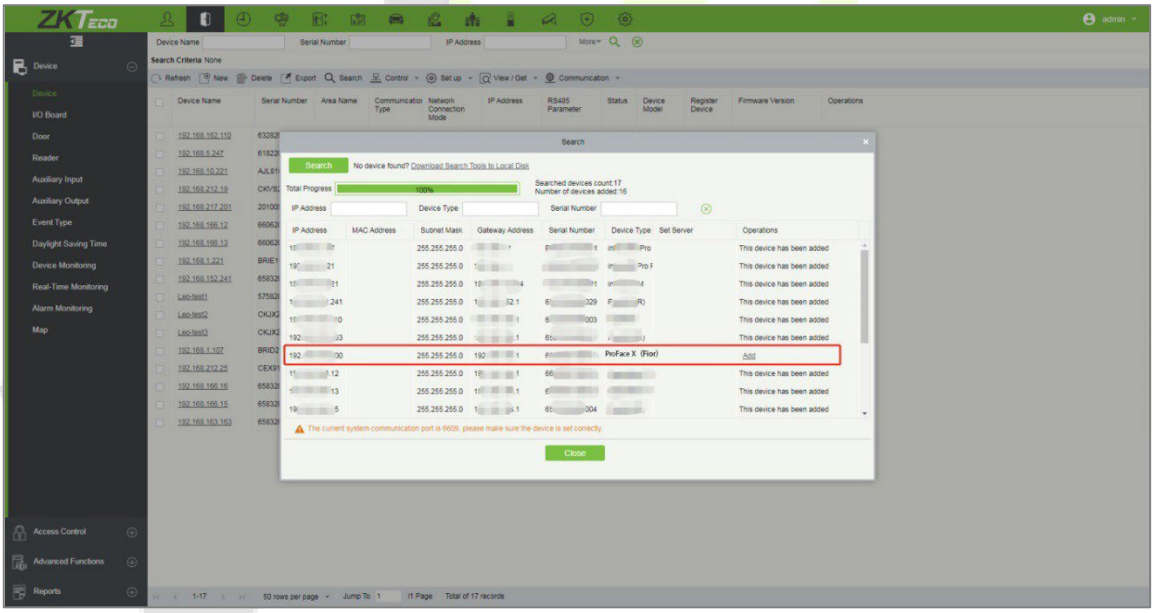
16.2 Adicionar Dispositivo no Software

Adicione o dispositivo realizando uma busca. O processo é o seguinte:

1) Clique em **Acesso** > **Dispositivo** > **Busca** para abrir a interface de busca no software.

2) Clique em **Busca** e ele exibirá a mensagem [Buscando...].

3) Após a busca, a lista com o número total de controladores de acesso será exibida.

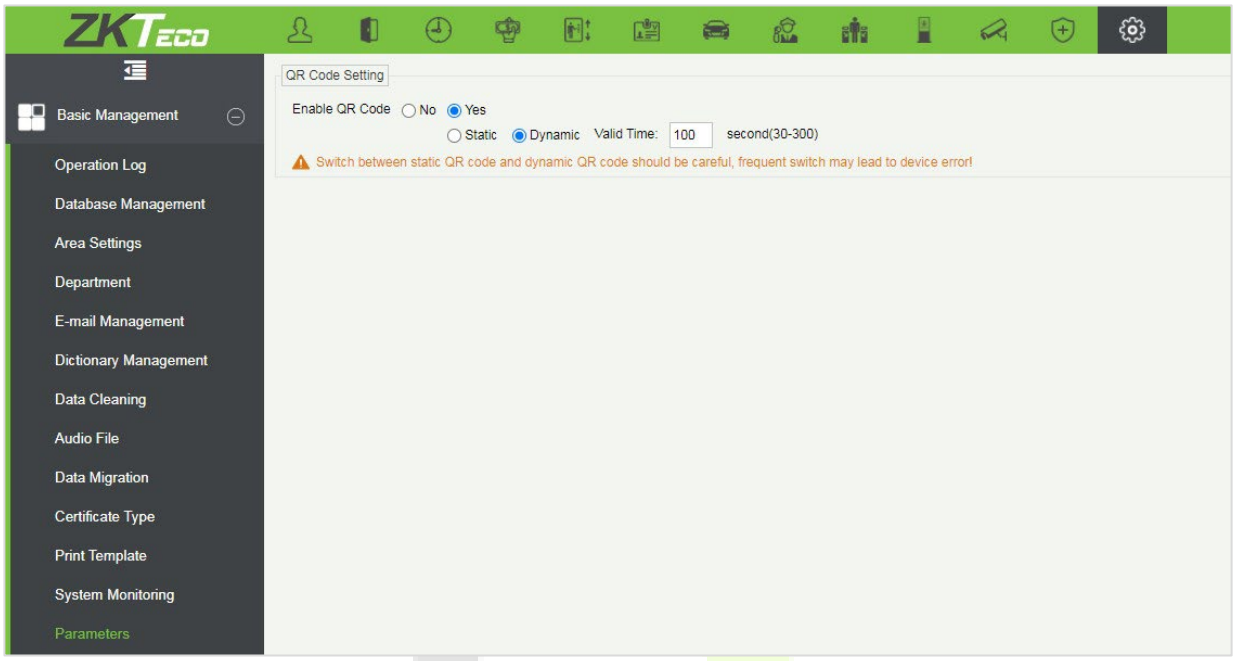


4) Clique em **[Adicionar]** na coluna de operações, uma nova janela será aberta. Selecione o tipo de ícone, área e adicione ao nível em cada menu suspenso e clique em **[OK]** para adicionar o dispositivo.

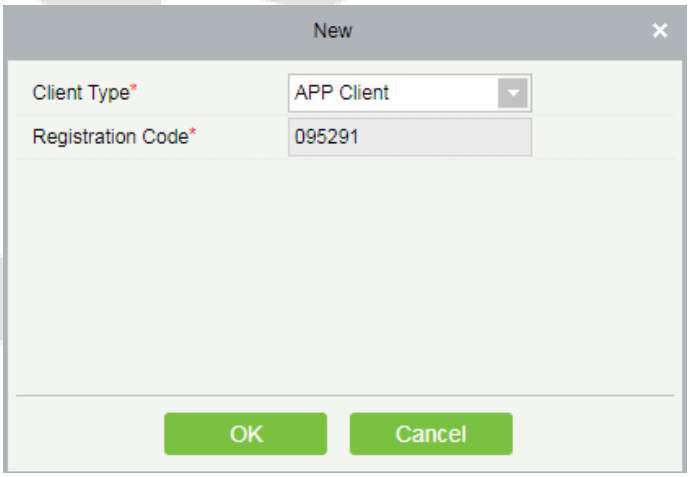
16.3 Credencial Móvel

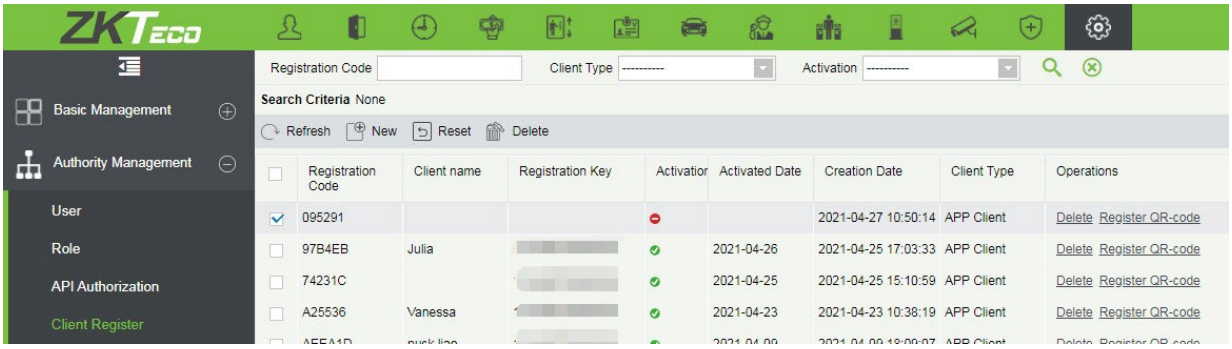
Após baixar e instalar o aplicativo, o usuário precisa configurar o servidor antes de fazer login. Os passos são os seguintes:

1. Em **[Sistema]** > **[Gerenciamento Básico]** > **[Parâmetros]**, defina "**Habilitar Código QR**" para "**Sim**" e selecione o status do código QR de acordo com a situação atual. O padrão é dinâmico, o tempo de validade do código QR pode ser definido.

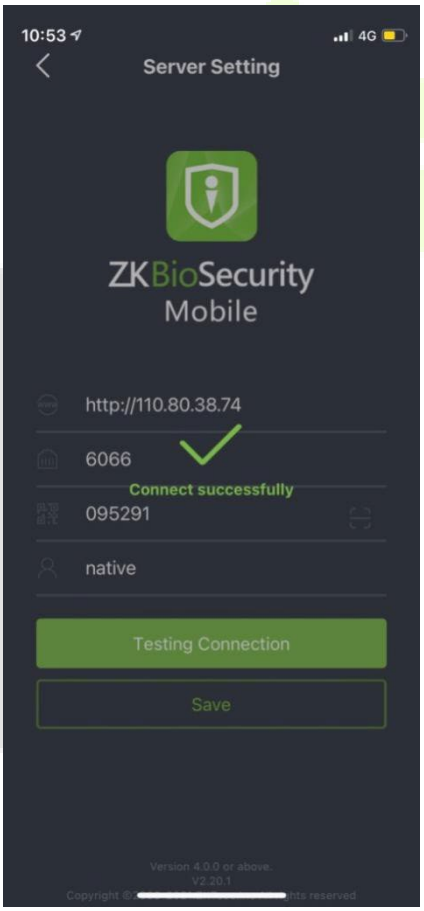


2. No servidor, escolha [**Sistema**] > [**Gerenciamento de Autoridade**] > [**Registro do Cliente**] para adicionar um cliente de aplicativo registrado.





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, juntamente com o número da porta.
4. Toque no **ícone de Código QR** para escanear o código QR do novo cliente do aplicativo. Após a identificação bem-sucedida do cliente, defina o nome do cliente e toque em **[Teste de Conexão]**.
5. Após a conexão de rede ser estabelecida com sucesso, toque em **[Salvar]**.

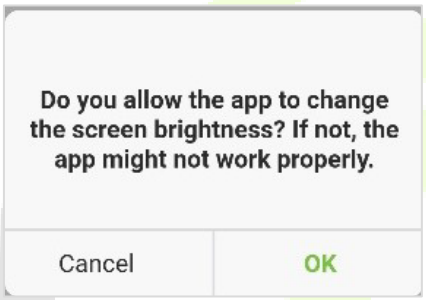


A função de Credencial Móvel só é válida ao fazer login como funcionário. Toque em **Funcionário** para alternar para a tela de login do funcionário. Digite o ID do Funcionário e a senha (Padrão: 123456) para fazer o login.

6. Toque em **[Credencial Móvel]** no aplicativo e um código QR será exibido, contendo informações do ID do funcionário e 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 autenticação sem contato e abrir a porta.

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



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

Observação: Para outras operações específicas, consulte o Manual do Usuário do ZKBioSecurity Mobile App.

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) A resolução deve estar entre 358 x 441 a 1080 x 1920.
4) A escala vertical da cabeça e do corpo deve estar na proporção de 2:1.
5) A foto deve incluir os ombros da pessoa capturada no mesmo nível horizontal.
6) Os olhos da pessoa capturada devem estar abertos e com a íris claramente visível.
7) Rosto ou sorriso simples são recomendados, sorriso excessivo mostrando os dentes não é recomendado.
8) 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) 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. 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