Manual do usuário

SpeedFace-V3L

Data: Agosto de 2023

Versão: 1.3

Português

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

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

Sem o consentimento prévio por escrito da ZKTeco, nenhuma parte deste manual pode ser copiada ou utilizada de qualquer forma ou formato. Os direitos de propriedade intelectual sobre este manual pertencem à ZKTeco e suas subsidiárias (doravante a "Empresa" ou "ZKTeco").

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

Fax +86 755 - 89602394

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

A ZKTeco é uma dos maiores fabricantes mundiais de leitores RFID e biométricos (Cartão, Facial, Veia do dedo). As ofertas de produtos incluem leitores e painéis de controle de acesso, câmeras de reconhecimento facial de alcance próximo e distante, controladores de acesso para elevadores/andares, catracas, controladores de portão de Reconhecimento de Placas de Veículos (LPR) e produtos de consumo, incluindo fechaduras de porta com leitor de cartão e reconhecimento facial operadas por bateria. Nossas soluções de segurança são multilíngues e localizadas em mais de 18 idiomas diferentes. Na instalação de fabricação ISO9001 certificada de última geração da ZKTeco, com 700.000 pés quadrados, controlamos a fabricação, o design de produtos, a montagem de componentes e a logística/envio, tudo sob o mesmo teto.

Os fundadores da ZKTeco têm se dedicado à pesquisa independente e ao desenvolvimento de procedimentos de autenticação biométrica e à criação de produtos baseados em SDK de autenticação biométrica, que inicialmente foram amplamente aplicados em segurança de PC e autenticação de identidade. Com o contínuo aprimoramento do desenvolvimento e diversas aplicações de mercado, a equipe gradualmente construiu um ecossistema de autenticação de identidade e um ecossistema de segurança inteligente, ambos baseados em técnicas de autenticação biométrica. Com anos de experiência na industrialização de verificações biométricas, a ZKTeco foi oficialmente estabelecida em 2007 e agora é uma das principais empresas do mundo no setor de autenticação biométrica, detendo várias patentes e sendo selecionada como Empresa Nacional de Alta Tecnologia por 6 anos consecutivos. Seus produtos são protegidos por direitos de propriedade intelectual.

Sobre o Manual

Este manual apresenta as operações do SpeedFace-V3L.

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

Recursos e parâmetros marcados com ★não estão disponíveis em todos os dispositivos.

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

ANATEL
16686-23-12720

Módulo: ITM-UB41-S20PXX0000NV1
"Incorpora produto homologado pela ANATEL sob número 16686-23-12720"

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

Convenções de Documentos

As convenções usadas neste manual estão listadas abaixo:

Convenções de Interface Gráfica

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 apenas as peças de reposição fornecidas pelo fornecedor. Substituições não autorizadas podem resultar em risco de queimaduras, choques ou outros perigos.

8. **Verificação de segurança**– Ao concluir o serviço ou reparo no dispositivo, peça ao técnico de serviço que realize verificações de segurança para garantir o funcionamento adequado do aparelho.

9. **Fontes de alimentação**– Opere o sistema apenas a partir da fonte de alimentação indicada na etiqueta. Se não estiver claro qual tipo de fonte de alimentação usar, 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 surtos de energia danifiquem o sistema.

Recomenda-se instalar os dispositivos em áreas com acesso limitado.

2 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.

3 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.
- 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:

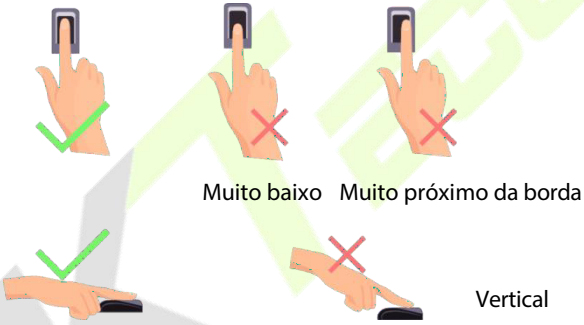
1) Certifique-se se a polaridade positiva e negativa do adaptador CA de 12V CC está conectada corretamente. Uma conexão reversa pode danificar o dispositivo. Não é aconselhável conectar o adaptador CA de 24V à porta de entrada de CC de 12V.
2) Certifique-se de conectar os fios seguindo a polaridade positiva e negativa indicada na placa de identificação do dispositivo.
3) 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.

4 Instruções de Uso

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

4.1 Posicionamento dos dedos

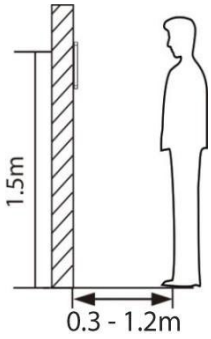
Dedos recomendados: Indicador, médio ou anelar; evite usar o polegar ou o mindinho, pois é difícil pressioná-los com precisão no leitor de impressões digitais.



Observação: Por favor, utilize o método correto ao pressionar seus dedos no leitor de impressões digitais para registro e identificação. Nossa empresa não assume nenhuma responsabilidade por problemas de reconhecimento que possam resultar do uso incorreto do produto. Reservamos o direito de interpretação final e modificação em relação a este ponto

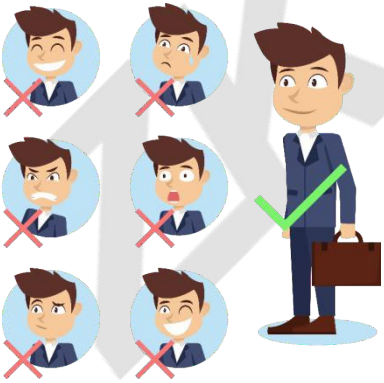
4.2 Posição em Pé, Expressão Facial e Postura em Pé

➢ **Distância recomendada**

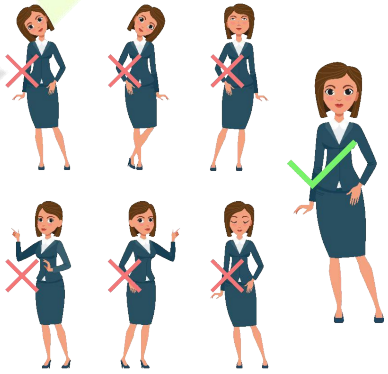


A distância recomendada entre o dispositivo e um usuário cuja altura esteja na faixa de 1,55m a 1,85m é de 0,3 a 2,5m. Os usuários podem se mover ligeiramente para frente ou para trás para melhorar a qualidade das imagens faciais capturadas.

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



Expressão Facial



Postura em pé

Observação: Por favor, mantenha sua expressão facial e postura em pé naturais durante o registro ou verificação.

4.3 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

- **Recomendações para cadastro de face**
  - 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.

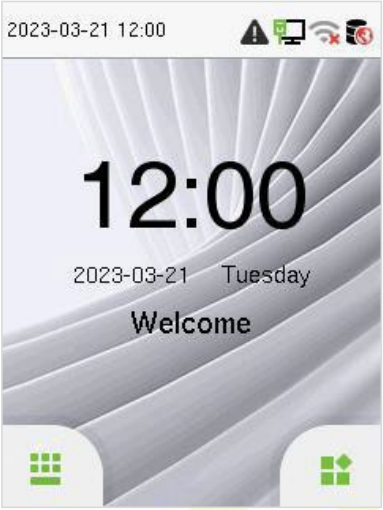
- Tenha cuidado para não exibir duas faces na tela. Cadastre uma pessoa por vez.
- Recomenda-se que um usuário que utilize óculos cadastre ambas as faces, com e sem óculos.

➢ **Recomendações para autenticar uma face**

- Certifique-se de que a face apareça dentro da linha 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.

4.4 Tela principal

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

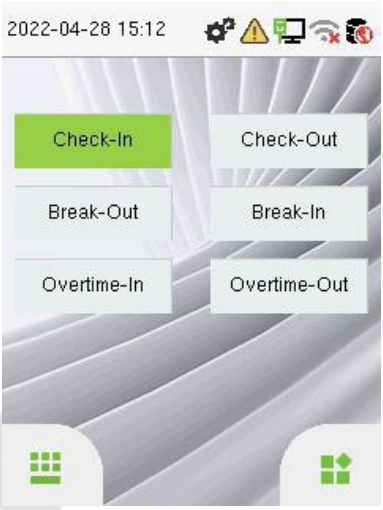


- Clique em para acessar a interface de entrada do ID do usuário.
- Quando não houver um Super Administrador configurado no dispositivo, toque para acessar o menu.
- Após adicionar um Super Administrador ao dispositivo, é necessário verificar o Super Administrador antes de abrir as funções do menu.

Observação:

Para a segurança do dispositivo, é recomendado registrar um super administrador na primeira vez que você utilizar o dispositivo.

- As opções de estado de registro também podem ser exibidas e usadas diretamente na interface de espera. Toque em qualquer lugar da tela, exceto nos ícones, e seis teclas de atalho aparecem na tela, conforme mostrado na figura abaixo:



- Pressione a tecla correspondente ao estado de presença desejado para selecionar o seu estado de presença atual, que será exibido em verde. Consulte "Mapeamento de Teclas de Atalho" para obter o método de operação específico.

Observação:

As opções de estado de registro estão desativadas por padrão e é necessário selecionar outras opções de modo em **Personalizar** > **Opção de Estado de Registro** para obter as opções de estado de registro na tela de espera.

4.5 Teclado Virtual

Observação:

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

- Toque em **[EN]** para alternar para o teclado numérico.
- Pressione **[123]** para alternar para o teclado de símbolos.
- Toque em **[@#&]** para voltar ao teclado em inglês.
- Toque em **[ ]** para sair do teclado virtual.

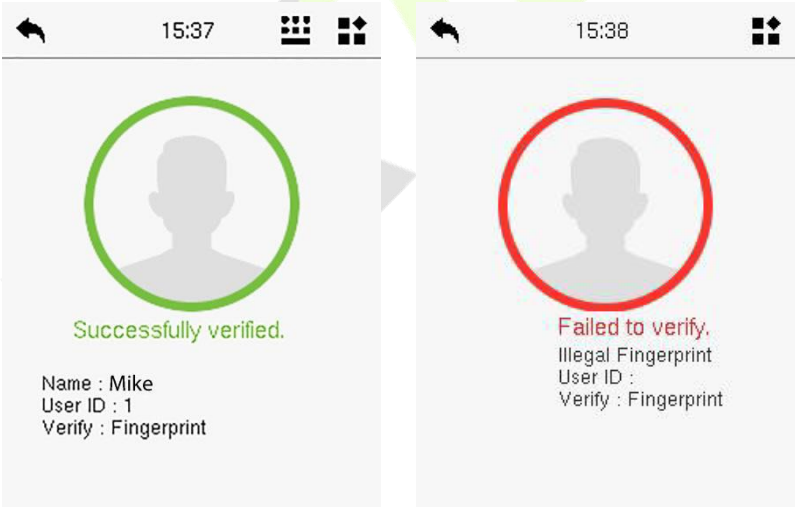
4.6 Modo de Autenticação

4.6.1 Autenticação de Impressão Digital

- **Autenticação de Impressão Digital 1:N**

Compara a impressão digital que está sendo pressionada no leitor de impressões digitais com todos os dados de impressões digitais armazenados no dispositivo. O dispositivo entra no modo de autenticação por impressão digital quando um usuário pressiona o dedo no scanner de impressões digitais. Por favor, siga a maneira correta de posicionar o dedo sobre o sensor. Para mais detalhes, consulte a seção Posicionamento do Dedo.

Verificação bem-sucedida: Verificação falhou:



- **Modo de Verificação de Impressão Digital 1:1**

Compara a impressão digital que está sendo pressionada no leitor de impressões digitais com as impressões digitais que estão vinculadas à entrada do ID do usuário através do teclado virtual.

Os usuários podem verificar suas identidades com o modo de verificação 1:1 quando não conseguem obter acesso com o método de autenticação 1:N.

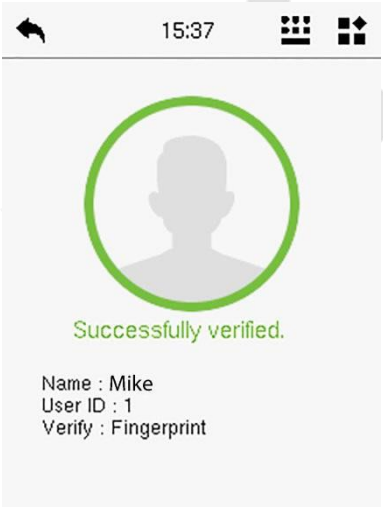
Pressione na interface principal e entre no modo de verificação de impressão digital 1:1.

Digite o ID do usuário e pressione **[OK]**.

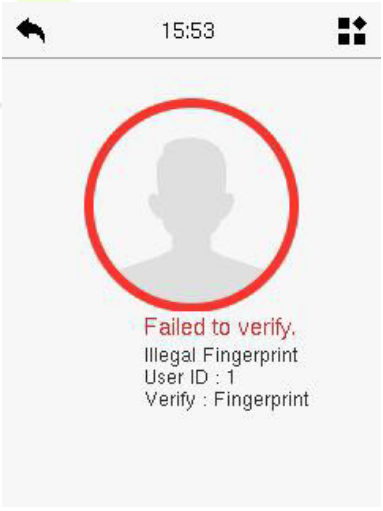
Se um funcionário registrar um modelo facial, senha e cartão, além da impressão digital, a seguinte tela aparecerá. Selecione o ícone para entrar no modo de verificação de impressão digital.

Pressione a impressão digital para verificar.

Verificação bem-sucedida:



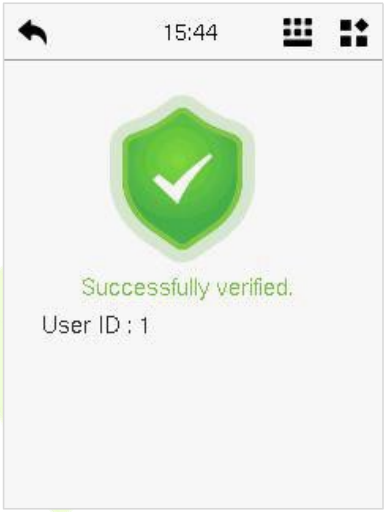
Verificação falhou:



4.6.2 Autenticação facial

- **Modo de Autenticação Facial 1:N**

  Ele compara as imagens faciais adquiridas com todos os templates faciais registrados no dispositivo. A seguir está a caixa de diálogo de prompt de resultados de comparação.

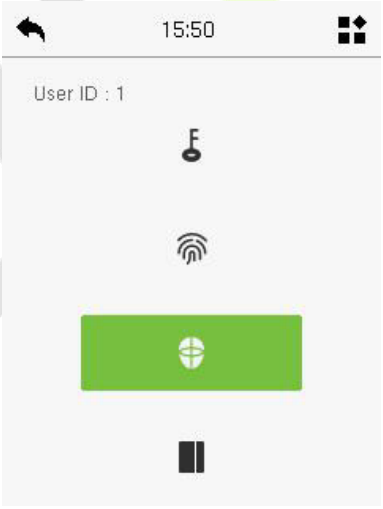


- **Modo de Autenticação Facial 1:1**

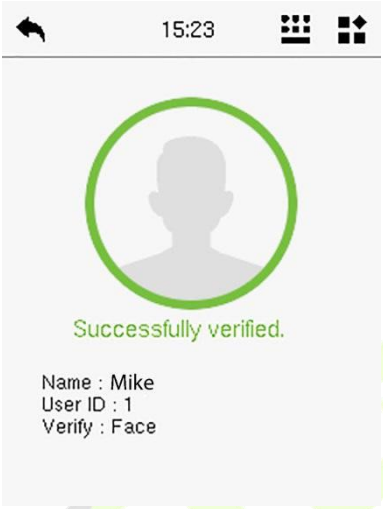
  Compara o rosto capturado pela câmera com o modelo facial relacionado ao ID de usuário inserido.

  Toque na interface principal e entre no modo de autenticação facial 1:1. Digite o ID do usuário e clique em **[OK]**.

Se um funcionário registrar senha e cartão além da face, a seguinte tela será exibida. Selecione o ícone para entrar no modo de autenticação facial.



Após a autenticação bem-sucedida, a caixa de prompt exibe **"Autenticação Bem- sucedida."**, como mostrado abaixo:

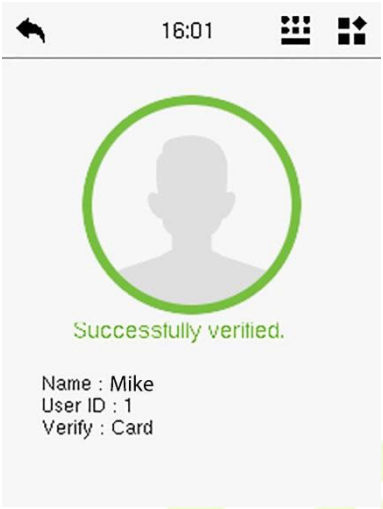


Se a autenticação falhar, ele exibirá a mensagem "Ajuste sua posição, por favor!".

4.6.3 Autenticação de Cartão

- **Modo de Autenticação de Cartão 1:N**

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



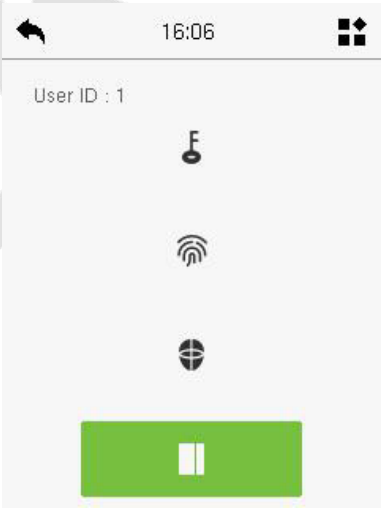
- **Modo de Autenticação de Cartão 1:1**

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

  Pressione na interface principal e entre no modo de verificação de cartão 1:1.

  Insira o ID do usuário e clique em **[OK]**.

Se um funcionário registrar uma impressão digital, um modelo facial e uma senha, além do cartão, a tela a seguir será exibida. Selecione o ícone para entrar no modo de verificação de cartão.

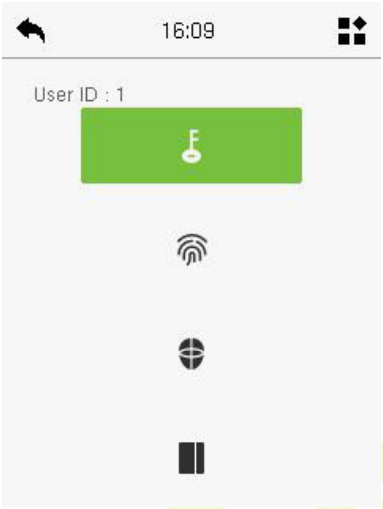


4.6.4 Autenticação de Senha

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

Toque no botão na tela principal para entrar no modo de verificação de senha 1:1.

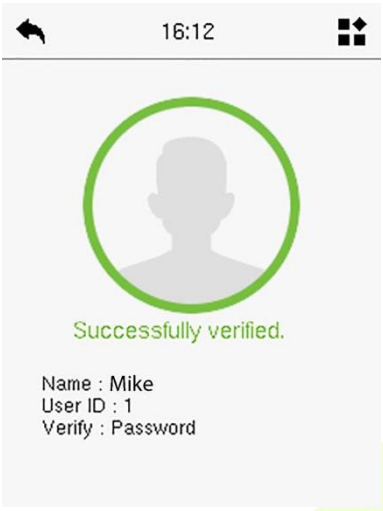
Se um funcionário registrar uma impressão digital, um modelo facial e um cartão, além da senha, a seguinte tela será exibida. Selecione o ícone para entrar no modo de verificação de senha.



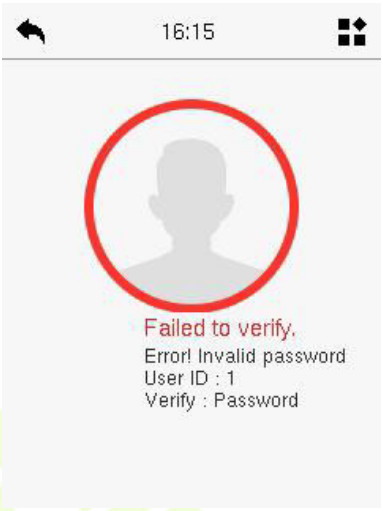
Digite a senha e pressione **[OK].**

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

Verificação bem-sucedida:



Verificação falhou:

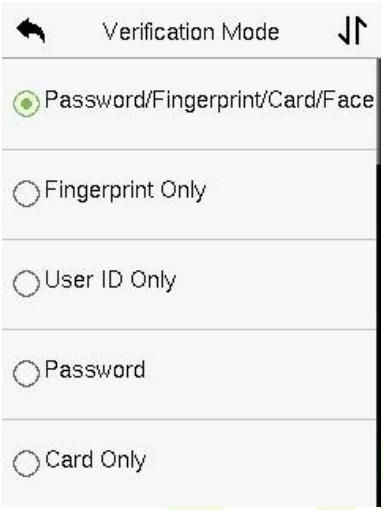


4.6.5 Autenticação Combinada

Este dispositivo permite que você utilize diversos métodos de verificação para aumentar a segurança. São um total de 21 combinações distintas de verificação que podem ser implementadas, conforme listado abaixo:

Definição de Símbolos de Autenticação 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.

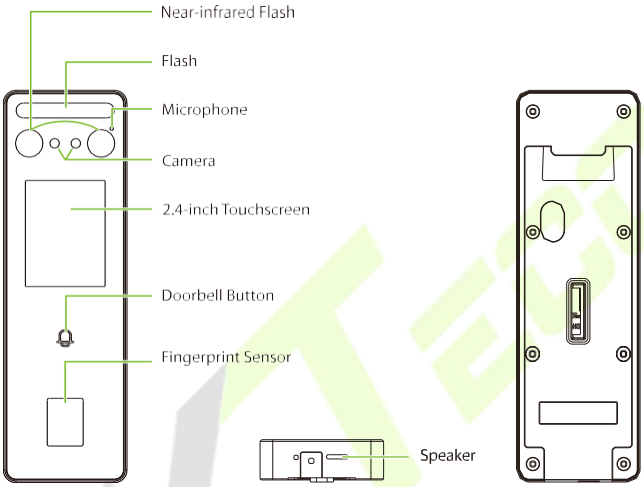


Procedimento para configurar o Modo de Verificação Combinada

- A verificação combinada requer que os funcionários registrem todos os diferentes métodos de verificação. Caso contrário, os funcionários não conseguirão concluir com sucesso o processo de verificação combinada.
- Por exemplo, se um funcionário tiver registrado apenas os dados do modelo facial, mas o modo de verificação do dispositivo estiver configurado como "Rosto + Senha", o funcionário não conseguirá concluir com êxito o processo de verificação.
- Isso ocorre porque o dispositivo compara o modelo facial da pessoa com o modelo de verificação registrado (tanto o modelo facial quanto a senha) previamente armazenado naquele ID de Pessoa no Dispositivo.
- No entanto, como o funcionário registrou apenas o modelo facial e não a senha, a verificação não será concluída e o dispositivo exibirá "Verificação Falhou".

5 Visão Geral

5.1 Aparência



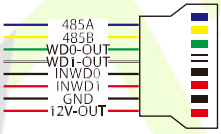
5.2 Descrição dos Cabos de Conexão e Cabeamento

5.2.1 Cabos de Conexão

Pino	Descrição
6	Entrada de Energia

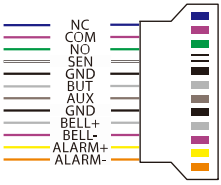
Pino	Descrição
4	Rede

Pino	Descrição
4	USB



Pino	Descrição	
8	485A	RS485
	485B	
	WD0-OUT	Saída Wiegand, Entrada Wiegand
	WD1-OUT	
	INWD0	
	INWD1	
	GND	

	12V-OUT	

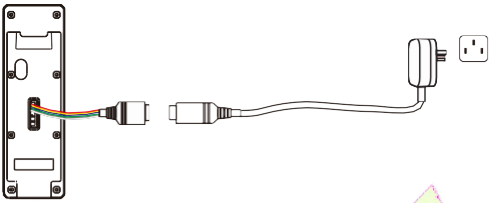


Pino	Descrição	
12	NC	Fechadura
	COM	
	NO	
	SEN	Sensor de Porta, Botoeira de Saída e Entrada Auxiliar
	GND	
	BUT	
	AUX	
	GND	
	BELL+	Campainha
	BELL-	
	ALARM+	Alarme
	ALARM-	

5.2.2 Descrição de Cabeamento

Pressione na interface inicial para entrar no menu principal, como mostrado abaixo:

➢ **Conexão de Energia**

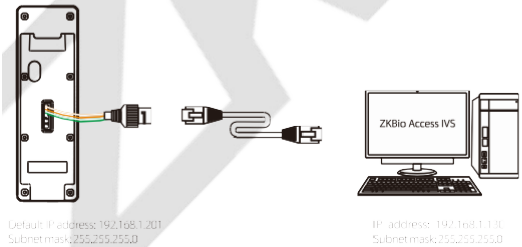


Adaptador AC Recomendado

1. 12V ± 10%, pelo menos 1500mA.
2. Para compartilhar a energia com outros dispositivos, use um Adaptador AC com classificações de corrente mais altas.

➢ **Conexão Ethernet**

Conecte o dispositivo e o software do computador através de um cabo Ethernet. Como mostrado no exemplo abaixo:



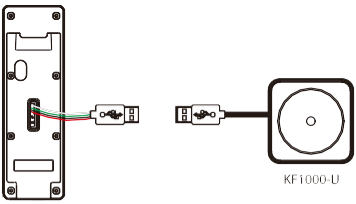
Clique em **Conf. Com** > **Ethernet** > **Endereço IP**, insira o endereço IP e clique em [OK].

Observação: Em uma rede local (LAN), os endereços IP do servidor (PC) e do dispositivo devem estar no mesmo segmento de rede ao conectar ao software ZKBio Access IVS.

- **Conexão USB**

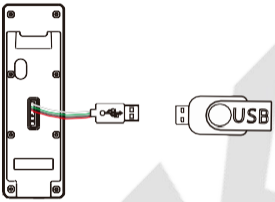
O dispositivo suporta a conexão do leitor KF1000-U e do disco USB.

Leitor KF1000-U:



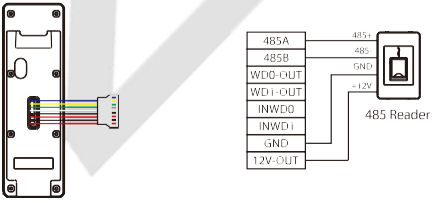
Para obter mais detalhes, consulte o Manual do Usuário do KF1000-U.

Disco USB:



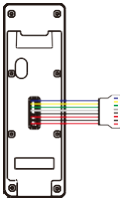
Para mais detalhes, por favor consulte 15 Gerenciador USB.

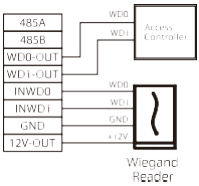
- **Conexão RS485 e Wiegand RS485:**



Observação: Os fios 485A e 485B podem ser conectados separadamente à catraca ou ao leitor 485, mas não podem ser conectados à catraca e ao leitor ao mesmo tempo.

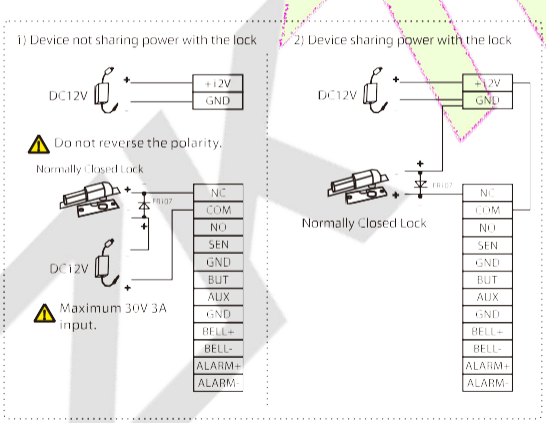
Wiegand:



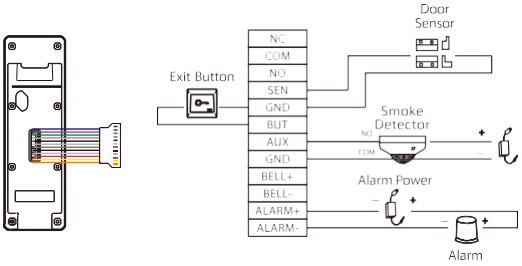


- **Conexão do Relé de Fechadura**

O sistema suporta Fechadura Normalmente Aberta (NO) e Fechadura Normalmente Fechada (NC). A fechadura NO (normalmente destravada quando ligada) é conectada aos terminais 'NO' e 'COM', enquanto a fechadura NC (normalmente travada quando ligada) é conectada aos terminais 'NC' e 'COM'. Abaixo, segue um exemplo utilizando a Fechadura NC:



➢ Conexão do Sensor de Porta, Botão de Saída, Alarme e Auxiliar



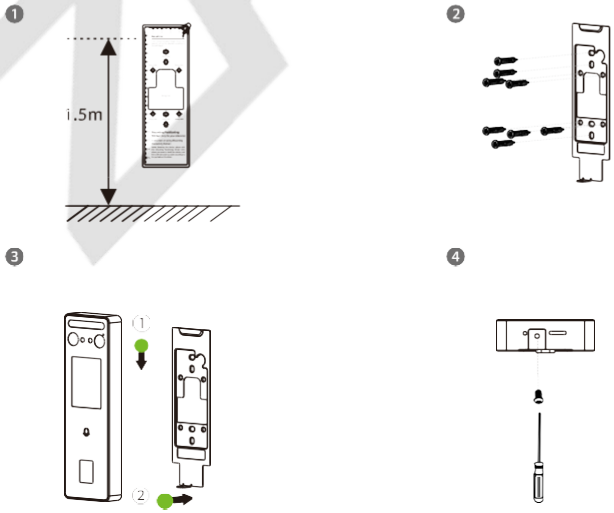
6 Instalação

6.1 Ambiente de Instalação

Por favor, consulte as seguintes recomendações para a instalação.

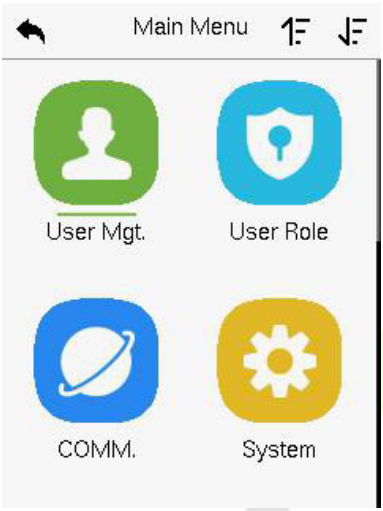
6.2 Instalação do Dispositivo

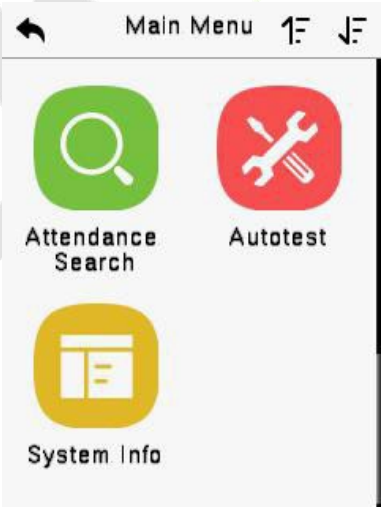
1. Fixe o adesivo do modelo de montagem na parede e faça furos de acordo com o papel de montagem.
2. Fixe a placa traseira na parede usando os parafusos de montagem na parede.
3. Anexe o dispositivo à placa traseira.
4. Prenda o dispositivo à placa traseira com um parafuso de segurança.



7 Menu Principal

Pressione na interface inicial para acessar o menu principal, como mostrado abaixo:





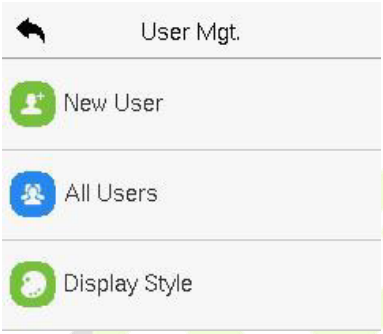
Descrição da Função

Menu	Descrição
Usuário Adm.	Para Adicionar, Editar, Visualizar e Deletar informações de um Usuário.
Priv. Usuário	Para definir o escopo de permissão da função personalizada e do inscritor para os usuários, ou seja, os direitos para operar o sistema.
Conf. Com.	Para configurar os parâmetros relevantes da Rede, Comunicação Serial, Conexão com PC, Wi-Fi, Servidor em Nuvem, Wiegand e Diagnóstico de Rede.
Sistema	Para configurar os parâmetros relacionados ao sistema, incluindo Data e Hora, Configuração de Registros de Acesso, Parâmetros de Rosto e Impressão Digital, Parâmetros de Vídeo Porteiro, Configurações de Segurança e redefinição para as configurações de fábrica.
Personalização	Para personalizar as configurações da Interface do Usuário, Voz, Programação de Campainha, Opções de Estado de Registro e Mapeamento de Teclas de Atalho.
Ger. Dados	Para deletar todos os dados relevantes no dispositivo.
Controle de Acesso	Para configurar os parâmetros da fechadura e do dispositivo de controle de acesso relevante, incluindo opções como programação de horário, configurações de feriado, verificação combinada, configuração de anti-passback e configurações de opções de situação de risco.
Gerenciador USB	Para fazer upload ou download de dados específicos de uma unidade USB.
Busca de Frequência	Para consultar os registros de eventos específicos.
Autoteste	Para testar automaticamente se cada módulo está funcionando corretamente, incluindo a tela LCD, áudio, microfone, sensor de impressão digital, câmera e relógio em tempo real.
Informações do Sistema	Para visualizar a Política de Privacidade, Capacidade de Dados e informações do dispositivo e firmware do dispositivo atual.

8 Gerenciamento de Usuários

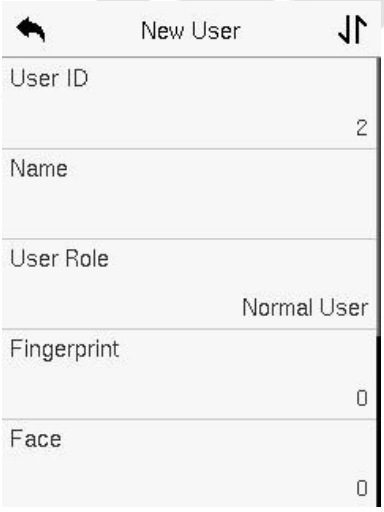
8.1 Registro de Usuário

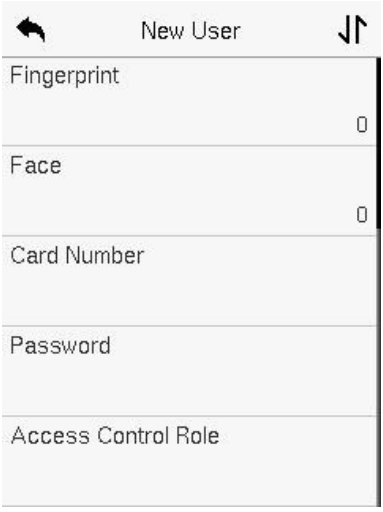
Toque em **Usuário Adm.** no menu principal.



8.1.1 ID do Usuário e Nome

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





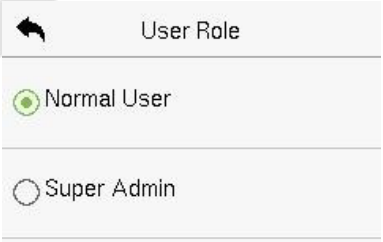
Observação:

1) AUm nome pode ter até 36 caracteres.
2) O ID do usuário pode conter de 1 a 14 dígitos por padrão, suportando 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.

8.1.2 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 realizar autenticações.
- **Funções Definidas pelo Usuário:** O Usuário Normal também pode ser atribuído a funções personalizadas com a Função Definida pelo Usuário. O usuário pode ter permissão para 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.

8.1.3 Registrar Impressão Digital

Toque em **Impressão Digital** na interface de **Novo Usuário** para acessar a página de registro de impressão digital.

- Selecione o dedo a ser cadastrado.
- Pressione o mesmo dedo no leitor de impressão digital três vezes.
- A cor verde indica que a impressão digital foi cadastrada com sucesso.

8.1.4 Face

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

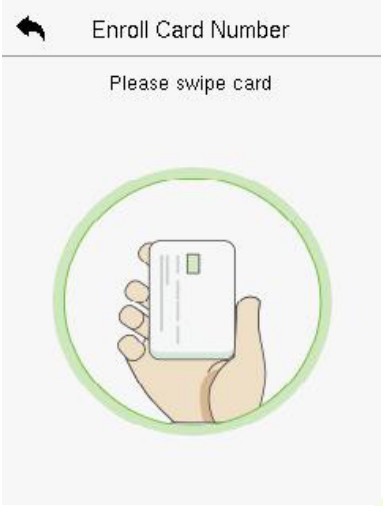
- Por favor, posicione-se de frente para a câmera e coloque-se de forma que sua imagem facial se encaixe dentro da caixa de orientação branca e permaneça imóvel durante o registro facial.
- Uma barra de progresso aparece durante o registro do rosto e, em seguida, a mensagem **Cadastrado com Sucesso** é exibida quando a barra de progresso é concluída.

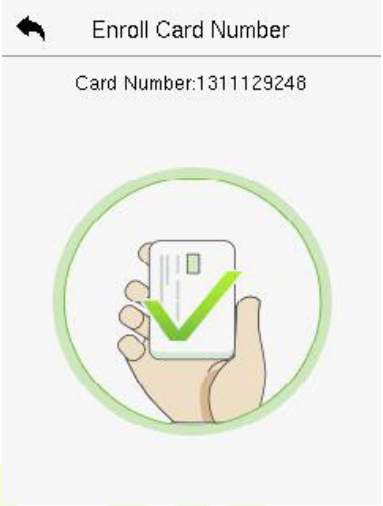
- Se a face já estiver cadastrada, a mensagem "Face Duplicada" é exibida. A interface de registro é a seguinte:

8.1.5 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 cadastrado, a mensagem **Erro! Cartão já cadastrado** aparecerá. A interface de registro se parece com isso:





8.1.6 Senha

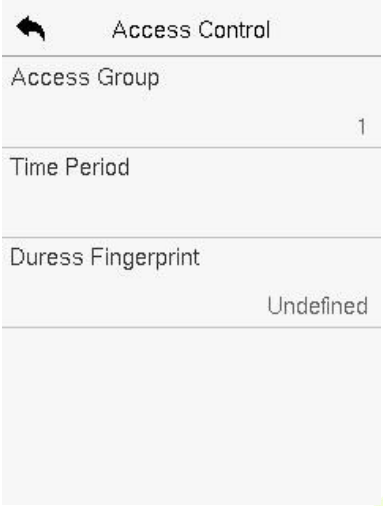
Toque em **Senha** na interface de **Novo Usuário** para acessar a página de registro de senha.

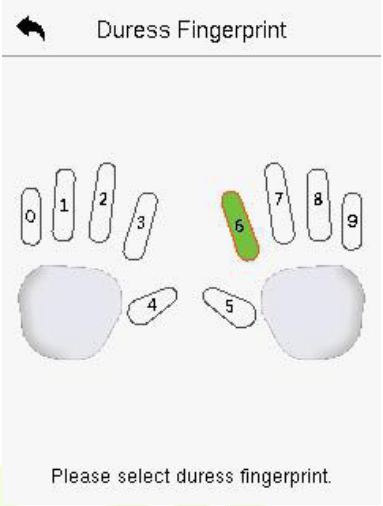
- Na interface de Senha, digite a senha necessária e digite novamente para confirmá-la e toque em OK.
- Se a senha digitada novamente for diferente da senha inicialmente inserida, o dispositivo exibirá a mensagem "Senha não corresponde!", e o usuário precisará confirmar a senha novamente.
- A senha pode conter de 6 a 8 dígitos por padrão.

8.1.7 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 uma melhor gestão. Os novos usuários pertencem ao Grupo 1 por padrão e podem ser realocados para outros grupos. O dispositivo suporta até 99 grupos de Controle de Acesso.
- Toque em **Período de Tempo** para selecionar o horário a ser utilizado.
- O usuário pode especificar uma ou mais impressões digitais que foram registradas como impressões digitais de situação de risco. Ao pressionar o dedo correspondente à impressão digital de situação de risco no sensor e passar pela verificação, o sistema imediatamente gerará um alarme de situação de risco.

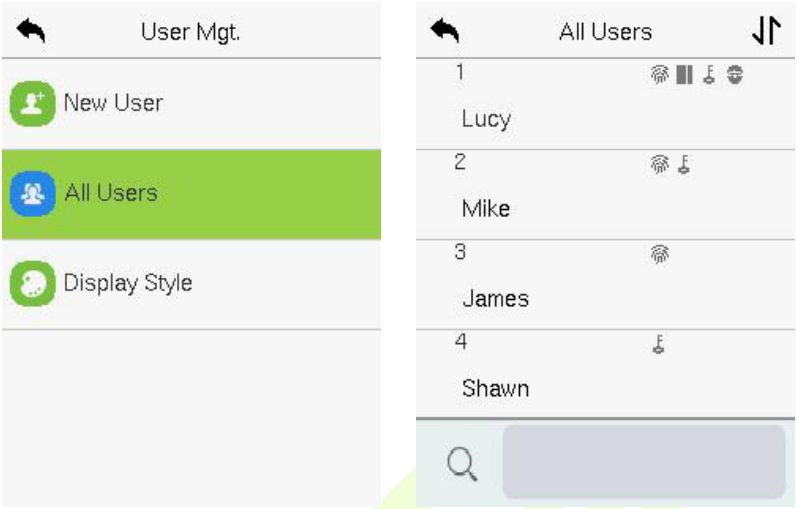




8.2 Buscar Usuário

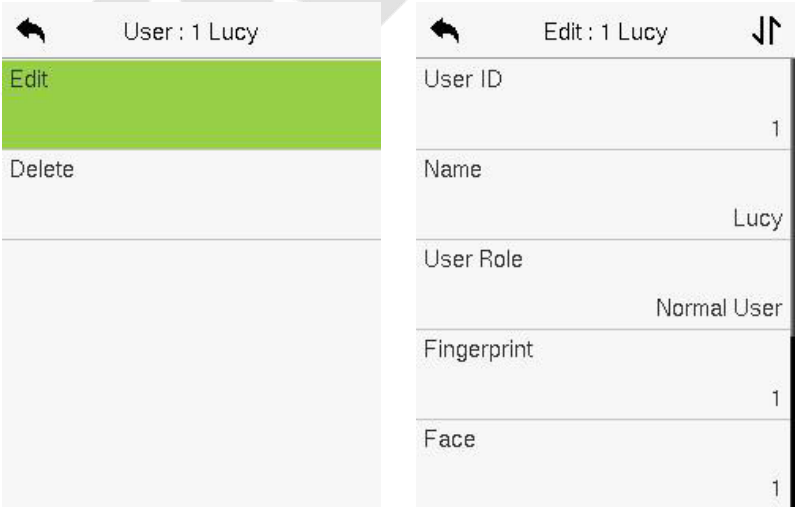
No Menu Principal, toque em **Usuário Adm** e, em seguida, toque em **Todos os Usuários** para buscar um Usuário.

- Na interface de **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 relacionadas ao usuário.



8.3 Editar Usuário

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



Observação:

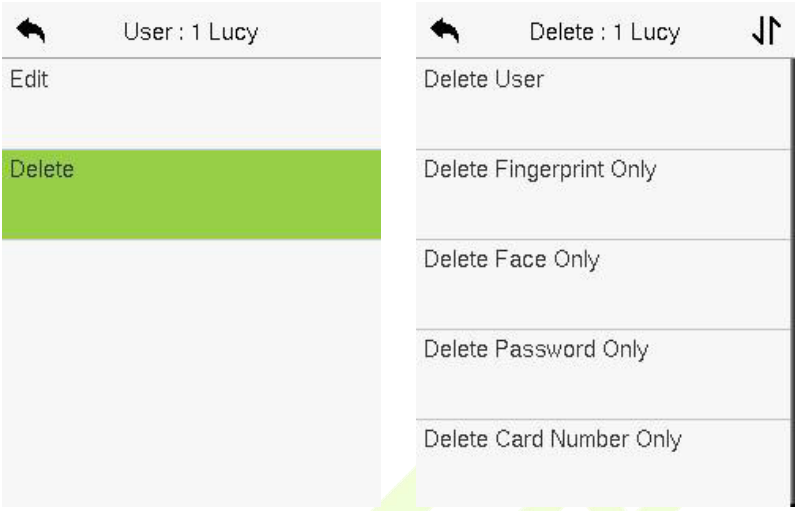
O processo de edição das informações do usuário é o mesmo que adicionar um novo usuário, exceto que o ID do usuário não pode ser modificado ao editar um usuário. O processo em detalhes está descrito em "6.1 Registro de Usuário".

8.4 Excluir Usuário

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

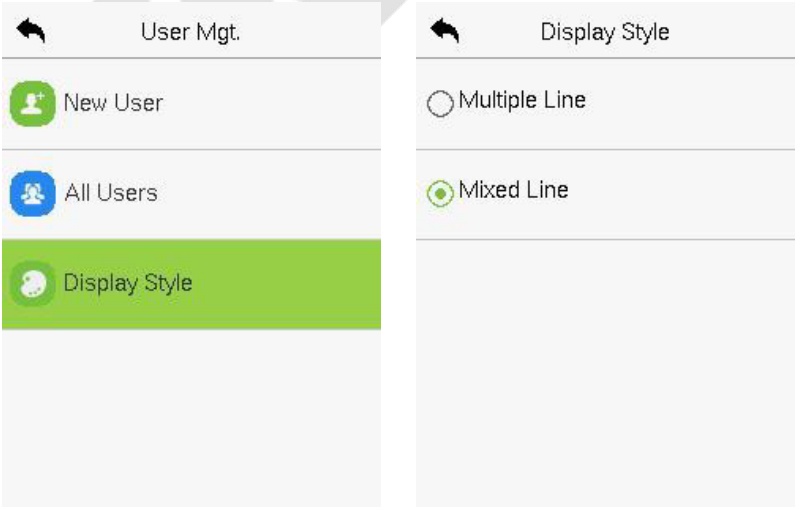
➢ **Operações de Exclusão**

- **Excluir Usuário:** Exclui todas as informações do usuário (exclui o Usuário selecionado como um todo) do Dispositivo.
- **Excluir Apenas Impressão Digital:** Exclui as informações de impressão digital do usuário selecionado.
- **Excluir Apenas Face:** Exclui as informações do rosto do usuário selecionado.
- **Excluir Apenas Senha:** Exclui as informações da senha do usuário selecionado.
- **Excluir Apenas Número do Cartão:** Exclui as informações do cartão do usuário selecionado.



8.5 Estilo de Exibição

No **Menu Principal**, toque em **Gerenciamento de Usuários e**, em seguida, toque em **Estilo de Exibição** para entrar na interface de configuração do **Estilo de Exibição**.



Todos os Estilos de Exibição são mostrados abaixo:

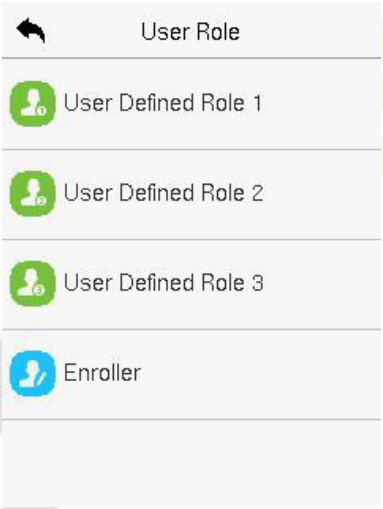
Múltiplas Linhas:

Linha Mista:

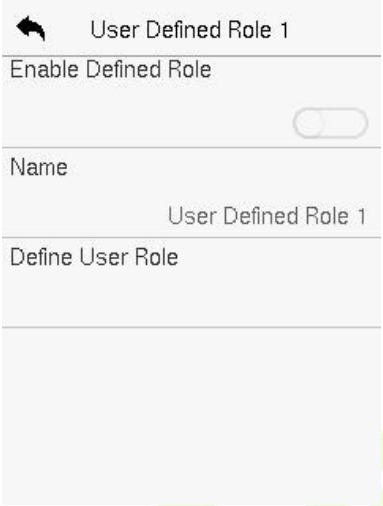
9 Privilégio do Usuário

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

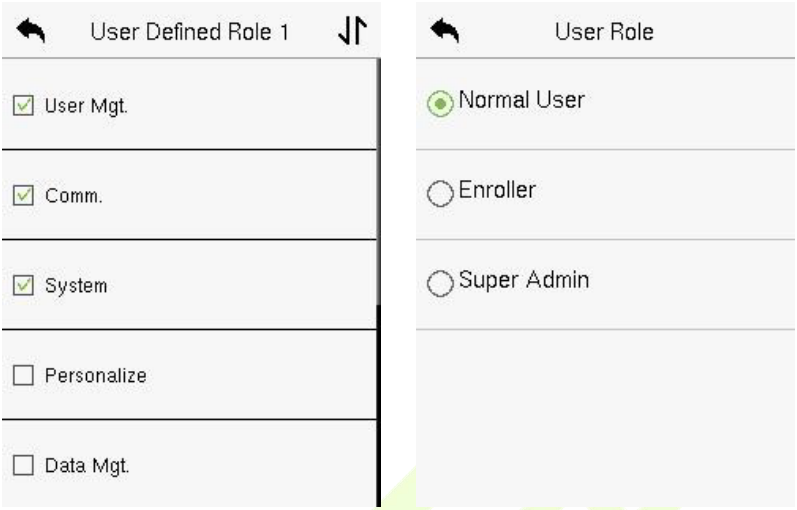
- No menu principal, toque em **Privilégio do Usuário** e, em seguida, toque na **Função Definida pelo Usuário** para definir as permissões definidas pelo usuário.
- O **escopo de permissão** da função personalizada pode ser configurado em 3 níveis, ou seja, o escopo operacional personalizado das funções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



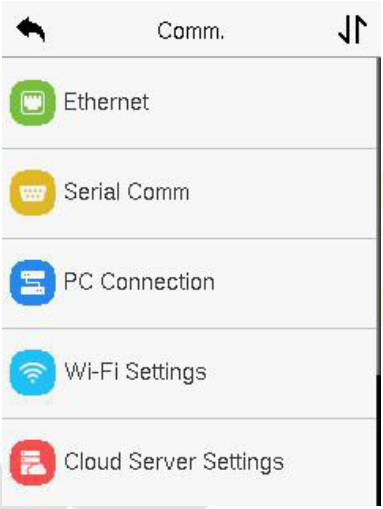
Observação:

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.

10 Configurações de comunicação

As Configurações de Comunicação são usadas para definir os parâmetros da Rede, Comunicação Serial, Conexão com PC, Wi-Fi, Servidor em Nuvem, Wiegand e Diagnóstico de Rede.

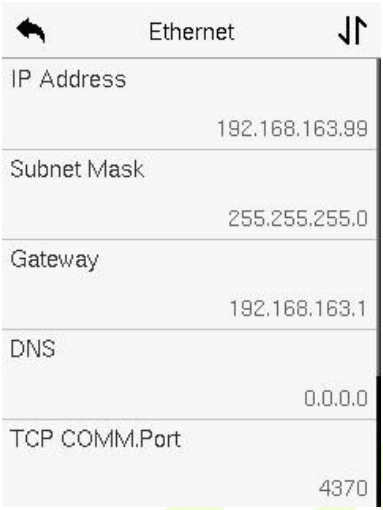
Toque em **Conf. Com.** no Menu Principal.



10.1 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.



Descrição da Função

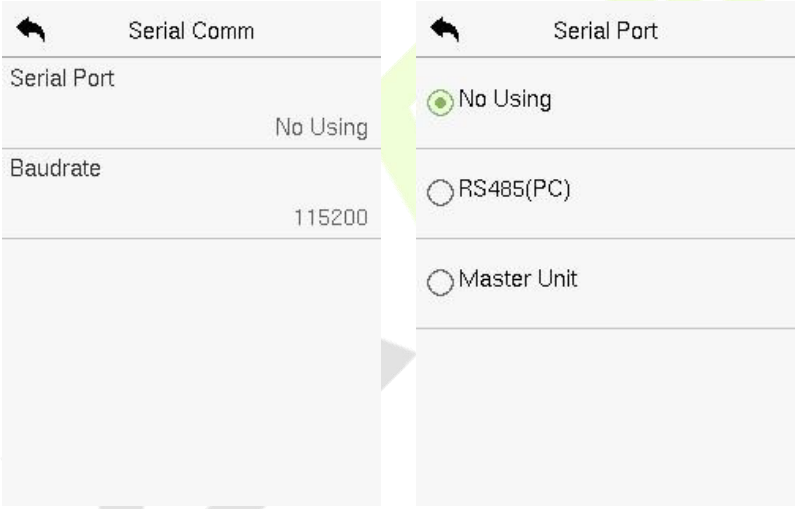
Nome da função	Descrição
TCP/IP	O endereço IP padrão é 192.168.1.201. Ele pode ser modificado de acordo com a disponibilidade da rede.
Máscara de Rede	A Máscara de Sub-rede padrão é 255.255.255.0. Ela pode ser modificada de acordo com a disponibilidade da rede.
Gateway	O endereço de Gateway Padrão é 0.0.0.0. Ele pode ser modificado de acordo com a disponibilidade da rede.
DNS	O endereço DNS padrão é 0.0.0.0. Ele pode ser modificado de acordo com a disponibilidade da rede.
Porta de Comunicação TCP	O valor padrão da porta de comunicação TCP é 4370. Ele pode ser modificado de acordo com a disponibilidade da rede.
DHCP	O Protocolo de Configuração Dinâmica de Host (DHCP) aloca dinamicamente endereços IP para clientes através de um servidor.

Exibir na Barra de Status	Alternar para definir se o ícone da rede deve ser exibido na barra de status.

10.2 Comunicação Serial

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

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



Descrição da Função

Nome da função	Descrição
Porta Serial	**Sem Uso:** Sem comunicação com o dispositivo através da porta serial. **RS485(PC):** Comunicação com o dispositivo através da porta serial RS485. **Unidade Mestre:** Quando o RS485 é usado como função de "Unidade Mestre", ele pode ser conectado a um leitor de cartões.

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

10.3 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.

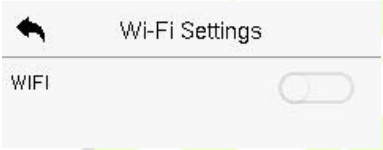
Descrição da Função

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.

10.4 Wi-Fi

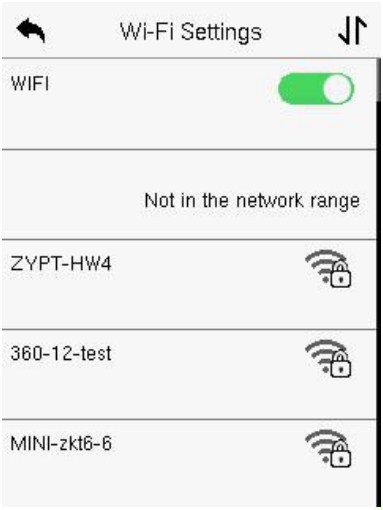
O dispositivo oferece um módulo Wi-Fi, que pode ser embutido no módulo do dispositivo. O módulo Wi-Fi permite a transmissão de dados via Wi-Fi (Wireless Fidelity) e estabelece um ambiente de rede sem fio. O Wi-Fi é ativado por padrão no dispositivo. Se você não precisa usar a rede Wi-Fi, pode alternar 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.

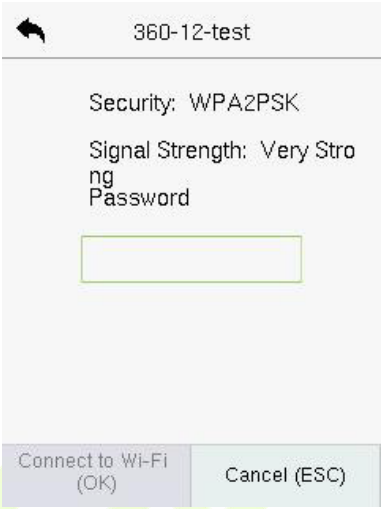


➢ **Procurando a Rede Wi-Fi**

- O WIFI é ativado no dispositivo por padrão. Alterne 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



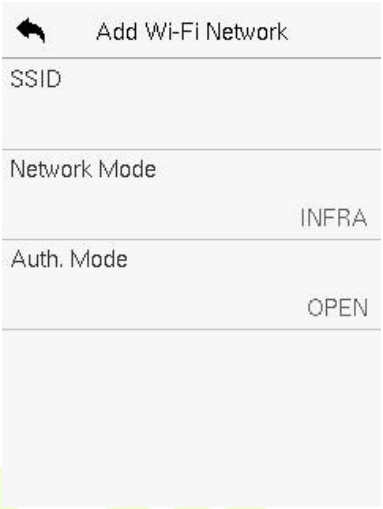
Toque no campo de senha para inserir a senha e toque em **Conectar ao WIFI (OK).**

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

➢ Adicionando uma Rede WIFI Manualmente

O Wi-Fi também pode ser adicionado manualmente se a rede Wi-Fi necessária não aparecer na lista.

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



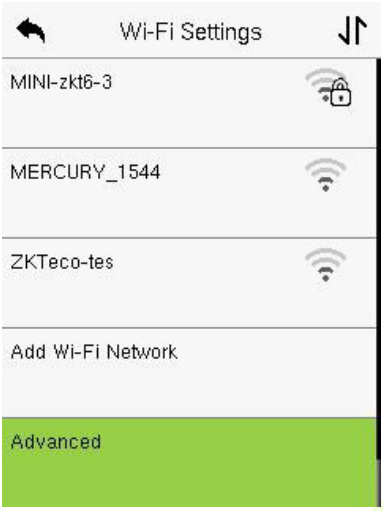
Nesta interface, insira os parâmetros da rede WIFI. (A rede adicionada deve existir.)

Observação:

Após adicionar o WIFI manualmente com sucesso, siga o mesmo processo para buscar pelo nome do WIFI adicionado.

Configuração Avançada

Na interface de **Configurações de Wi-Fi**, toque em **Avançado** para configurar os parâmetros relevantes conforme necessário.

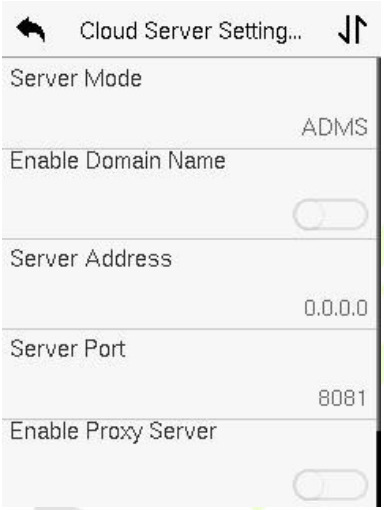


Descrição da Função

Função	Descrição
DHCP	O Protocolo de Configuração Dinâmica de Host (DHC) aloca dinamicamente endereços IP para clientes de rede Se o DHCP estiver ativado, o endereço IP não pode se definido manualmente.
Endereço IP	O endereço IP para a rede Wi-Fi, o padrão é 0.0.0.0. Ele pode ser modificado de acordo com a disponibilidade da rede.
Máscara de Sub-rede	A Máscara de Sub-rede padrão da rede Wi-Fi é 255.255.255.0. Ela pode ser modificada de acordo com a disponibilidade da rede.
Gateway	O endereço de Gateway Padrão é 0.0.0.0. Ele pode ser modificado de acordo com a disponibilidade da rede.

10.5 Configuração do Servidor de Nuvem

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



Descrição da Função

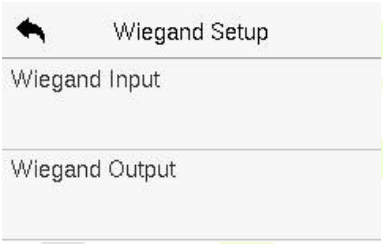
Função		Descrição
Ativar nome de domínio	**Endereço do servidor**	Uma vez habilitada esta função, será utilizado o modo de nome de domínio "http://...", como http:// www.XYZ.com, enquanto "XYZ" será o nome de domínio (quando este modo está LIGADO).
Desativar nome de domínio	**Endereço do servidor**	Endereço 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.

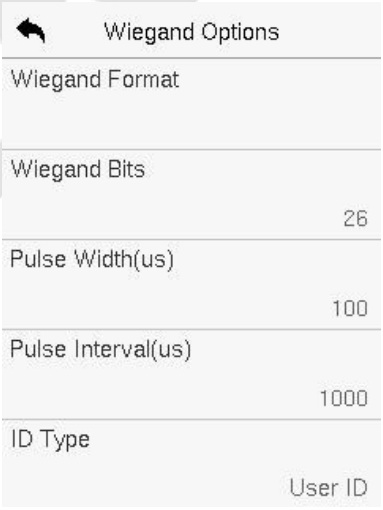
10.6 Configuração Wiegand

É usado para configurar os parâmetros de entrada e saída Wiegand.

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



10.6.1 Entrada Wiegand



Descrição da Função

Função	Descrição
Formato Wiegand	Os valores variam de 26 bits, 34 bits, 36 bits, 37 bits e 50 bits
Wiegand Bits	O número de bits dos dados Wiegand.
Largura de Pulso (μs)	O valor da largura de pulso enviada pelo Wiegand é de 100 microssegundos por padrão, podendo ser ajustado dentro da faixa de 20 a 400 microssegundos.
Intervalo de Pulso (μs)	O valor padrão é de 1000 microssegundos e pode ser ajustado dentro da faixa de 200 a 20000 microssegundos.
Tipo de ID	Selecione entre o ID do usuário e o número do cartão.

Descrição de vários formatos comuns do Wiegand:

Formato Wiegand	Descrição
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCCO 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	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCO 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	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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; and "**S**" Código do Site.

10.6.2 Saída Wiegand

Descrição da Função

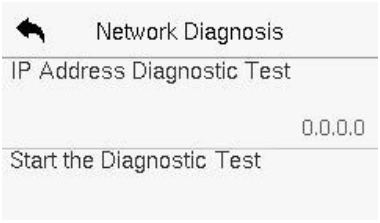
Função	Descrição
Formato Wiegand	O valor do formato Wiegand pode ser de 26 bits, 34 bits, 36 bits, 37 bits e 50 bits.
Bits de Saída Wiegand	Após selecionar o formato Wiegand necessário, selecione os dígitos de bits de saída correspondentes ao formato Wiegand.

ID inválido	Se a verificação falhar, o sistema enviará o ID inválido para o dispositivo e substituirá o número do cartão ou ID do pessoal pelo novo.
Código do Site	O código do site é semelhante ao ID do dispositivo. A diferença é que um código do site pode ser definido manualmente e pode ser repetido em um dispositivo diferente. O valor válido varia de 0 a 256 por padrão.
Largura de Pulso (µs)	A largura de tempo representa as mudanças na quantidade de carga elétrica com capacitância de alta frequência regular dentro de um tempo especificado.
Intervalo de Pulso (µs)	O intervalo de tempo entre pulsos.
Tipo de ID	Selecione os tipos de ID como ID do usuário ou número do cartão.

10.7 Diagnóstico de Rede

Isso ajuda a configurar os parâmetros de diagnóstico de rede.

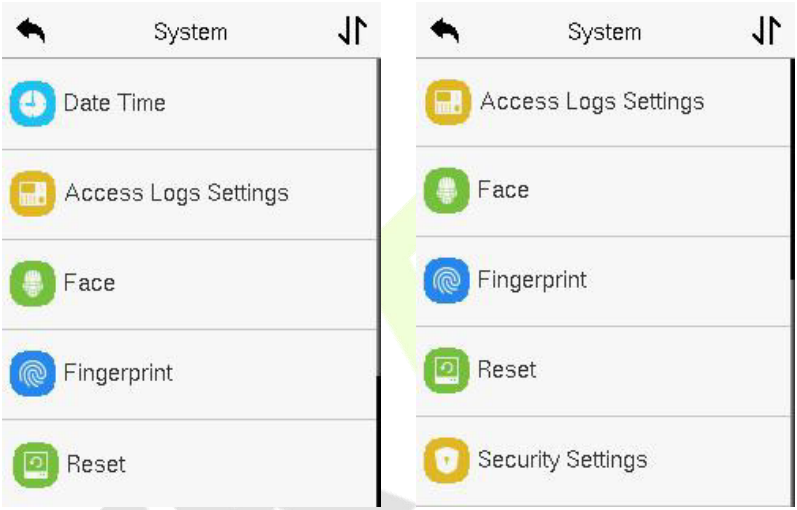
Toque em **Diagnóstico de Rede** na interface de **Configurações de Comunicação**. Insira o endereço IP que precisa ser diagnosticado e toque em **Iniciar Teste de Diagnóstico** para verificar se a rede pode se conectar ao dispositivo.



11 Configurações do Sistema

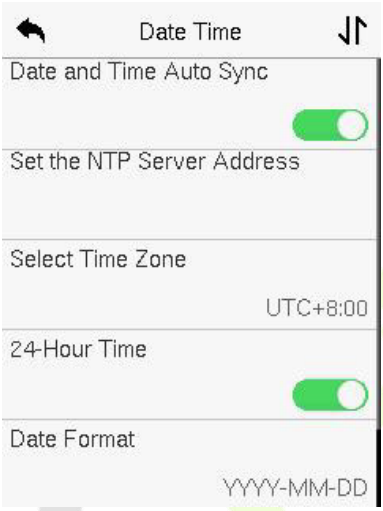
Isso ajuda a configurar os parâmetros do sistema relacionados para otimizar a acessibilidade do dispositivo.

Toque em **Sistema** na interface do Menu Principal para acessar suas opções de menu.

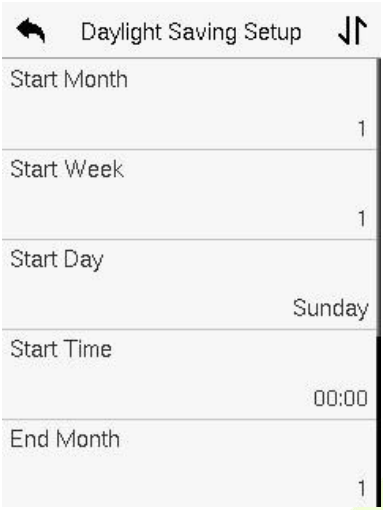


11.1 Data e Hora

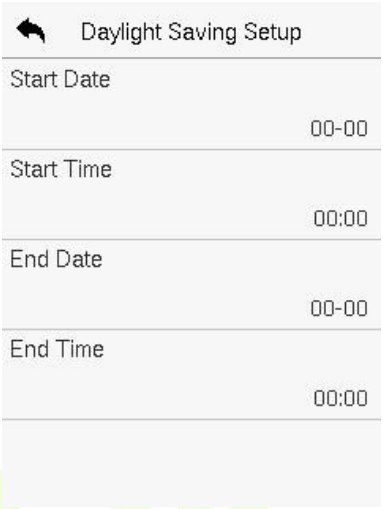
Toque em **Data e Hora** na interface do **Sistema** para configurar a data e a hora.



- Toque em **Sincronização Automática de Data e Hora** para habilitar a sincronização automática do horário 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 selecionar manualmente o fuso horário onde o dispositivo está localizado.
- Ative ou desative o formato de 24 horas tocando em **Horário de 24 Horas.** Se estiver ativado, selecione o **Formato de Data** para configurar a data.
- Toque em **Horário de Verão** para habilitar ou desabilitar a função. Se estiver 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 de mudança.



Modo Semanal



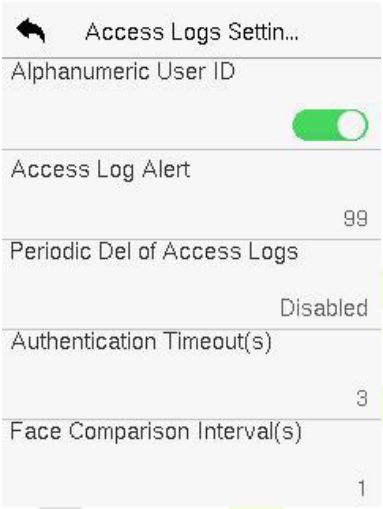
Modo de Data

- 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 hora do dispositivo não podem ser restauradas.

Observação: Por exemplo, se um usuário define a hora do dispositivo para 18h35 em 15 de março de 2020 e, em seguida, restaura as configurações de fábrica, a hora do dispositivo permanecerá em 18h30 em 1º de janeiro de 2021.

11.2 Configuração de Registros de Acesso

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



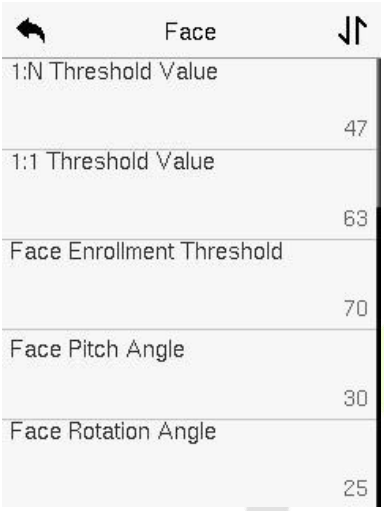
Descrição da Função

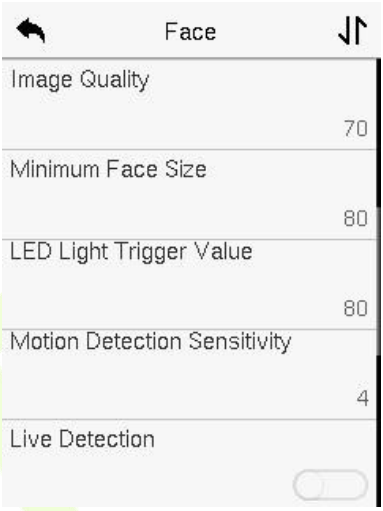
Nome da função	Descrição
ID do Usuário Alfanumérico	Ativar/Desativar o uso de alfanuméricos como ID do usuário.
Alerta de Registro de Acesso	Quando o espaço de armazenamento dos registros de acesso atinge o valor máximo definido, o dispositivo exibe automaticamente um aviso de espaço de memória. Os usuários podem desativar essa função ou definir um valor válido entre 1 e 9999.

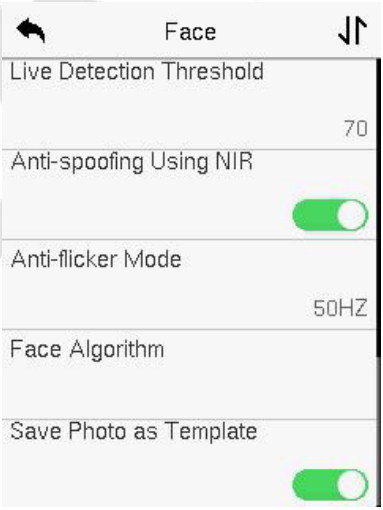
Exclusão Periódica de Registros de Acesso	Quando os registros de acesso atingem sua capacidade máxima, o dispositivo automaticamente exclui um conjunto de registros de acesso antigos. Os usuários podem desativar essa função ou definir um valor válido entre 1 e 999.
Tempo Limite de Autenticação (em segundos)	O tempo necessário para exibir uma mensagem de verificação bem-sucedida. Valor válido: de 1 a 9 segundos.
Intervalo de Comparação Facial (em segundos)	Após selecionar o intervalo de identificação, por exemplo, se o intervalo de comparação for definido como 5 segundos, o reconhecimento facial verificará o rosto a cada 5 segundos. Valor válido: de 0 a 9 segundos. 0 significa identificação contínua, de 1 a 9 significa identificação em intervalos.

11.3 Parâmetros de Reconhecimento Facial

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







Descrição da Função

Nome da função	Descrição
Limiar 1:N	No modo de autenticação 1:N, a autenticação será bem- sucedida apenas quando a semelhança entre a imagem facial adquirida e todos os modelos faciais registrados for maior que o valor definido. O valor válido varia de 0 a 100. Quanto maior o valor do limiar, menor será a taxa de erro de avaliação e maior será a taxa de rejeição, e vice-versa. É recomendado definir o valor padrão como 47.
Limiar 1:1	No modo de autenticação 1:1, a autenticação será bem- sucedida apenas quando a semelhança entre a imagem facial adquirida e os modelos faciais do usuário inscritos no dispositivo for maior que o valor definido. O valor válido varia de 0 a 100. Quanto maior o valor do limiar, menor será a taxa de erro de avaliação e maior será a taxa de rejeição, e vice-versa. É recomendado definir o valor padrão como 63.
Limiar de Cadastramento de Face	Durante o cadastramento de face, é usada a comparação 1:N para determinar se o usuário já foi Limiar de Cadastramento de Face registrado anteriormente. Quando a semelhança entre a imagem facial adquirida e todos os modelos faciais registrados for maior que o limiar definido, isso indica que o rosto já foi registrado.
Ângulo de Inclinação da Face	É a tolerância de ângulo de inclinação de um rosto

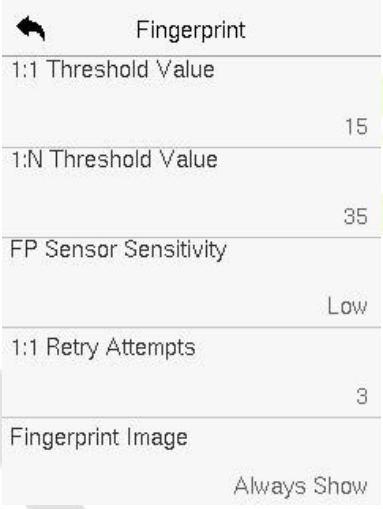
	para o registro e comparação de modelos faciais. Ângulo de Inclinaçãoda Face Se o ângulo de inclinação do rosto exceder o valor definido, ele será filtrado pelo algoritmo, ou seja, ignorado pelo terminal, assim nenhuma interface de registro e comparação será acionada
Ângulo de Rotaçãoda Face	É a tolerância de ângulo de rotação de um rosto para o registro e comparação de modelos faciais. Se o ângulo de rotação da face exceder o valor definido, ela será filtrada pelo algoritmo, ou seja, ignorada pelo terminal, assim 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.
Tamanho Mínimo da Face	Define o tamanho mínimo de face 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 uma face. Esse valor também pode ser interpretado como a distância de comparação facial. Quanto mais distante a pessoa estiver, menor será a face e menor será o número de pixels da face obtida pelo algoritmo. Portanto, ajustar esse parâmetro pode ajustar a distância máxima de comparação de rostos. Quando o valor é 0, a distância de comparação de rostos não é limitada.

Limiar de Acionamentoda Luz LED	Este valor controla o acionamento e desligamento da luz LED. Quanto maior o valor, mais frequentemente a luz LED será ligada ou desligada.
Sensibilidade de Detecção de Movimento	Ele define o valor para a quantidade de mudança no campo de visão da câmera, conhecido 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.
Detecção em Tempo Real	Isso detecta tentativas de fraude usando imagens de luz visível para determinar se a amostra biométrica fornecida é de uma pessoa real (um ser humano vivo) ou uma representação falsa.
Limiar de Detecção em Tempo Real	Facilita a avaliação se a imagem visível capturada é de uma pessoa real (um ser humano vivo). Quanto maior o valor, melhor será o desempenho contra fraudes usando luz visível.
Anti-fraude Usando NIR	Usando imagens de espectros de infravermelho próximo para identificar e prevenir ataques de fotos e vídeos falsos.
Modo Anti-Cintilação	É usado quando o WDR está desligado. Ajuda a reduzir o efeito de cintilação quando a tela do dispositivo pisca na mesma frequência da luz
Algoritmo Facial	Ele tem informações relacionadas ao algoritmo facial e pausa a atualização do modelo facial.

Salvar Foto como Template	Após desabilitar essa função, será necessário re-registrar o rosto após uma atualização do algoritmo.

11.4 Parâmetros de Impressão Digital

Toque em **Impressão Digital** na interface do **Sistema** para acessar as configurações de parâmetros de impressão digital.



Descrição da Função

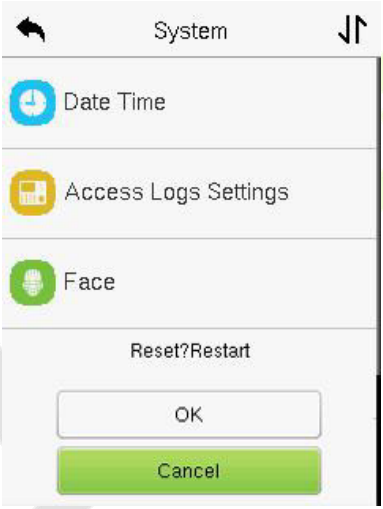
Nome da função	Descrição
Valor de Limiar 1:1	No método de verificação 1:1, a verificação será bem-sucedida apenas quando a similaridade entre os dados de impressão digital adquiridos e o modelo de impressão digital associado ao ID do usuário inserido e registrado no dispositivo for maior que o valor definido.

Valor de Limiar 1:N	No método de verificação 1:N, a verificação será bem-sucedida apenas quando a similaridade entre os dados de impressão digital adquiridos e os modelos de impressão digital registrados no dispositivo for maior que o valor definido.
Sensibilidade do Sensor de Impressão Digital	Para ajustar a sensibilidade da aquisição de impressões digitais, é recomendado usar o nível padrão Médio. Quando o ambiente estiver seco, resultando em uma detecção lenta das impressões digitais, você pode ajustar o nível para Alto para aumentar a sensibilidade; quando o ambiente estiver úmido, dificultando a identificação da impressão digital, você pode ajustar o nível para Baixo.
Tentativas 1:1	Na Verificação 1:1, os usuários podem esquecer a impressão digital registrada ou pressionar o dedo de forma inadequada. Para reduzir o processo de reingresso do ID do usuário, é permitida uma nova tentativa.
Imagem de Impressão Digital	Para definir se exibir a imagem da impressão digital na tela durante o cadastro ou verificação da impressão digital, existem quatro opções disponíveis: **Mostrar durante o Cadastro:** exibir a imagem da impressão digital somente na tela durante o cadastro. **Mostrar durante a Verificação:** exibir a imagem da impressão digital somente na tela durante a verificação. **Sempre Mostrar:** exibir a imagem da impressão digital na tela durante o cadastro e a verificação. **Nenhum:** não exibir a imagem da impressão digital.

11.5 Restauração dos padrões de fábrica

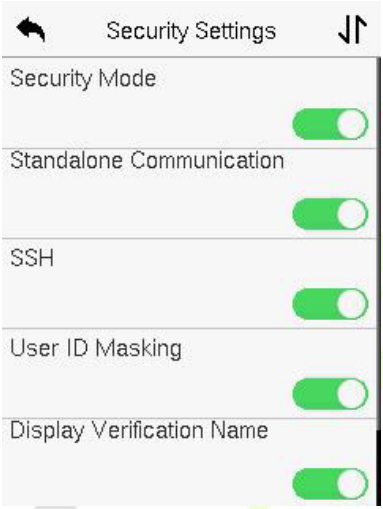
A função de Restauração de Fábrica restaura as configurações do dispositivo, como configurações de comunicação e configurações do sistema, para as configurações de fábrica padrão (esta função não apaga os dados de usuário registrados).

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



11.6 Configurações de Segurança

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



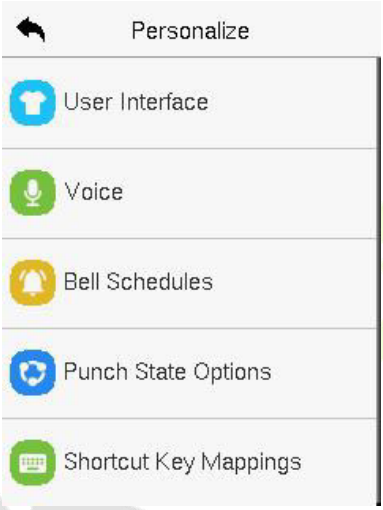
Descrição da Função

Nome da função	Descrição
Modo de Segurança	Selecione se deseja ativar 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 Independente	Para evitar ficar impossibilitado de usar quando o dispositivo estiver offline, você pode baixar antecipadamente o software C/S em seu computador para uso offline.

SSH	O SSH é usado para acessar o sistema operacional do dispositivo para fins de manutenção.
Mascaramento do ID do Usuário	Quando ativado e o usuário for comparado e verificado com sucesso, o ID do usuário no resultado da verificação exibido será substituído por * para garantir a proteção segura de dados privados sensíveis.
Exibição do Nome de Verificação	Defina se deseja exibir o nome do usuário na interface de resultado da verificação.
Exibição do Modo de Verificação	Defina se deseja exibir o modo de verificação na interface de resultado da verificação.

12 Configurações de Personalização

Toque em **Personalizar** na interface do **Menu Principal** para personalizar as configurações da interface, voz, toque, opções de estado de registro e mapeamento de teclas de atalho.



12.1 Configurações de Exibição

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

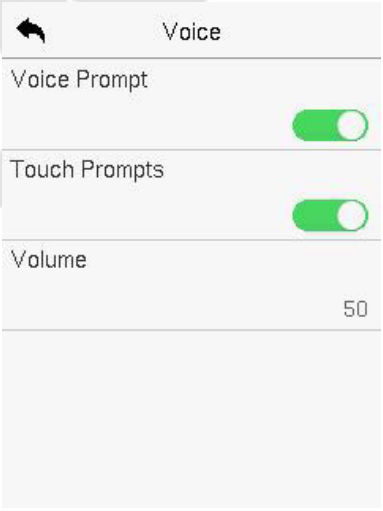
Descrição da Função

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.

12.2 Configurações de voz

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

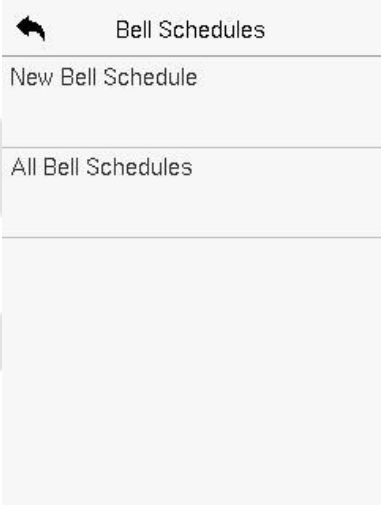


Descrição da Função

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.

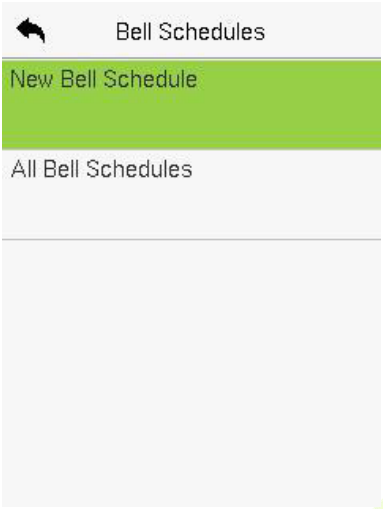
12.3 Horários

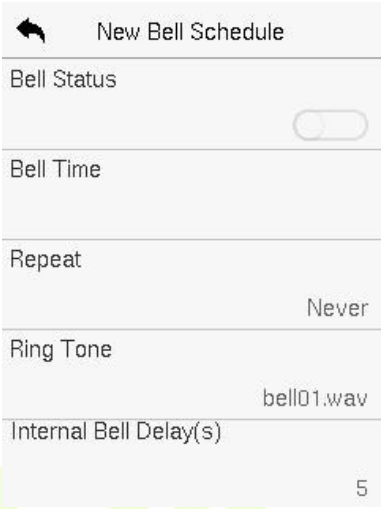
Toque em **Horários** na interface **Personalização** para definir as configurações de **Horários**.



- **Novo Horário**

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





Descrição da Função

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**

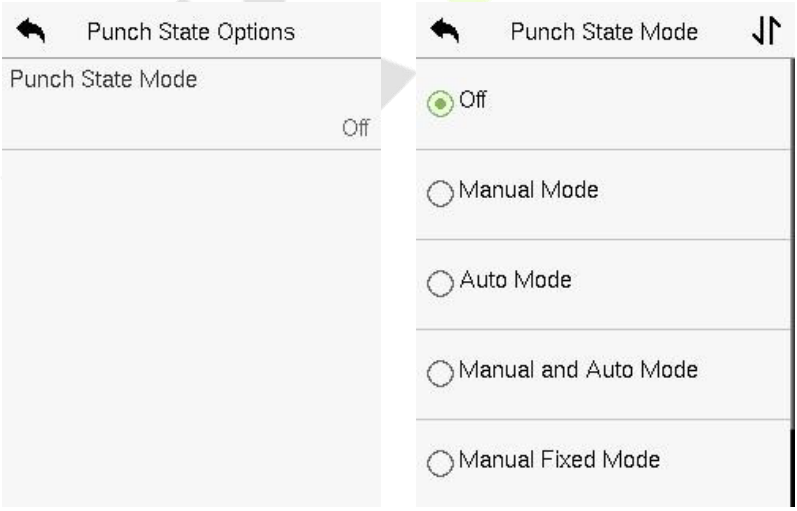
  Na interface **Todos os Horários**, toque na programação de campainha e toque em **Editar** para editar a programação de campainha selecionada. O método de edição é o mesmo que as operações de adição de uma nova programação de campainha.

- **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.

12.4 Opções de Estados de Registro

Toque em **Opções de Estados de Registro** na interface **Personalização** para configurar as configurações de estados de registro.



Descrição da Função

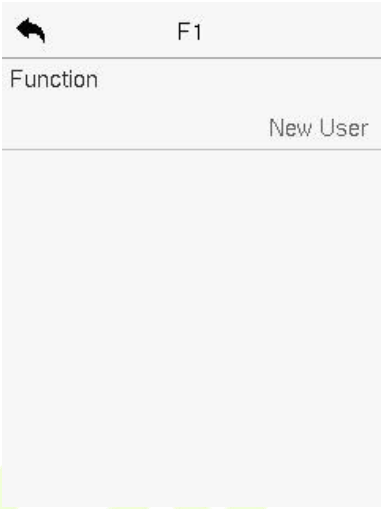
Função	Descrição
Modo de Estado de Registro	**Desligado:** Desativa a função de estado de registro. Portanto, a tecla de estado de registro definida no menu de Mapeamento de Teclas de Atalho se tornará inválida. **Modo Manual:** Altera manualmente a tecla de estado de registro, e a tecla de estado de registro desaparecerá após o tempo limite do estado de registro. **Modo Automático:** A tecla de estado de registro será alternada automaticamente para um estado de registro específico de acordo com o cronograma de tempo predefinido, que pode ser configurado no menu de Mapeamento de Teclas de Atalho. **Modo Manual e Automático:** A interface principal exibirá a tecla de estado de registro de alternância automática. No entanto, os usuários ainda poderão selecionar uma alternativa que seja o status de registro manual. Após o tempo limite, a tecla de estado de registro de alternância manual se tornará a tecla de estado de registro de alternância automática. **Modo Manual Fixo:** Após a tecla de estado de registro ser definida manualmente para um status de registro específico, a função permanecerá inalterada até que seja alterada manualmente novamente. **Modo Fixo:** Apenas a tecla de estado de registro fixa manualmente será mostrada. Os usuários não podem alterar o status pressionando outras teclas.

12.5 Mapeamento de Teclas de Atalho

Os usuários podem definir teclas de atalho para o status de registro e para teclas funcionais que serão definidas na interface principal. Assim, na interface principal, quando as teclas de atalho são pressionadas, o status de registro correspondente ou a interface da função serão exibidos diretamente.

Toque em **Mapeamento de Teclas de Atalho** na interface de personalização para configurar as teclas de atalho necessárias.

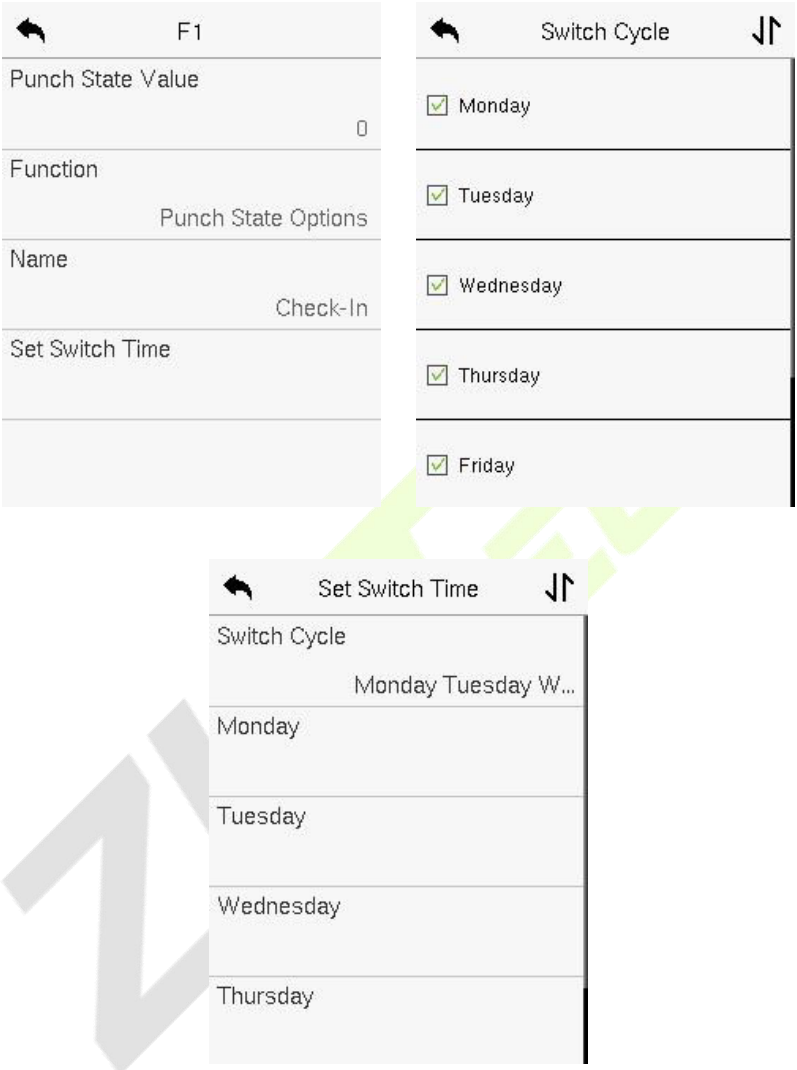
- Na interface **Mapeamento de Teclas de Atalho**, toque na tecla de atalho necessária para configurar as configurações da tecla de atalho.
- Na interface da Tecla de Atalho (por exemplo, "F1"), toque em **função** para definir o processo funcional da tecla de atalho, seja como tecla de estado de registro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



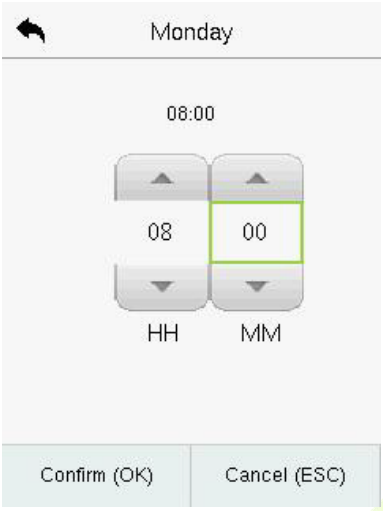
- Se a tecla de atalho for definida como uma tecla de estado de registro (como entrada, saída, etc.), é necessário configurar o valor do estado de registro (valor válido de 0 a 250) e o nome correspondente.

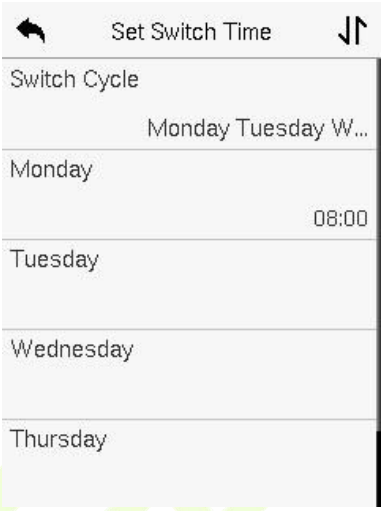
➢ **Defina o Tempo de Alternância:**

- O tempo de alternância é configurado de acordo com as opções de estado de registro.
- Quando o Modo de Estado de Registro é definido como Modo Automático, o tempo de alternância deve ser configurado.
- Na interface da Tecla de Atalho, toque em "Definir Tempo de Alternância" para configurar o tempo de alternância.
- Na interface do Ciclo de Alternância, selecione o ciclo de alternância (segunda-feira, terça-feira, etc.), conforme mostrado na imagem abaixo.



- Após selecionar o ciclo de alternância, defina o tempo de alternância para cada dia e toque em OK para confirmar, conforme mostrado na imagem abaixo.





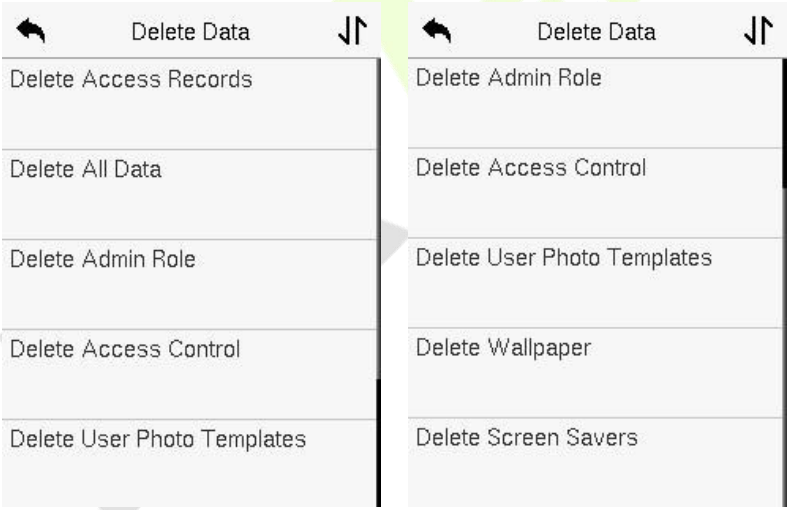
Observação: Quando a função é definida como "Indefinida", o dispositivo não ativará a tecla de estado de registro.

13 Gerenciamento de Dados

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

13.1 Excluir dados

Toque em **Excluir Dados** na interface de **Gerenciamento de Dados** para excluir os dados desejados.

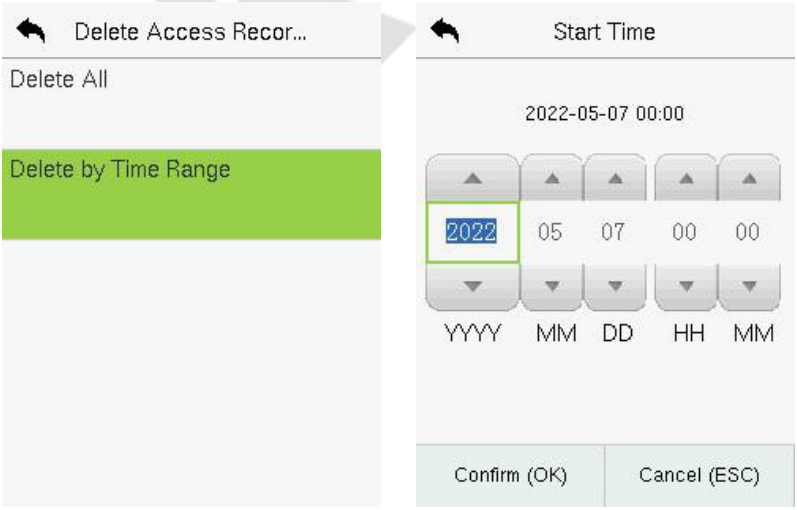


Descrição da Função

Função	Descrição
Excluir reg. de acesso	Para apagar dados de frequência / registros de acesso.

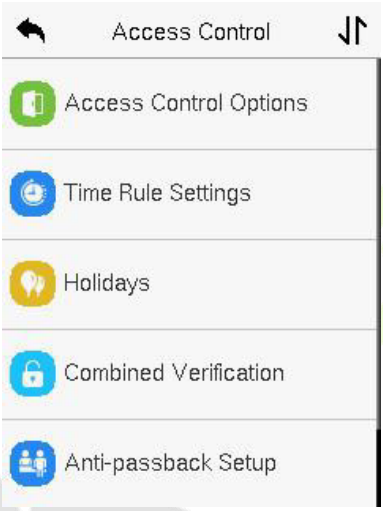
Excluir todos os dados	Para apagar informações e registros de presença / registros de acesso de todos os usuários registrados.
Excluir privilégios de administrador	Para remover todos os privilégios de administrador.
Excluir dados de acesso	Para apagar todos os dados de acesso
Excluir Templates de Fotos de Usuários	Para excluir templates de fotos de usuário no dispositivo. Ao excluir as fotos do template, há um lembrete de risco: "É necessário fazer o novo registro do face após uma atualização do algoritmo."
Apagar Wallpaper	Para excluir todos os papéis de parede no dispositivo.
Apagar Protetores de Tela	Para excluir todos os protetores de tela no dispositivo.

O usuário pode selecionar **Excluir Tudo** ou **Excluir por Intervalo de Tempo** ao deletar os registros de acesso, fotos de presença ou fotos na lista de bloqueio. Ao selecionar **Excluir por Intervalo de Tempo**, é necessário definir um intervalo de tempo específico para excluir todos os dados dentro desse período.



14 Controle de Acesso

No **Menu Principal**, toque em **Controle de Acesso** para configurar o agendamento da abertura da porta, controle de fechaduras e para ajustar outras configurações de parâmetros relacionados ao controle de acesso.

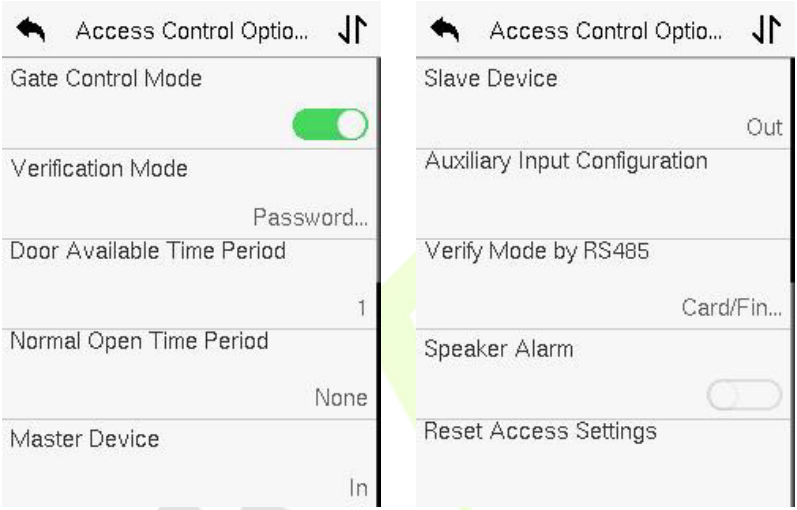


Para obter acesso, o usuário registrado deve cumprir as seguintes condições:

1. O horário de desbloqueio atual da porta relevante deve estar dentro de qualquer fuso horário válido do período de tempo do usuário.
2. O grupo correspondente do usuário deve estar previamente configurado na combinação de desbloqueio da porta (e se houver outros grupos configurados na mesma combinação de acesso, então a autenticação dos membros desses grupos também é necessária para desbloquear a porta).
3. Nas configurações padrão, novos usuários são alocados no primeiro grupo com o fuso horário padrão do grupo, onde a combinação de acesso é "1" e está definida como estado de desbloqueio por padrão.

14.1 Opções de Controle de Acesso

Toque em **Opções de Controle de Acesso** na interface de **Controle de Acesso** para configurar os parâmetros do controle de bloqueio do terminal e dos equipamentos relacionados.



Descrição da Função

Nome da Função	Descrição
Modo de controle de portão/catraca	"Ele alterna entre a opção LIGADO ou DESLIGADO para entrar no modo de controle de portão ou não. Quando definido como LIGADO, a interface remove as opções de relé de fechadura da porta, relé do sensor da porta e tipo de sensor da porta."
Atraso de Fechadura da Porta (s)	O período de tempo durante o qual o dispositivo controla a fechadura elétrica para ficar no estado de desbloqueio. Valor válido: 1~99 segundos.

Atraso do Sensor da Porta (s)	Se a porta não estiver trancada e ficar 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	Há três tipos de sensores: **Nenhum**, **Normalmente Aberto** e **Normalmente Fechado.** **Nenhum:** Significa que o sensor de porta não está em uso. **Normalmente Aberto (NA):** Significa que a porta está sempre aberta quando a energia está ligada. **Normalmente Fechado (NF):** Significa que a porta está sempre fechada quando a energia está ligada
Modos de verificação	Os modos de verificação suportados incluem Senha/Impressão Digital/Cartão/Face, Apenas Impressão Digital, Apenas ID do Usuário, Senha, Apenas Cartão, Impressão Digital/Senha, Impressão Digital/Cartão, ID do Usuário + Impressão Digital, Impressão Digital + Senha, Impressão Digital + Cartão, Impressão Digital + Senha + Cartão, Senha + Cartão, Senha/Cartão, ID do Usuário + Impressão Digital + Senha, Impressão Digital + (Cartão/ID do Usuário), Apenas Face, Face + Impressão Digital, Face + Senha, Face + Cartão, Face + Impressão Digital + Cartão, Face + Impressão Digital + Senha.
Período de Tempo de Disponibilidade da Porta	Define o horário para a porta, de modo que a porta só seja acessível durante esse período.

Período de Tempo Normalmente Aberto	É o período de tempo agendado para o modo 'Normalmente Aberto', de modo que a porta fique sempre aberta durante esse período.
Dispositivo Principal	Ao configurar os dispositivos principal e auxiliar, você pode definir o estado do dispositivo principal como Saída ou Entrada. **Saída:** Um registro de autenticação no dispositivo principal é um registro de saída. **Entrada:** Um registro de autenticação no dispositivo principal é um registro de entrada.
Dispositivo Auxiliar	Ao configurar os dispositivos principal e auxiliar, você pode definir o estado do dispositivo auxiliar como Saída ou Entrada. **Saída:** Um registro de autenticação no dispositivo auxiliar é um registro de saída. **Entrada:** Um registro de autenticação no dispositivo auxiliar é um registro de entrada.
Configuração de Entrada Auxiliar	Define o período de tempo de desbloqueio da porta e o tipo de saída auxiliar do dispositivo de terminal auxiliar. Os tipos de saída auxiliar incluem Nenhum, Acionar abertura da porta, Acionar alarme, Acionar abertura da porta e alarme.
Alarme do Alto-Falante	Ele emite um alarme sonoro ou um alarme de desmontagem local. Quando a porta é fechada ou a autenticação é bem-sucedida, o sistema cancela o alarme local.

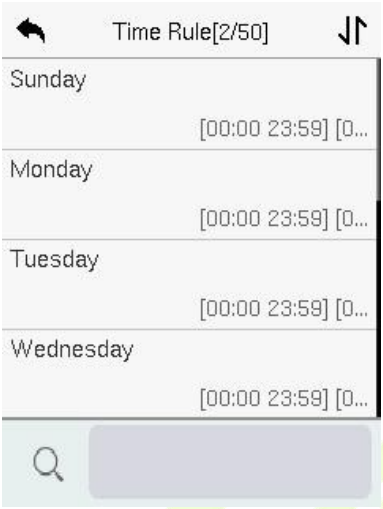
Redefinir Configurações de Acesso	Os parâmetros de redefinição do controle de acesso incluem atraso do fechamento da porta, atraso do sensor da porta, tipo de sensor da porta, modo de verificação, período de tempo disponível da porta, período de tempo de abertura normal, dispositivo principal e alarme. No entanto, os dados de controle de acesso apagados em Gerenciamento de Dados estão excluídos.

14.2 Regra de Tempo

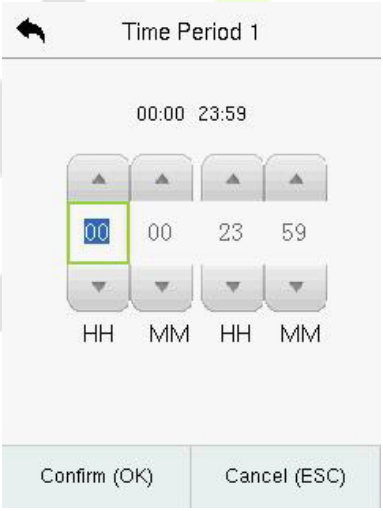
Toque em **Configurações de Regra de Tempo** na interface de Controle de Acesso para configurar as configurações de tempo.

- Todo o sistema pode definir até 50 Períodos de Tempo.
- Cada período de tempo representa 10 Fusos Horários, ou seja, 1 semana e 3 feriados, e cada fuso horário é um período padrão de 24 horas por dia, e o usuário só pode fazer verificações dentro do período de tempo válido
- É possível definir um máximo de 3 períodos de tempo para cada fuso horário. A relação entre esses períodos de tempo é "OU". Assim, quando o horário de autenticação estiver dentro de qualquer um desses períodos de tempo, a autenticação será válida.
- O formato do fuso horário de cada período de tempo é HH MM-HH MM, o qual é preciso até os minutos, de acordo com o relógio de 24 horas.

Toque na caixa cinza para pesquisar o Fuso Horário necessário e especifique o número do Fuso Horário necessário (máximo de até 50 zonas).



Na interface do número do Fuso Horário selecionado, toque no dia necessário (segunda-feira, terça-feira, etc.) para definir o horário.



Especifique o horário de início e de término, e em seguida toque em **OK**.

Observação:

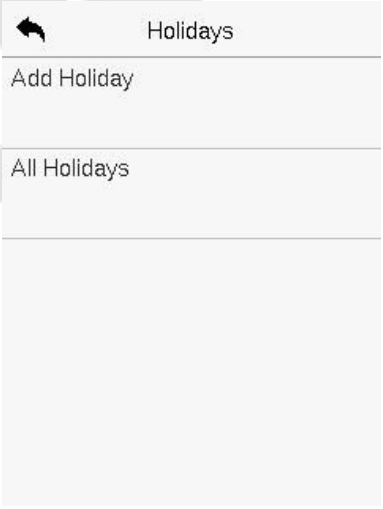
- A porta é inacessível durante todo o dia quando o Horário de Término ocorre antes do Horário de Início (por exemplo **23:57~23:56**).
- É o intervalo de tempo para acesso válido quando o Horário de Término ocorre depois do Horário de Início (por exemplo **08:00~23:59**).
- A porta é acessível durante todo o dia quando o Horário de Término ocorre após o Horário de Início (como no caso em que o Horário de Início é **00:00** e o Horário de Término é **23:59**).

O Fuso Horário padrão 1 indica que a porta está aberta durante todo o dia.

14.3 Feriados

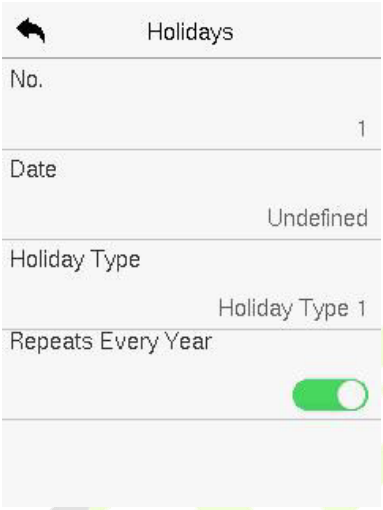
Sempre que houver feriado, poderá necessitar de um horário de acesso especial; mas alterar o horário de acesso de todos um por um é extremamente complicado, então você pode definir um horário de acesso de feriado que seja aplicável a todos os funcionários, e o usuário poderá abrir a porta durante os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

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



➢ Adicionar um novo feriado

oque 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.

14.4 Acesso combinado

Grupos de acesso são organizados em diferentes combinações de desbloqueio de portas para alcançar verificações múltiplas e fortalecer a segurança.

Em uma combinação de desbloqueio de portas, a faixa do número combinado N é **0 ≤ N ≤ 5** e o número de membros N pode pertencer a um único grupo de acesso ou a cinco grupos de acesso diferentes.

Toque em **Autenticação Combinada** na interface de **Controle de Acesso** para configurar a configuração de autenticação combinada.

Na interface de autenticação combinada, toque na Combinação de Desbloqueio de Porta a ser configurada, e toque nas setas **para cima** e **para baixo** para inserir o número da combinação e, em seguida, pressione **OK**.

Exemplo:

- Se a **Combinação de Desbloqueio de Porta 1** for configurada como **(01 03 05 06 08)**, isso indica que a combinação de desbloqueio 1 consiste em 5 pessoas e todas as 5 pessoas são de 5 grupos diferentes, a saber, Grupo de Acesso 1, Grupo de Acesso 3, Grupo de Acesso 5, Grupo de Acesso 6 e Grupo de Acesso 8, respectivamente.
- Se a **Combinação de Desbloqueio de Porta 2** for configurada como (**02 02 04 04 07)**, isso indica que a combinação de desbloqueio 2 consiste em 5 pessoas; as duas primeiras são do Grupo de Acesso 2, as duas seguintes são do Grupo de Acesso 4 e a última pessoa é do Grupo de Acesso 7.

- Se a **Combinação de Desbloqueio de Porta 3** for configurada como **(09 09 09 09 09)**, isso indica que há 5 pessoas nesta combinação; todas elas são do Grupo de Acesso 9.
- Se a **Combinação de Desbloqueio de Porta 4** for configurada como **(03 05 08 00 00)**, isso indica que a combinação de desbloqueio 4 consiste apenas em três pessoas. A primeira pessoa é do Grupo de Acesso 3, a segunda pessoa é do Grupo de Acesso 5 e a terceira pessoa é do Grupo de Acesso 8.

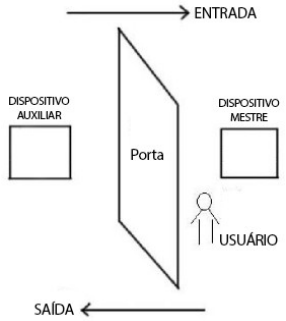
Observação: Para excluir a combinação de desbloqueio de porta, configure todas as combinações de desbloqueio de porta para 0.

14.5 Configuração de anti-passback

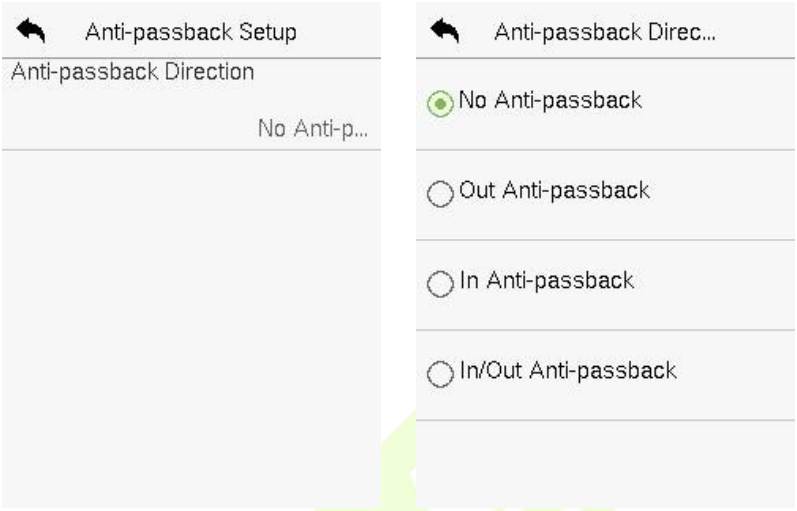
Um usuário pode ser seguido por uma ou mais pessoas para entrar na porta sem verificação, resultando em uma violação de segurança. Portanto, para evitar tais situações, a opção Anti-Passback foi desenvolvida. Uma vez habilitada, o registro de entrada e saída deve ocorrer alternadamente para abrir a porta e representar um padrão consistente.

Essa função requer que dois dispositivos funcionem juntos:

Um dispositivo é instalado no lado interno da porta (dispositivo principal), e o outro é instalado no lado externo da porta (dispositivo escravo). Os dois dispositivos se comunicam por meio do sinal Wiegand. O formato Wiegand e o tipo de saída (ID do usuário/número do cartão) adotados pelo dispositivo principal e pelo dispositivo escravo devem ser consistentes.



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



Descrição da Função

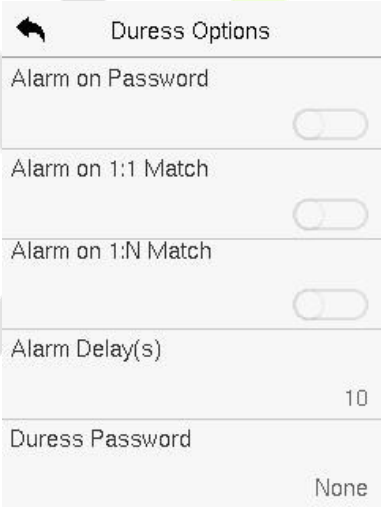
Nome da Função	Descrição
Direção do Anti-Passback	Sem Anti-passback: A função Anti-Passback está desativada, o que significa que a verificação bem-sucedida através do dispositivo principal ou do dispositivo escravo pode destrancar a porta. O estado de comparecimento não é registrado nesta opção. Anti-passback de saída: O usuário só pode fazer o check-out se o último registro for um registro de check-in, caso contrário, um alarme será acionado. No entanto, o usuário pode fazer 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 será acionado. No entanto, o usuário pode fazer check-out livremente.

	Anti-passback de entrada/saída: Nesse caso, um usuário só pode fazer check-in se o último registro for um check-out, ou pode fazer check-out somente se o último registro for um check-in, caso contrário, o alarme é acionado.

14.6 Configurações de Situação de Emergência

Uma vez que um usuário ativa a função de verificação de situação de emergência com um método de autenticação específico (ou métodos), e quando ele/ela está sob coerção e se autentica usando a verificação de situação de emergência, o dispositivo destranca a porta como de costume. Ao mesmo tempo, um sinal é enviado para acionar o alarme também.

Na interface de Controle de Acesso, toque em **Opções de Situação de Emergência** para configurar as configurações de situação de emergência.



Descrição da Função

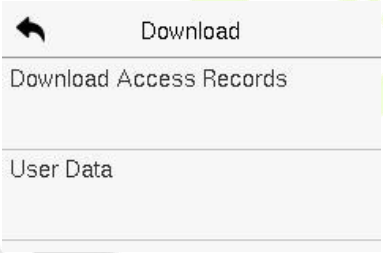
Nome da Função	Descrição
Alarme com Senha	Quando um usuário utiliza o método de verificação de senha, um sinal de alarme será gerado, caso contrário, não haverá sinal de alarme.
Alarme em Verificação 1:1	Quando um usuário utiliza o método de verificação 1:1, um sinal de alarme será gerado; caso contrário, não haverá sinal de alarme.
Alarme em Verificação 1:N	Quando um usuário utiliza o método de verificação 1:N, um sinal de alarme será gerado; 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 seja decorrido. O valor varia de 1 a 999 segundos.
Senha de Emergência	Defina a senha de emergência de 6 dígitos. Quando o usuário inserir essa senha de emergência para verificação, um sinal de alarme será gerado.

15 Gerenciador USB

Você pode importar informações de usuário, dados de acesso e outros dados de uma unidade USB para o computador ou outros dispositivos. Antes de fazer o upload ou download de dados de ou para a unidade USB, insira-a primeiro na porta USB.

Clique em **Gerenciador USB** na interface do menu principal.

15.1 Download

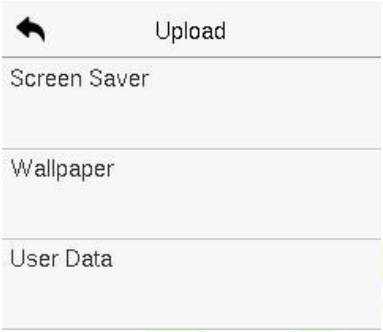


Descrição da Função

Nome da Função	Descrição
Baixar Registros de Acesso	Para baixar os dados de acesso dentro de um período de tempo especificado ou todos os dados para uma unidade USB.
Dados do Usuário	Para baixar todas as informações do usuário do dispositivo para uma unidade USB.

15.2 Upload

Uma vez que a identidade de um usuário é verificada, o registro de acesso é salvo no dispositivo. Essa função permite aos usuários verificar seus registros de eventos.



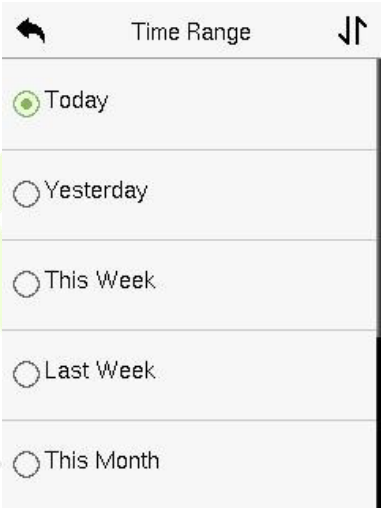
Descrição da Função

Nome da Função	Descrição
Protetor de tela	Para fazer o upload de um protetor de tela de uma unidade USB para o dispositivo. Antes de fazer o upload, você pode selecionar **Enviar imagem selecionada** ou **Enviar todas as imagens**.
Papel de parede	Para fazer o upload de um papel de parede de uma unidade USB para o dispositivo. Antes de fazer o upload, você pode selecionar **Enviar imagem selecionada** ou **Enviar todas as imagens**. As imagens serão exibidas na tela após configurações manuais.
Dados do usuário	Para fazer o upload de todas as informações do usuário de uma unidade USB para o dispositivo.

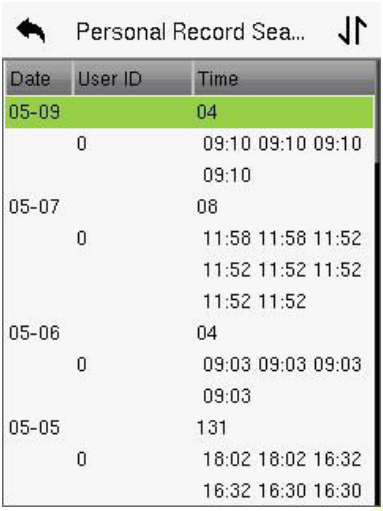
16 Procurar registros

Uma vez que a identidade de um usuário é verificada, o registro de acesso é salvo no dispositivo. Essa função permite que os usuários verifiquem seus registros de eventos.
Selecione **Procurar Registros** na interface do Menu Principal para buscar os registros de eventos necessários.

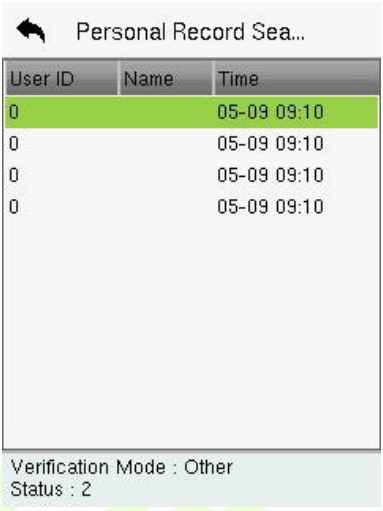
1. Insira o ID do usuário a ser pesquisado e clique em OK. Se desejar pesquisar logs de todos os usuários, clique em OK sem inserir nenhum ID de usuário.



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



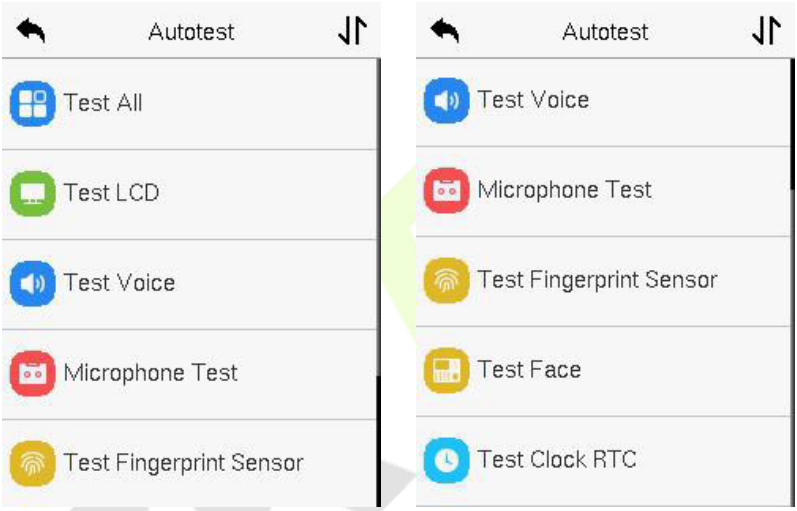
3. Depois que a pesquisa de log for bem-sucedida, toque no registro destacado em verde para visualizar seus detalhes.



4. A figura mostra os detalhes do log selecionado.

17 Autoteste

Selecione **Menu Principal**, toque em **Autoteste**. Isso permite que o sistema teste automaticamente se as funções de vários módulos estão funcionando normalmente, incluindo o LCD, Voz, Microfone, Impressão Digital, Câmera e Relógio em Tempo Real (RTC).



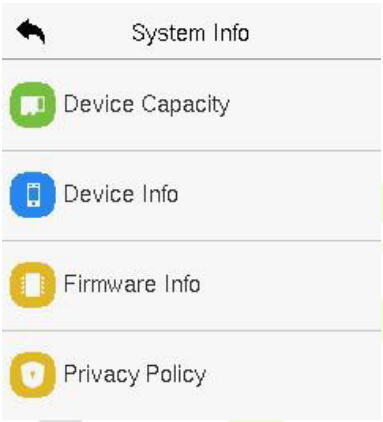
Descrição da Função

Nome da Função	Descrição
Testar Todos	Para testar automaticamente se o LCD, Voz, Microfone, Impressão Digital, Câmera e Relógio em Tempo Real (RTC) estão normais.
Testar o LCD	Para testar automaticamente o efeito de exibição da tela LCD, exibindo cores completas, branco puro e preto puro para verificar se a tela exibe cores normalmente.

Testar Voz	Para testar automaticamente se os arquivos de áudio armazenados no dispositivo estão completos e se a qualidade do som está boa.
Teste do Microfone	Para testar se o microfone está funcionando corretamente, fale no microfone.
Testar o Sensor de Impressão Digital	Para testar o sensor de impressão digital, pressione um dedo no scanner para verificar se a imagem da impressão digital adquirida está clara. Quando você pressionar um dedo no scanner, a imagem da impressão digital será exibida na tela.
Testar Face	Testar se a câmera funciona corretamente verificando as fotos tiradas para ver se estão suficientemente claras.
Testar o Relógio em Tempo Real	Para testar o RTC. O dispositivo testa se o relógio funciona normalmente e com precisão com um cronômetro. Toque na tela para iniciar a contagem e pressione novamente para parar a contagem.

18 Informação do sistema

No Menu Principal, toque em **Informação do sistema** para visualizar o status de armazenamento, as informações da versão do dispositivo, informações do firmware e a política de privacidade.



Descrição da Função

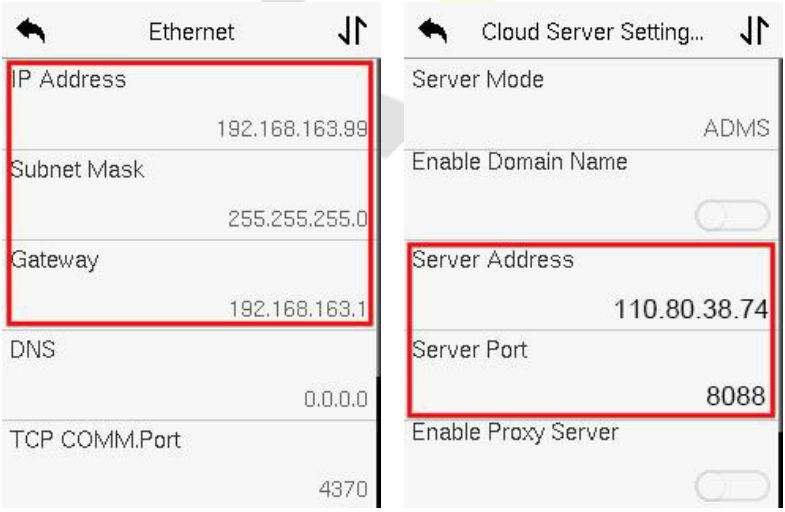
Nome da Função	Descrição
Capacidade do Dispositivo	Exibe o armazenamento atual do usuário do dispositivo, armazenamento de impressões digitais, cartão, senha e rosto, administradores e registros.
Informações do Dispositivo	Exibe o nome do dispositivo, número de série, endereço MAC, algoritmo de impressão digital, algoritmo de rosto, informações da plataforma, versão do MCU, fabricante e data de fabricação.
Informações do Firmware	Exibe a versão do firmware e outras informações de versão do dispositivo.
Política de Privacidade	Exibe a política de privacidade do dispositivo.

19 Conectar ao Software ZKBioAccess IVS

19.1 Configurar o Endereço de Comunicação

➢ **Lado do Dispositivo**

1. Toque em **Conf. Com.** > **Ethernet** no menu principal para configurar o endereço IP e o gateway do dispositivo.
(**Observação:** O endereço IP deve ser capaz de se comunicar com o servidor ZKBioAccess IVS, de preferência no mesmo segmento de rede que o endereço do servidor).
2. No menu principal, clique em **Conf. Com.** > **Configuração do Servidor de Nuvem** para configurar o endereço do servidor e a porta do servidor.
Endereço do servidor: Configure o endereço IP do servidor ZKBioAccess. **Porta do servidor:** Configure a porta do servidor ZKBioAccess (O padrão é 8088).



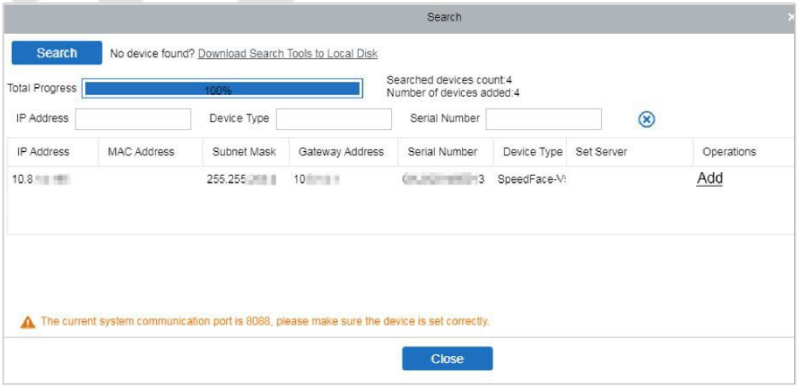
➢ **Lado do Software**

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

19.2 Adicionar Dispositivo no Software

Adicione o dispositivo por meio da busca. O processo é o seguinte:

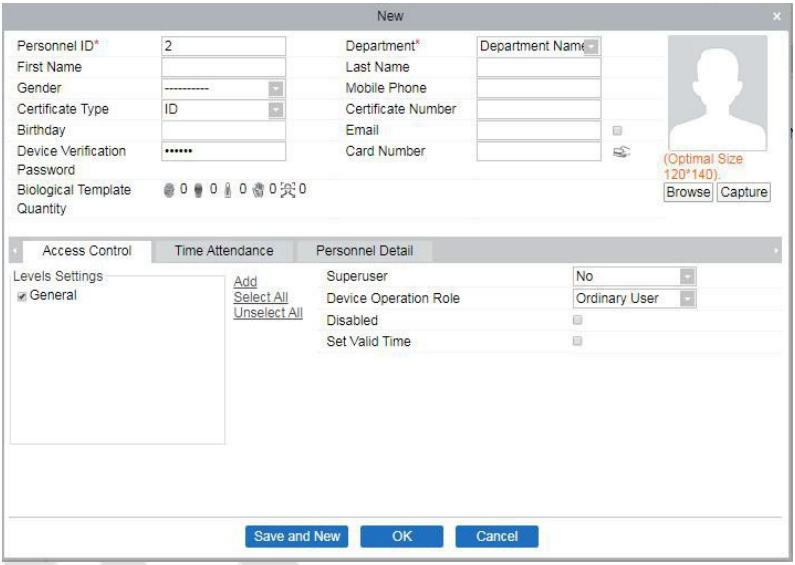
1. Clique em **Presença > Dispositivo de Presença > Dispositivo > Buscar**, para abrir a interface de Busca no software.
2. Clique em **Buscar** e isso irá mostrar [**Buscando...**].
3. Após a busca, a lista e o número total de controladores de acesso serão exibidos.



4. Clique em Adicionar na coluna de operação, uma nova janela irá aparecer. Selecione Área de Presença e Fuso Horário de cada menu suspenso e clique em OK para adicionar o dispositivo.

19.3 Adicionar Pessoal no Software

1. Clique em **Pessoal** > **Pessoa** > **Nova**:



2. Preencha todos os campos obrigatórios e clique em **OK** para registrar um novo usuário.

3. Clique em **Presença > Dispositivo de Presença > Dispositivo > Controle > Sincronizar Dados do Software** para o Dispositivo para sincronizar todos os dados no dispositivo, incluindo os novos usuários.

   Para mais detalhes, consulte o Manual do Usuário do ZKBioAccess IVS.

Apêndice 1

Requisitos para Cadastro Facial no equipamento:

1) É recomendável realizar o registro em um ambiente interno com uma fonte de luz apropriada, sem subexposição ou superexposição no rosto.
2) Não posicione o dispositivo em direção a fontes de luz externa, como portas ou janelas, ou outras fontes de luz intensa.
3) São recomendadas roupas de cores escuras, diferentes da cor de fundo, para o registro.
4) Exponha seu rosto e testa adequadamente e não cubra seu rosto e sobrancelhas com o cabelo.
5) É recomendável mostrar uma expressão facial normal. (Um sorriso é aceitável, mas não feche os olhos ou incline a cabeça para qualquer direção).
6) Duas imagens são necessárias para pessoas com óculos, uma imagem com óculos e outra sem eles.
7) Não use acessórios como lenço ou máscara que possam cobrir sua boca ou queixo.
8) Por favor, vire-se para a direita em direção ao dispositivo de captura e posicione seu rosto na área de captura de imagem, conforme mostrado na imagem abaixo.
9) Não inclua mais de um rosto na área de captura.
10) Uma distância de 50cm a 80cm é recomendada para a captura da imagem. (a distância é ajustável, dependendo da altura do corpo).

Requisitos para Upload de fotos no software

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

- **Distância dos olhos**

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

- **Expressão Facial**

Rosto neutro ou sorriso simples e olhos naturalmente abertos são recomendados

- **Gesto e ângulo**

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

- **Acessórios**

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

- **Face**

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

- **Formato de imagem**

Deve estar em BMP, JPG, ou JPEG.

- **Requisito de dados**

Deve seguir os requisitos:

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

Apêndice 2

Política de Privacidade

Aviso:

Para ajudar você a utilizar melhor os produtos e serviços da ZKTeco e suas afiliadas, doravante referidas como "nós", "nossa" ou "nos", o provedor de serviços inteligentes, coletamos constantemente suas informações pessoais. Como compreendemos a importância de suas informações pessoais, levamos sua privacidade a sério e formulamos esta política de privacidade para proteger suas informações pessoais. Abaixo, listamos as políticas de privacidade para que você compreenda precisamente os dados e as medidas de proteção à privacidade relacionados 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

Vamos coletar as informações fornecidas voluntariamente por você ou autorizadas por você durante o registro e uso, ou geradas como resultado do seu uso dos serviços.

1. **Informações de Registro do Usuário: No seu primeiro registro, o template de características (template de impressão digital/template de rosto/template de palma)** será salvo no dispositivo de acordo com o tipo de dispositivo que você selecionou para verificar a similaridade única entre você e o ID do usuário que você registrou. Você também pode opcionalmente inserir seu Nome e Código.

As informações acima são necessárias para que você possa usar nossos produtos. Se você não fornecer tais informações, não poderá utilizar algumas funcionalidades 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 em que nossos serviços são usados serão coletadas quando o produto estiver conectado ao software, incluindo o Modelo do Produto, Número da Versão do Firmware, Número de Série do Produto e Informações de Capacidade do Produto. **Ao conectar seu produto ao software, por favor, leia atentamente a política de privacidade específica do software.**

II. Segurança e Gerenciamento do Produto

1. Ao utilizar nossos produtos pela primeira vez, você deve definir o privilégio de Administrador antes de realizar operações específicas. Caso contrário, você será lembrado com frequência para definir o privilégio de Administrador ao entrar na interface do menu principal. **Se você ainda não definir o privilégio de Administrador após receber o aviso do sistema, deve estar ciente do possível risco de segurança (por exemplo, os dados podem ser modificados manualmente).**

2. Todas as funções de exibição das informações biométricas estão desativadas por padrão em nossos produtos. 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 da privacidade pessoal especificados na política de privacidade.a

3. Apenas o 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. **Se você**

optar por exibir tais informações, assumimos que você está ciente dos possíveis riscos de segurança (por exemplo, sua foto será exibida na interface do dispositivo).

4. A função da câmera é desativada por padrão em nossos produtos. Se você desejar habilitar essa função para tirar fotos de si mesmo para registro de presença ou tirar fotos de estranhos para controle de acesso, o produto ativará o tom de aviso da câmera. **Uma vez que você habilite essa função, assumimos que você está ciente dos possíveis riscos de segurança.**

5. Todos os dados coletados por nossos produtos são criptografados usando o algoritmo AES 256. Todos os dados enviados pelo Administrador para nossos produtos são automaticamente criptografados usando o algoritmo AES 256 e armazenados com segurança. Se o Administrador fizer o download de dados de nossos produtos, assumimos que você precisa processar os dados e está ciente dos possíveis riscos de segurança. Nesse caso, você deve assumir a responsabilidade pelo armazenamento dos dados. Saiba que alguns dados não podem ser baixados por razões de segurança de dados.

6. Todas as informações pessoais em nossos produtos podem ser consultadas, modificadas ou excluídas. Se você não utilizar mais nossos produtos, por favor, limpe seus dados pessoais.

III. Como lidamos com informações pessoais de menores

Nossos produtos, site e serviços são principalmente projetados para adultos. Sem o consentimento dos pais ou responsáveis legais, os menores não devem criar suas próprias contas. Se você for menor de idade, é recomendável que peça aos seus pais ou responsável legal que leiam atentamente esta Política e só use nossos serviços ou informações fornecidas por nós com consentimento de seus pais ou responsável legal.

Usaremos ou divulgaremos informações pessoais de menores coletadas

com o consentimento de seus pais ou responsáveis legais, na medida em que tal uso ou divulgação seja permitido por lei ou tenhamos obtido o consentimento explícito de seus pais ou responsáveis legais, e tal uso ou divulgação seja com o objetivo de proteger menores.

Ao perceber que coletamos informações pessoais de menores sem o consentimento prévio de pais verificáveis, excluiremos tais informações o mais rápido possível.

IV. Outros

Você pode visitar https://www.zkteco.com/cn/index/Index/privacy_protection.html para saber mais 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, continuaremos a deliberar 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)	Mercúrio (Hg)	Cádmio (Cd)	Crómio hexavalente (Cr6+)	Bifenilos Polibro (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