Manual do Usuário

SpeedFace-V5L (ZAM180)

Revisão do documento: V1.5.03.2025

Versão de firmware: ZAM180-NF50VA-Ver.4.1.4

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.

Copyright © 2023 ZKTECO CO., LTD. Todos os direitos reservados.

Marca Registrada

ZKTeco é uma marca registrada da ZKTeco. Outras marcas comerciais envolvidas neste manual são propriedade de seus respectivos proprietários.

Responsabilidade

Este manual contém informações sobre a operação e manutenção dos produtos ZKTeco. Os direitos de propriedade intelectual de todos os documentos, desenhos, etc., em relação aos produtos fornecidos pela ZKTeco são de propriedade da ZKTeco.

O conteúdo deste documento não deve ser usado ou compartilhado pelo receptor com terceiros sem a permissão expressa por escrito da ZKTeco. O conteúdo deste manual deve ser lido na íntegra antes de iniciar a utilização e manutenção do produto adquirido. Se algum dos conteúdos do manual parecer pouco claro ou incompleto, entre em contato com a ZKTeco antes de iniciar a utilização e/ou manutenção do referido produto.

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

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

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

A ZKTeco reserva-se o direito de adicionar, apagar, alterar ou modificar as informações contidas no manual de tempos em tempos, independente de aviso prévio, por meio de circulares, cartas, notas e/ou novas edições do manual, visando a melhor utilização e/ou segurança do produto.

Os mais recentes procedimentos de utilização e documentos relevantes estão disponíveis em http://www.zkteco.com.br/ sendo de responsabilidade do usuário verificar eventuais atualizações e informes, especialmente se o produto indicar problemas no funcionamento ou se restarem dúvidas sobre sua instalação, manejo, armazenamento, operação e/ou manutenção.

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

ZKTeco filial Brasil

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

Telefone +55 31 3055-3530

Para dúvidas relacionadas a negócios, escreva para nós em: comercial.brasil@zkteco.com

Para saber mais sobre nossas filiais globais, visite www.zkteco.com.br.

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

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

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

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

Módulo IC01 (M330-L_V34): "Incorpora produto homologado pela ANATEL sob número 12509-20-12720"

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

Módulo L287B-SR: "Incorpora produto homologado pela ANATEL sob número 11891-22-11470

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

Sobre a Empresa

A ZKTeco é uma das 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 V5L.**

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.

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. Por exemplo, **OK, Confirmar, Cancelar**.
>	Os menus de vários níveis são separados por esses colchetes. Por exemplo, 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 importante
	Cuidado para evitar perigos ou erros
	Declaração ou evento que avisa sobre algo ou que serve como um exemplo de advertência

Índice

DECLARAÇÃO DE SEGURANÇA DE DADOS

Como fornecedor de produtos inteligentes, talvez precisemos conhecer e coletar algumas de suas informações pessoais para melhor auxiliá-lo no uso de nossos produtos e serviço. Assim sendo, trataremos sua privacidade com cuidado de acordo com nossa Política de Privacidade.

Por favor, leia e entenda completamente todos os regulamentos da política de proteção de privacidade e pontos-chave que aparecem no dispositivo antes de usar nossos produtos.

Como usuário do produto, você deve cumprir as leis e regulamentos aplicáveis relacionados à proteção de dados pessoais ao coletar, armazenar e usar dados pessoais, incluindo, entre outros, tomar medidas de proteção para dados pessoais, tais como realizar gerenciamento de direitos para dispositivos, fortalecer a segurança física de cenários de aplicação de dispositivos e assim por diante

MEDIDAS DE SEGURANÇA

As instruções abaixo visam garantir que o usuário possa usar o produto corretamente para evitar perigos ou perdas materiais. As seguintes precauções são para manter os usuários seguros e evitar qualquer dano. Por favor, leia atentamente antes da instalação.

O descumprimento das instruções pode causar danos ao produto ou lesões físicas (pode até causar a morte).

1. **Leia, siga e retenha as instruções** - Todas as instruções operacionais e de segurança devem ser lidas e seguidas corretamente antes de colocar o dispositivo em funcionamento.
2. **Não ignore os avisos** - Siga todos os avisos na unidade e nas instruções de operação.
3. **Acessórios** - Use somente acessórios recomendados pelo fabricante ou vendidos pelo produto. Por favor, não use nenhum outro componente além dos materiais sugeridos pelo fabricante.
4. **Precauções para a instalação** – Não coloque este dispositivo em um suporte ou estrutura instável, uma vez que pode cair e causar ferimentos graves em pessoas e danos ao aparelho.
5. **Manutenção** - Não tente consertar esta unidade por conta própria. Abrir ou remover tampas pode expor você a tensões perigosas ou outros perigos.
6. **Danos que requerem manutenção**- Desconecte o sistema da fonte de alimentação CA ou CC e leve para o serviço de manutenção nas seguintes condições:

   - Quando o controle do cabo ou da conexão é afetado.
   - Quando o líquido derramar ou um item cair no sistema.
   - Se exposto à água ou devido ao mau tempo (chuva, neve e muito mais).
   - Se o sistema não estiver funcionando normalmente, consulte as instruções de operação.

   Apenas altere os controles definidos nas instruções de operação. O ajuste inadequado dos controles pode causar danos e envolver um técnico qualificado para retornar o dispositivo à operação normal. Não conecte vários dispositivos a um único adaptador de energia, pois a sobrecarga do adaptador pode causar superaquecimento e risco de incêndio.
7. **Peças de reposição** - Quando forem necessárias peças de reposição, os técnicos de manutenção devem usar apenas peças de reposição fornecidas pelo fornecedor. Substitutos não autorizados podem resultar em queimaduras, choques ou outros perigos.
8. **Verificação de segurança** - Após a conclusão do serviço ou reparo na unidade, peça ao técnico para realizar verificações de segurança para garantir a operação adequada do dispositivo.

9. **Fonte de alimentação** - Opere o sistema apenas com a fonte de alimentação indicada. Se o tipo de fonte de alimentação a ser usado não estiver explicito, entre em contato com seu revendedor.
10. **Raios** -Para-raios externos podem ser instalados para proteção contra tempestades elétricas. Os dispositivos devem ser instalados em áreas com acesso limitado.

Segurança elétrica

- Antes de conectar um cabo externo ao dispositivo, complete o aterramento corretamente e configure a proteção contra surtos; caso contrário, a eletricidade estática danificará a placa mãe.
- Certifique-se de que a energia foi desconectada antes de conectar, instalar ou desmontar o dispositivo.
- Certifique-se de que o sinal conectado ao dispositivo seja um sinal de corrente fraca (interruptor); caso contrário, os componentes do dispositivo serão danificados.
- Certifique-se de que a voltagem padrão aplicável em seu país ou região seja aplicada. Se você não tiver certeza sobre a tensão padrão endossada, consulte sua empresa de energia elétrica local. A incompatibilidade de energia pode causar um curto-circuito ou danos ao dispositivo.
- Em caso de danos na fonte de alimentação, devolva o dispositivo ao pessoal técnico profissional ou ao seu revendedor para manuseio.
- Para evitar interferência, mantenha o dispositivo longe de dispositivos de alta radiação eletromagnética, como geradores (incluindo geradores elétricos), rádios, televisores, monitores (especialmente CRT) ou alto-falantes.

Segurança da Operação

- Se fumaça, odor ou ruído subirem do dispositivo, desligue a energia imediatamente e desconecte o cabo de alimentação e, em seguida, entre em contato com o centro de serviço.
- O transporte e outras causas imprevisíveis podem danificar o hardware do dispositivo. Verifique se o dispositivo apresenta algum dano intenso antes da instalação.
- Se o dispositivo tiver grandes defeitos que você não consiga resolver, entre em contato com o revendedor o mais rápido possível.
- Poeira, umidade e mudanças bruscas de temperatura podem afetar a vida útil do dispositivo. Aconselha-se a não manter o dispositivo em tais condições.
- Não mantenha o dispositivo em um local que vibre. Manuseie o dispositivo com cuidado. Não coloque objetos pesados em cima do aparelho.
- Não aplique resina, álcool, benzeno, pesticidas e outras substâncias voláteis que possam danificar o gabinete do dispositivo. Limpe os acessórios do aparelho com um pano macio ou uma pequena quantidade de agente de limpeza.
- Se você tiver alguma dúvida técnica sobre o uso, entre em contato com pessoal técnico certificado ou experiente.

Nota:

- Certifique-se de que a polaridade positiva e a polaridade negativa da fonte de alimentação DC 12V estejam conectadas corretamente. Uma conexão reversa pode danificar o dispositivo. Não é aconselhável conectar a fonte de alimentação AC 24V à porta de entrada DC 12V.
- Certifique-se de conectar os fios seguindo a polaridade positiva e a polaridade negativa mostradas na placa de identificação do dispositivo.
- O serviço de garantia não cobre danos acidentais, danos causados por operação incorreta e danos devido à instalação independente ou reparo do produto pelo usuário

1 Visão geral

O SpeedFace-V5L utiliza algoritmos inteligentes de reconhecimento facial e a mais recente tecnologia de visão computacional. Ela oferece suporte a impressão digital e verificação facial com grande capacidade e reconhecimento rápido. A câmera facial também suporta QR Code com aplicativo móvel, melhorando o desempenho de segurança em todos os aspectos.

O SpeedFace-V5L adota tecnologia de reconhecimento sem contato e identificação individual com máscara, eliminando efetivamente preocupações de higiene. Ele também está equipado com um algoritmo antifraude evoluído para reconhecimento facial e palma, contra quase todos os tipos de ataques com fotos e vídeos falsos.

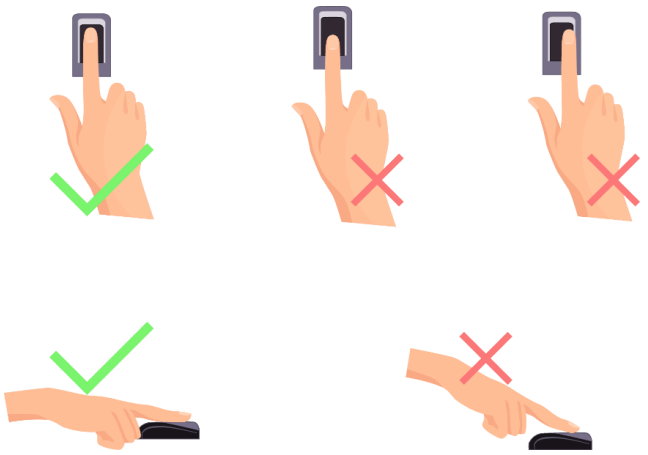
O SpeedFace-V5L oferece suporte a vídeo porteiro, além de serem integrados ao protocolo de vídeo ONVIF, permitindo que se conectem a NVRs para vigilância e gravação de vídeo.

2 Instruções de Uso

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

2.1 Posicionamento dos dedos

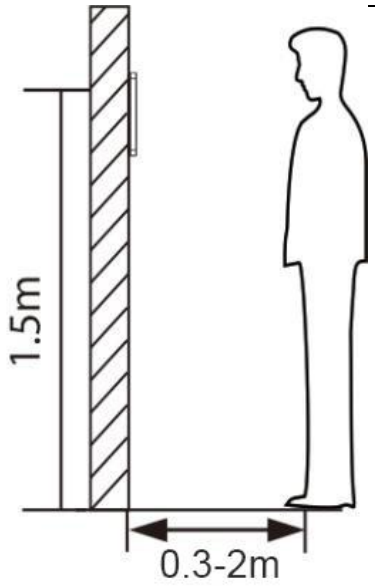
Dedos recomendados: Indicador, médio ou anelar; evite usar o polegar ou o mindinho, pois é difícil pressioná-los com precisão no leitor de impressões digitais.



Observação: Utilize o método correto ao pressionar seus dedos no leitor de impressões digitais para cadastro e autenticação. Nossa empresa não assume nenhuma responsabilidade por problemas de reconhecimento ocasionados pelo uso incorreto do produto. Reservamos o direito de interpretação final e modificação em relação a este ponto.

2.2 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, de forma natural durante o cadastro/autenticação.

2.3 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 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, sobrancelhas e orelhas.
- Não use chapéus, bonés, máscaras, óculos de grau, óculos de sol durante o cadastro.
- Tenha cuidado para não exibir duas faces na tela. Cadastre uma pessoa por vez.
- Recomenda-se que um usuário que utilize óculos cadastre s faces, tirando e colocando o óculos durante o cadastro.

Recomendações durante a autenticação facial:

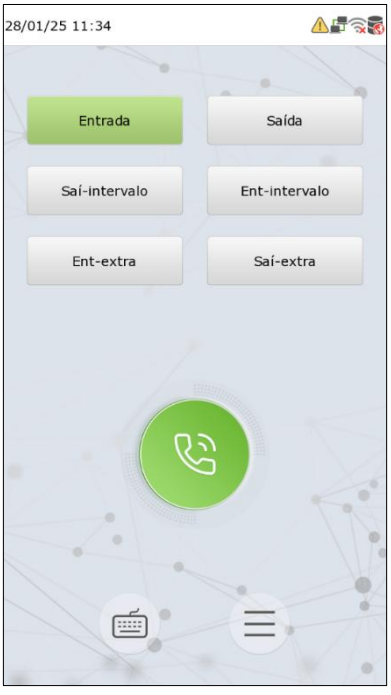
- Certifique-se de que a face apareça dentro da linha guia exibida na tela do dispositivo.
- Se os óculos foram trocados, a autenticação pode falhar. Se a face sem óculos tiver sido cadastrada, autentique sem óculos. Se a face com óculos foi cadastrada, autentique com os óculos.
- Se uma parte da face 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 a face, sobrancelhas e as orelhas.

2.4 Tela principal

Após conectar a fonte de alimentação e o equipamento ligar por completo, a seguinte tela será exibida:

Nota:

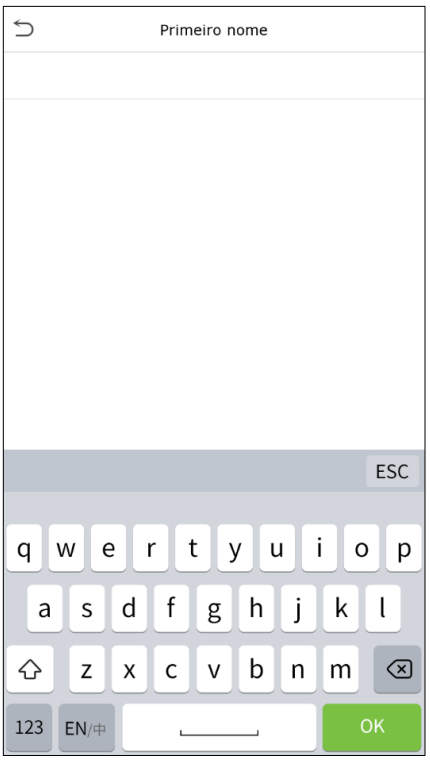
- Clique em para autenticar com o ID do usuário.
- Quando não houver um super administrador cadastrado no dispositivo, clique em para ir ao menu.
- Após adicionar um Super Administrador no dispositivo, é necessário a verificação do Super Administrador antes de abrir as funções de menu. **Observação**: Para a segurança do dispositivo, é recomendado cadasdtrar um super administrador na primeira vez que você usar o dispositivo.
- As opções de status de registro de presença também podem ser exibidas e usadas diretamente na tela de espera. Toque em qualquer lugar da tela, exceto nos ícones, e seis teclas de atalho aparecerão na tela, conforme mostrado na figura abaixo:



- Pressione a tecla do estado de presença desejado para selecionar o seu estado de presença atual, que será exibido em verde.

Observação: As opções de status de registro de presença estão desativadas por padrão e é necessário selecionar outras opções de modo "***Menu>Personalização>Config. Status de ponto***" para exibir as opções de status de registro de presença na tela de espera.

2.5 Teclado Virtual



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

- Clique em [**En**] para alternar para o teclado em inglês.
- Pressione [**123**] para alternar para o teclado numérico e simbólico.
- Clique em [**ABC**] para retornar ao teclado alfabético.
- Clique na caixa de entrada para o teclado virtual ser exibido.
- Clique em [**ESC**] para sair do teclado virtual.

2.6 Modos de autenticação

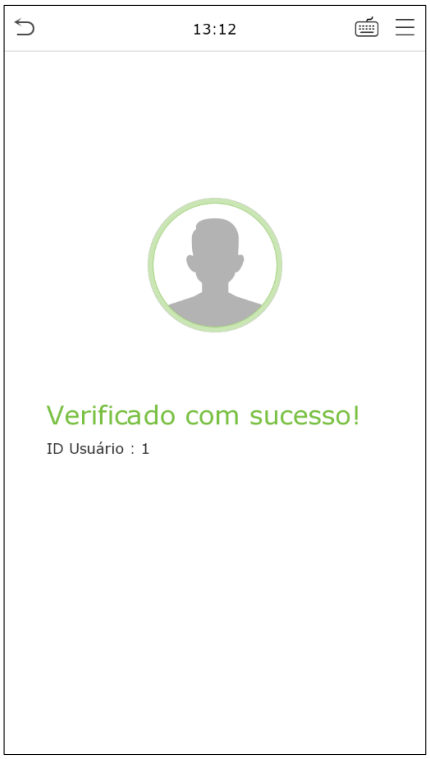
2.6.1 Autenticação de impressão digital

- **Modo de autenticação de impressão digital 1: N**

Compara a impressão digital que está sendo pressionada no leitor de impressões digitais com todos os dados de impressão digital armazenados no dispositivo.

O dispositivo entra no modo de autenticação de impressão digital quando o usuário pressiona o dedo no leitor de impressões digitais.

Por favor, siga a maneira correta de posicionar o seu dedo no sensor. Para mais detalhes, consulte a seção Posicionamento dos Dedos.



Autenticação bem-sucedida

Autenticação falhou

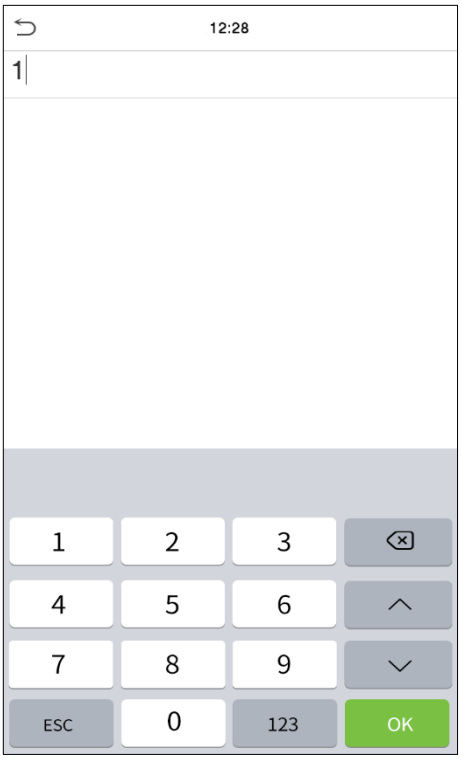
- **Modo de autenticação de impressão digital 1:1**

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

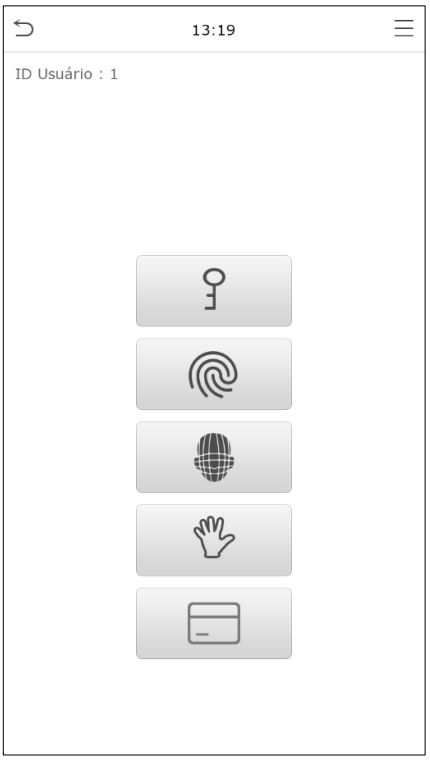
Os usuários podem verificar suas identidades no modo de verificação 1:1 quando não conseguem ter acesso com o método de autenticação 1:N.

Pressione na tela principal e entre no modo de autenticação de impressão digital 1:1

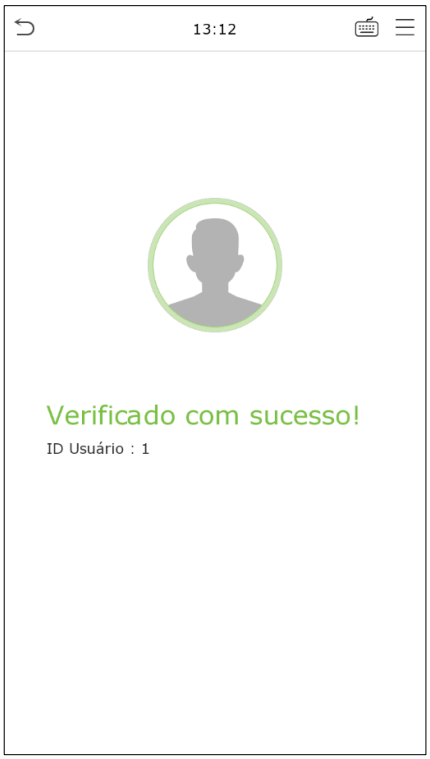
Digite o ID do usuário e clique em [**OK**].



Se o usuário tiver cadastrado outras credenciais, além das impressões digitais, e o método de verificação estiver definido como verificação de senha/impressão digital/face, a seguinte tela aparecerá. Selecione o ícone de impressão digital para entrar no modo de verificação de impressão digital.



Pressione a impressão digital para verificar.



Autenticação bem-sucedida

Autenticação falhou

2.6.2 Autenticação por cartão

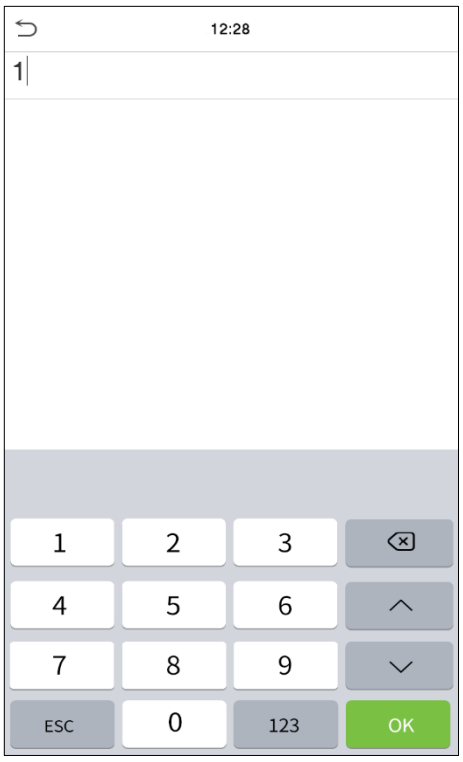
- **Modo de autenticação por cartão 1: N**

O modo de autenticação por cartão 1:N compara o número do cartão lido com todos os números de cartão cadastrados no dispositivo; A seguir está a tela de autenticação de cartão:

- **Modo de autenticação por cartão 1:1**

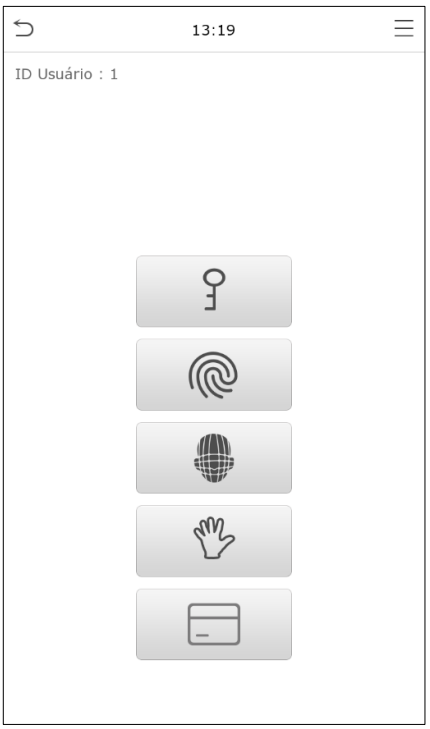
O modo de autenticação por cartão 1:1 compara o número do cartão lido com o número associado ao ID de usuário mencionado e cadastrado no dispositivo.

Selecione na tela principal para abrir o modo de autenticação de cartão 1:1.



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

Se um funcionário registrar uma impressão digital além do cartão, a seguinte tela aparecerá. Selecione o ícone para entrar no modo de verificação do cartão.



Aqui estão as telas de exibição após inserir um cartão correto e um cartão incorreto, respectivamente:

Autenticação bem-sucedida

Autenticação falhou

2.6.3 Autenticação facial

- **Modo de autenticação facial 1:N**

Verificação convencional

Neste modo de verificação, o dispositivo compara as imagens faciais coletadas com todos os dados faciais cadastrados no dispositivo. A seguir está a tela de um resultado de autenticação bem-sucedido

Detecção de máscara ativada

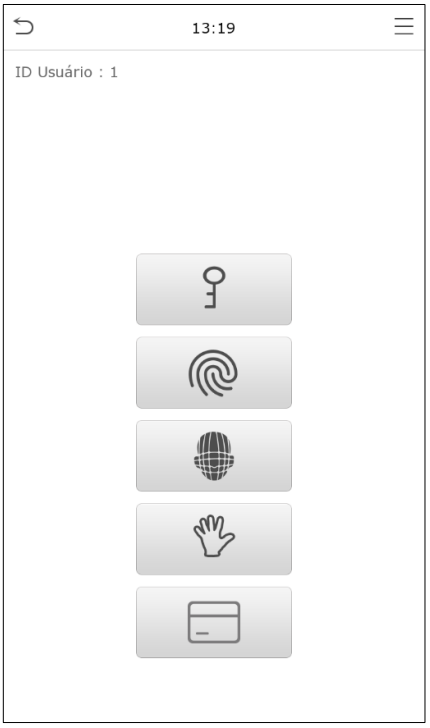
Quando o usuário habilita a função de detecção de máscara, o dispositivo identificará se o usuário está usando máscara ou não durante a verificação. A seguir estão as janelas do resultado da autenticação.

- **Modo de autenticação facial 1:1**

Compare a face capturada pela câmera com o cadastro facial relacionado ao ID do usuário inserido. Pressione na tela principal para entrar no modo de verificação facial 1:1.

Digite o ID do usuário e clique em OK.

Se o usuário cadastrou outros métodos de autenticação além da face, a seguinte tela aparecerá:



Após a verificação bem-sucedida, será exibida a mensagem "Verificado com sucesso", conforme mostrado abaixo:

Se a verificação falhar, será exibida a mensagem "Ajuste a sua posição!".

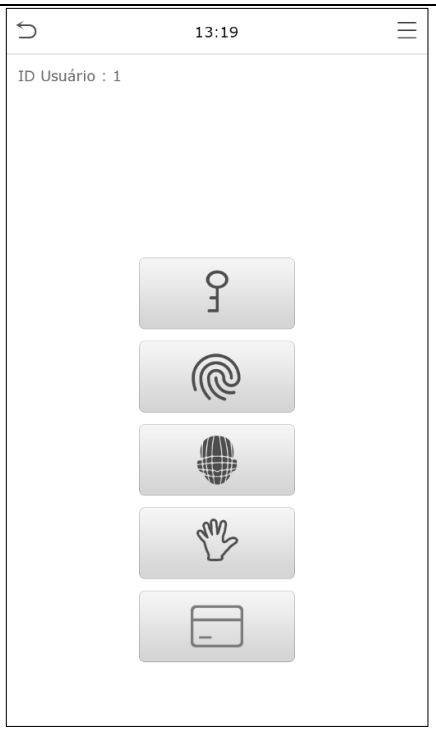
2.6.4 Autenticação por senha

O dispositivo compara a senha inserida com a senha cadastrada do ID do usuário fornecido. Toque no botão na tela principal para entrar no modo de verificação de senha 1:1.

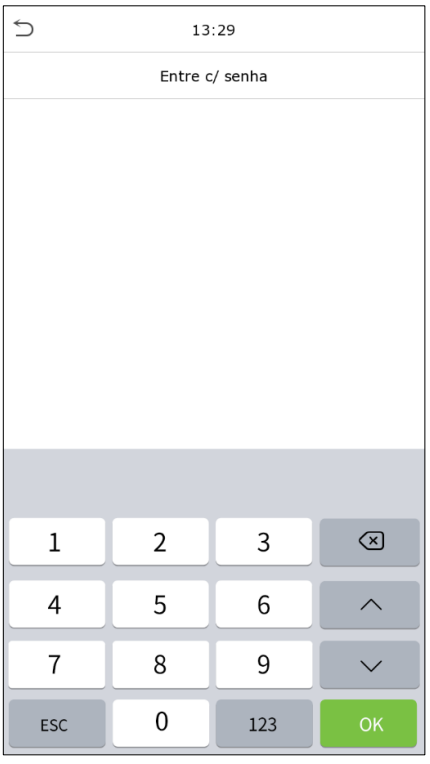
Em seguida, insira o ID do usuário e pressione OK

Se o usuário cadastrou outros métodos de autenticação além da face, a seguinte tela aparecerá:

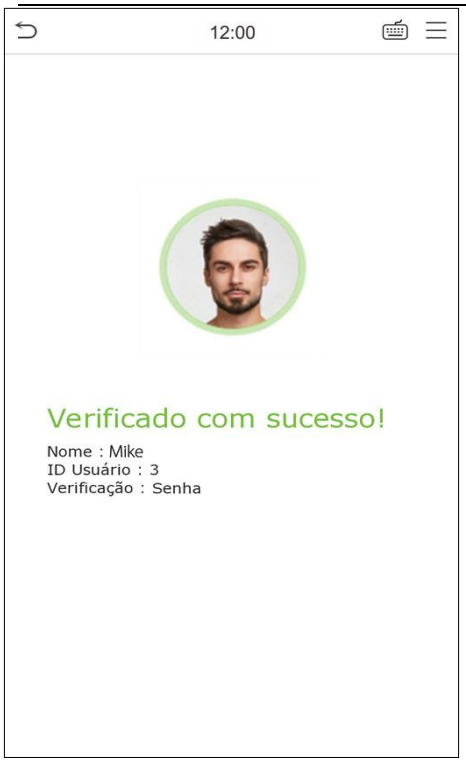
Selecione para entrar no modo de verificação por senha



Digite a senha e pressione **OK.**



Aqui estão as telas de exibição após inserir uma senha correta e uma senha incorreta, respectivamente:

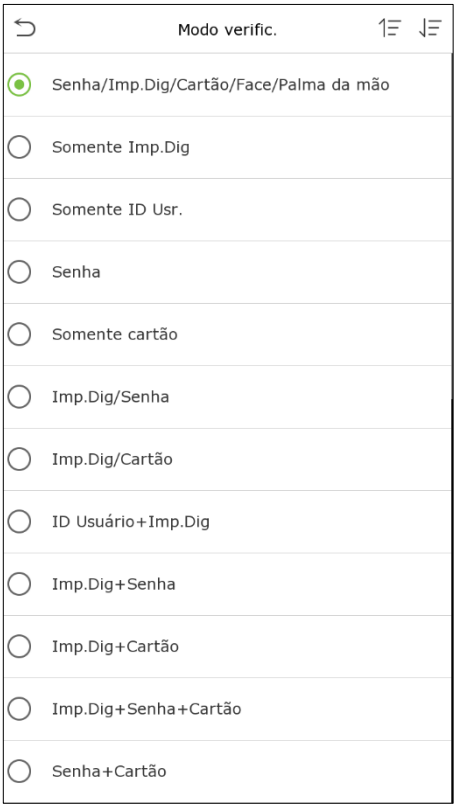


Autenticação bem-sucedida

Autenticação falhou

2.6.5 Autenticação combinada

Para aumentar a segurança, este dispositivo oferece a opção de usar múltiplos métodos de autenticação.



Procedimento para configurar o modo de autenticação combinada.

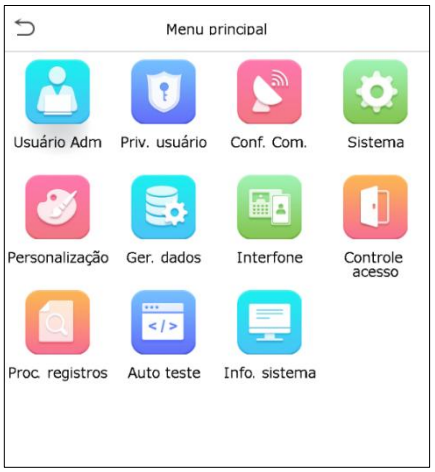
- A autenticação combinada requer que os usuários cadastrem mais de um método de autenticação diferentes. Caso contrário, os usuários podem não conseguir autenticar com sucesso por meio do processo de autenticação combinada.
- Por exemplo, quando um usuário cadastra apenas os dados faciais, mas o modo de verificação do dispositivo está configurado como "Face + Senha", o usuário não conseguirá concluir com sucesso o processo de autenticação.
- Isso ocorre porque o dispositivo compara o modelo facial escaneado da pessoa com o modelo de verificação cadastrado (tanto o face quanto a senha) armazenado anteriormente naquele ID do usuário no dispositivo. No entanto, como o usuário cadastrou apenas a face e não a senha, a verificação não será concluída e o dispositivo exibirá "Verificação falhou".

Observação:

- "/" significa "ou" e "+" significa "e"
- Você deve cadastrar as informações de autenticação necessárias antes de usar o modo de autenticação combinada, caso contrário, a autenticação poderá falhar.

3 Menu Principal

Selecione na tela de principal para entrar no menu, a seguinte tela será exibida:



Menu	Descrição
Usuário Adm.	Para adicionar, editar, visualizar e excluir informações básicas de um usuário
Priv. Usuário	Para definir as permissões de função personalizada e de cadastrador para os usuários, ou seja, os direitos para utilizar o menu sistema.
Conf. Com.	Para definir os parâmetros de rede, comunicação serial, conexão de PC, rede sem fio, servidor de nuvem, Wiegand e diagnóstico de rede.
Sistema	Para definir os parâmetros relacionados ao sistema, incluindo Data e Hora, Configuração de logs de acesso, Parâmetros de face, digital, senha e cartão, redefinir padrões de fábrica, Configuração de tipo de dispositivo e Configuração de detecção.
Personalização	Isso inclui configurações de Interface do Usuário, Voz, Alarme, Presença e Atalhos.
Ger. Dados	Para excluir todos os dados de acesso no dispositivo.
Interfone	Para definir os parâmetros de configurações SIP e ONVIF.

Controle Acesso	Para definir os parâmetros de controle de acesso, incluindo opções como Regra de tempo, Configurações de feriado, acesso combinado, Configuração de antipassback e Configurações das opções de coação.
Proc. Registros	Para consultar os logs de eventos, ver as fotos de presença e as fotos de presença da lista de bloqueios.
Autoteste	Para testar automaticamente se cada módulo funciona corretamente, incluindo a tela LCD, áudio, microfone, sensor de digital, câmera e o relógio em tempo real.
Informação de sistema	Para visualizar as informações de capacidade de dados do dispositivo e firmware.

Nota: Quando os usuários usam o produto pela primeira vez, eles devem operá-lo após definir os privilégios de administrador. Toque em Usuário Adm. para adicionar um administrador ou editar permissões de usuário como super administrador.

Se o produto não tiver uma configuração de administrador, o sistema mostrará uma janela de configuração de administrador toda vez que você entrar no menu do dispositivo.

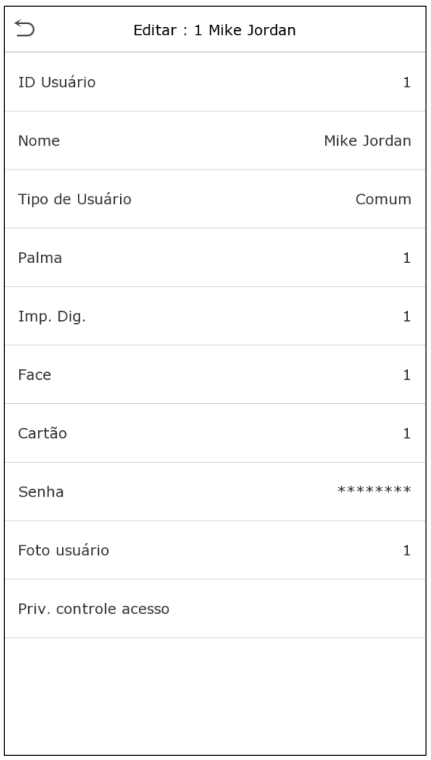
4 Gestão de Usuários

4.1 Cadastro de Usuários

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

4.1.1 ID de usuário e nome

Toque em **Novo Usuário** Insira o ID do usuário e o nome.



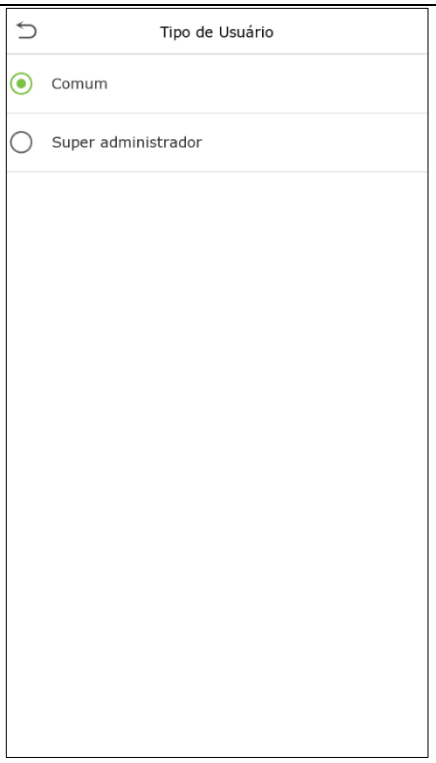
Observação:

- Um nome pode ter até 17 caracteres.
- O ID do usuário pode conter de 1 a 9 dígitos por padrão.
- Durante o cadastro inicial, você pode modificar seu ID, que não pode ser modificado após salvar.
- Se a mensagem "Duplicado!" aparecer, você deve escolher outro ID, pois o ID de usuário inserido já existe.

4.1.2 Privilégio do usuário (Tipo de usuário)

Existem dois tipos de contas de usuário: **usuário comum** e **super administrador**. Caso já exista um administrador cadastrado, os usuários normais não possuem direitos de gerenciamento do sistema, podendo apenas fazer autenticação. O administrador possui todos os privilégios de gerenciamento. Se uma função personalizada for definida, você também poderá selecionar permissões de **função definida pelo usuário** para o usuário.

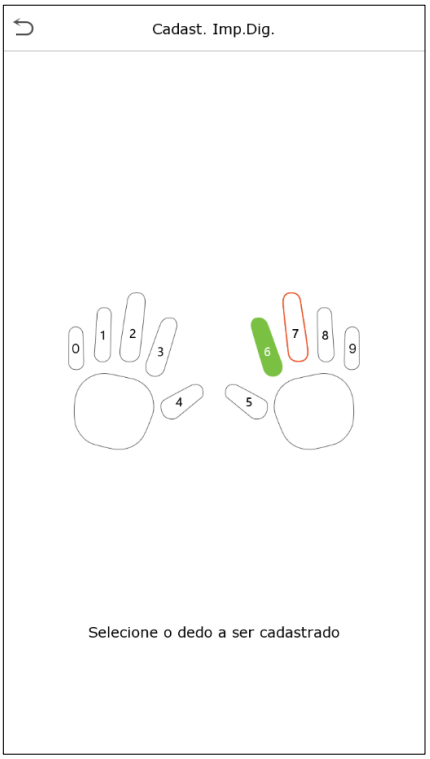
Clique em **Tipo de Usuário** para definir a função do usuário como Usuário Comum ou Super Admin.



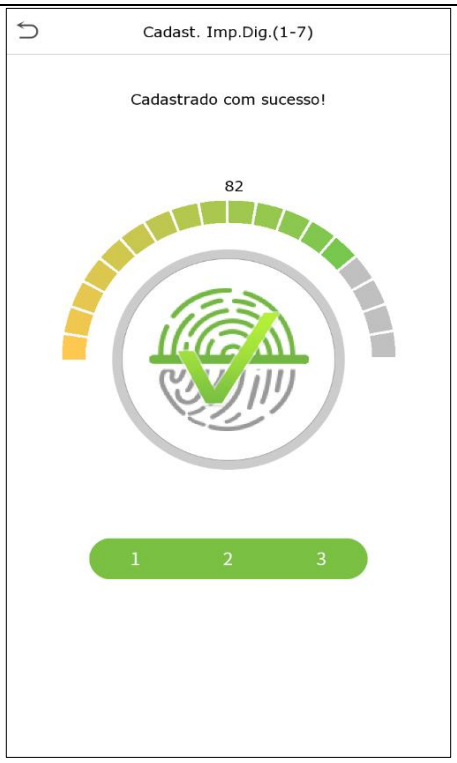
Observação: Se a função de usuário selecionada for o Super administrador, o usuário deverá fazer a autenticação para acessar o menu principal. A autenticação é baseada no(s) método(s) de autenticação que o super administrador cadastrou. Por favor, consulte "Modos de Autenticação".

4.1.3 Cadastro de Impressão Digital

Clique em **Impressão Digital** para acessar a página de cadastro de impressões digitais. Selecione o dedo a ser cadastrado



Pressione o mesmo dedo no leitor de impressões digitais três vezes. A cor verde indica que a impressão digital foi cadastrada com sucesso.



4.1.4 Cadastro de Face

Clique em "**Face**" para acessar a página de cadastro de face. Posicione-se em frente à câmera e mantenha-se imóvel durante o cadastro facial. A tela de cadastro é a seguinte:

4.1.5 Cadastro do Número do Cartão

- **Cadastro de Cartão**

Toque em **Cartão** na tela do **Novo Usuário** para entrar na página de cadastro de cartão.

- Passe o cartão na área de leitura. O cadastro de número de cartão vai ser coletado.
- Se o cartão já estiver cadastrado, a mensagem "Cartão Duplicado" aparecerá.
- A tela de cadastro é a seguinte:

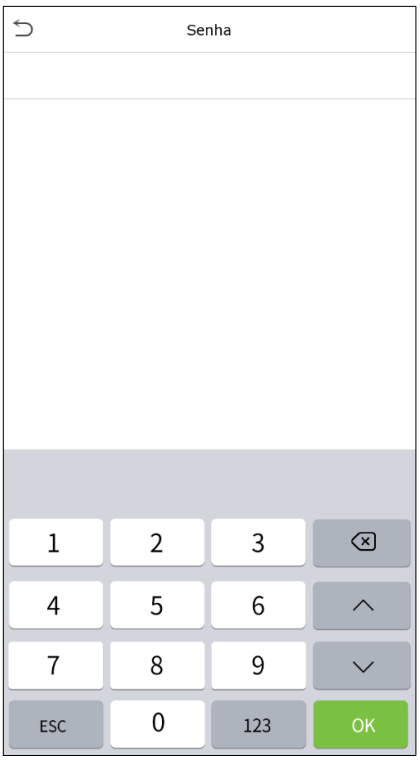
- **Cadastro de QR Code Estático (Campo de Cartão)**

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

- Na interface do Cartão, mostre clique no ícone de QR Code e aponte para a câmera. O cadastro do QR Code será bem-sucedido.
- Se o QR Code já estiver cadastrado, a mensagem "**Erro! Cartão já cadastrado**" será exibida. A tela de cadastro é a seguinte:

4.1.6 Cadastro de Senha

Toque em **Senha** para acessar a página de cadastro de senha. Digite uma senha e digite-a novamente. Toque em **OK**. Se as duas senhas digitadas forem diferentes, o aviso "**Senha não coincide!**" será exibido



Observação: A senha pode conter de um a oito dígitos por padrão.

4.1.7 Cadastro da Foto do Usuário

Quando um usuário cadastrado com uma foto faz a autenticação, a foto do cadastro poderá ser exibida. Clique em **Foto do Usuário**, clique no ícone da câmera para tirar uma foto. O sistema retornará à tela de **Novo Usuário** após tirar a foto.

Observação: Ao cadastrar uma face, o sistema capturará automaticamente uma imagem como foto do usuário. Se você não deseja cadastrar uma foto do usuário, o sistema definirá automaticamente a imagem capturada como foto padrão

4.1.8 Privilégios de controle de Acesso

O controle de acesso do usuário define os direitos de desbloqueio da porta de cada pessoa, incluindo o grupo e o horário ao qual o usuário pertence.

Clique em **Priv. controle de Acesso > Grupo de Acesso**, atribua 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

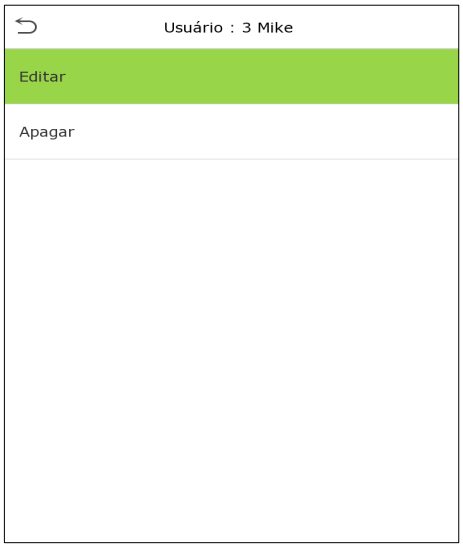
Clique em Horário, selecione o período de tempo a ser utilizado.

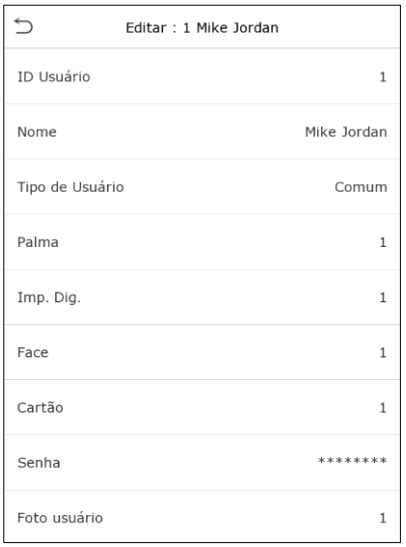
4.2 Busca de Usuários

No Menu Principal, toque em **Gerenciamento de Usuários** e, em seguida, toque em **Todos os Usuários** para pesquisar um usuário. Na tela **Todos os Usuários**, toque na barra de pesquisa na lista de usuários para inserir a palavra-chave de busca necessária (onde a palavra-chave dever ser o ID do usuário) e o sistema buscará as informações relacionadas ao usuário.

4.3 Editar Usuário

Na tela **Todos os Usuários**, toque no usuário desejado na lista e em seguida 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. Para o processo detalhado, veja "**Cadastro de Usuário".**

4.4 Excluir Usuário

Na tela **Todos os Usuários**, toque no usuário desejado na lista e em seguida toque em **Excluir** para remover o usuário ou informações específicas do usuário no dispositivo. Na tela de exclusão, toque na operação necessária e depois toque em **OK** para confirmar a exclusão

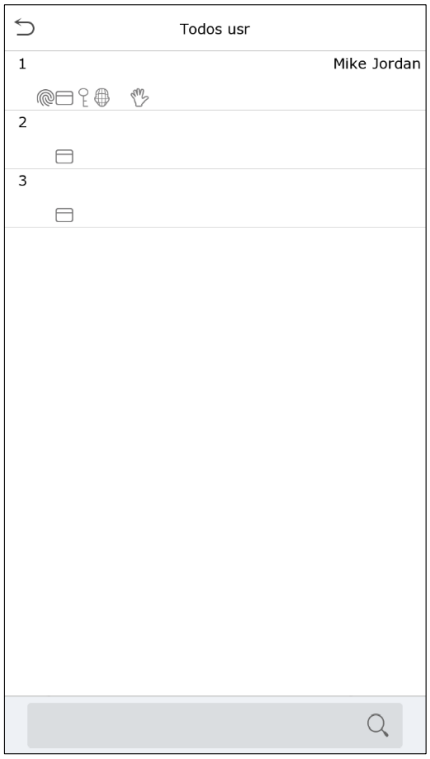
Operações de Exclusão:

- **Apg. Usuário:** Exclui todas as informações do usuário (exclui o usuário selecionado como um todo) do dispositivo**.**
- **Apg. Imp. Dig.:** Exclui apenas as informações de impressão digital do usuário selecionado.
- **Excluir apenas a face:** Exclui apenas a face do usuário selecionado.
- **Apg. Senha:** Exclui apenas a senha do usuário selecionado.
- **Apg. Apenas No. De chip:** Exclui apenas o número de cartão do usuário selecionado.
- **Apg. Foto:** Exclui apenas a foto do usuário selecionado (Apenas foto, não o cadastro de face).
- **Remover apenas a palma de mão:** Exclui apenas a palma de mão do usuário selecionado.

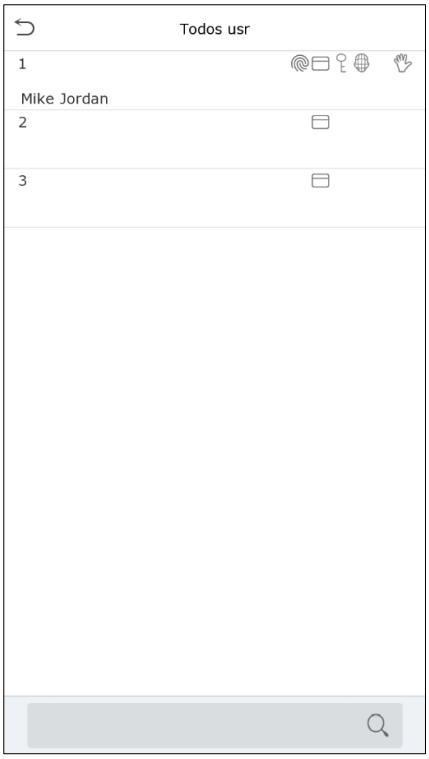
4.5 Estilo do Display

No menu principal, clique em **Usuário Adm**. e, em seguida, clique em **Estilo de exibição** para entrar na interface de configuração do **Estilo de exibição.**

Todos os estilos de exibição são mostrados como abaixo:



Múltiplas Linhas



Linhas Mistas

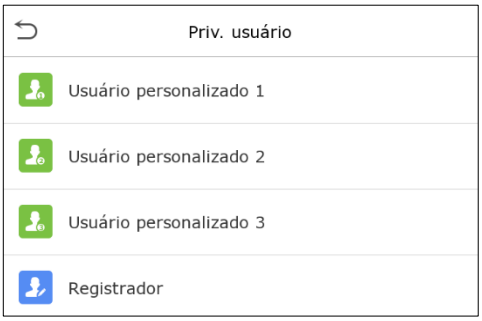
5 Privilégio do Usuário

Se você precisar atribuir permissões específicas a determinados usuários, poderá editar o **Privilégio do Usuário** no menu de **Tipo de Usuário**.

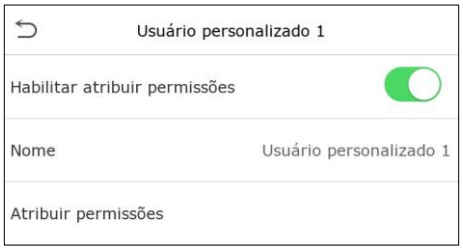
Observação: Antes de ativar estes perfis, é necessário cadastrar um usuário super administrador

Você pode editar as permissões de forma personalizadas para os perfis já existentes, porém não é possível criar perfis!

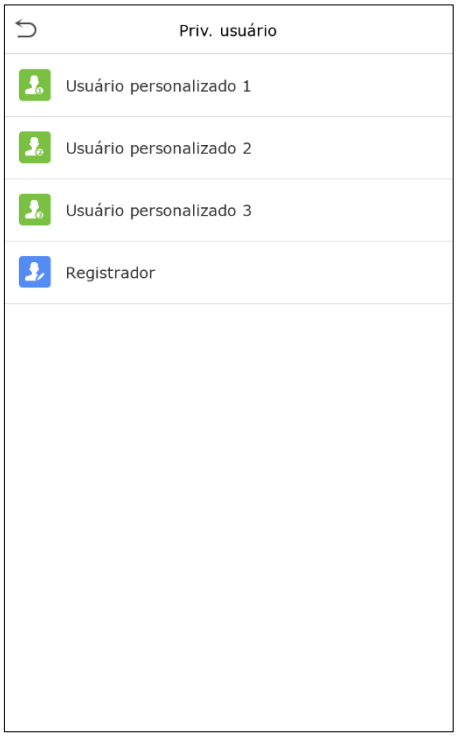
Clique em **Priv. Usuário** na interface do menu principal.



1. Clique em qualquer Usuário Personalizado, em seguida, selecione o botão **Habilitar Atribuir Permissões**, para ativar ou desativar a função do grupo selecionado.



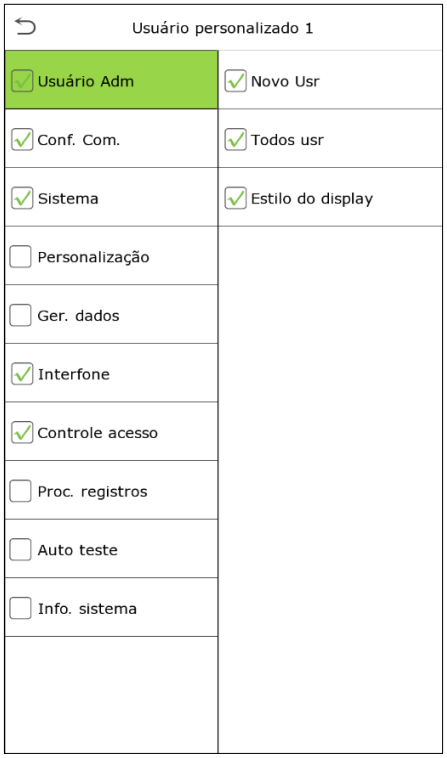
Toque em **Nome** para inserir o nome personalizado da função.

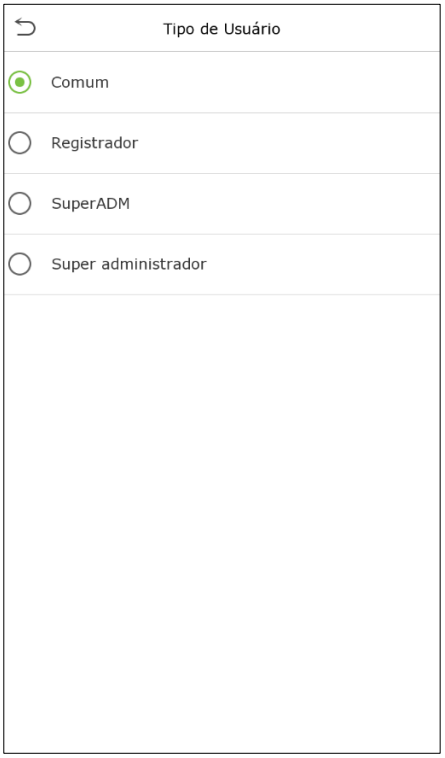


Em seguida, toque em **Atribuir permissões** e selecione os privilégios necessários para atribuir ao novo perfil e, em seguida, toque no botão **Retornar**.

Durante a atribuição de permissões, os nomes das funções do **Menu Principal** serão exibidos à esquerda e seus submenus serão listados à direita.

Primeiro, toque nas funções desejadas do **Menu Principal** e, em seguida, selecione os submenus necessários da lista aos quais o usuário pode ter acesso.





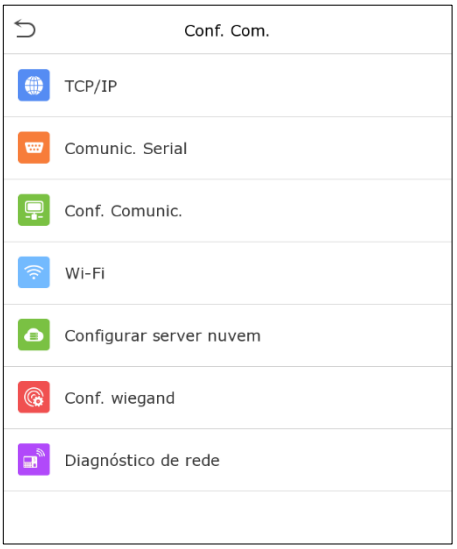
Observação: Se o **Tipo do Usuário** estiver habilitado no dispositivo, toque em **Usuários** > **Novo Usuário** > **Tipo de Usuário** para atribuir os perfis editados aos usuários escolhidos. No entanto, se não houver um super administrador

cadastrado no dispositivo, o dispositivo exibirá a mensagem **"Cadastre super administrador primeiro"** ao tentar habilitar a função de atribuir permissões

6 Configurações de Comunicação

As configurações de comunicação são utilizadas para definir os parâmetros de rede, comunicação serial, conexão de PC, rede sem fio, servidor de nuvem, Wiegand e diagnóstico de rede.

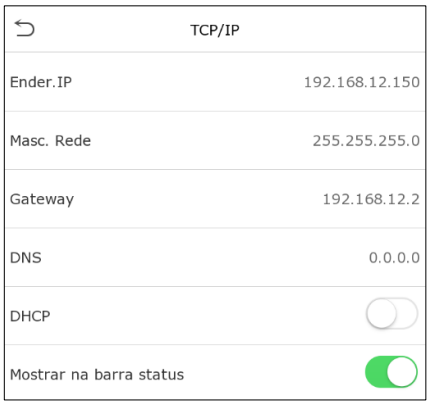
Toque em **Conf. Com.** no Menu Principal



6.1 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.



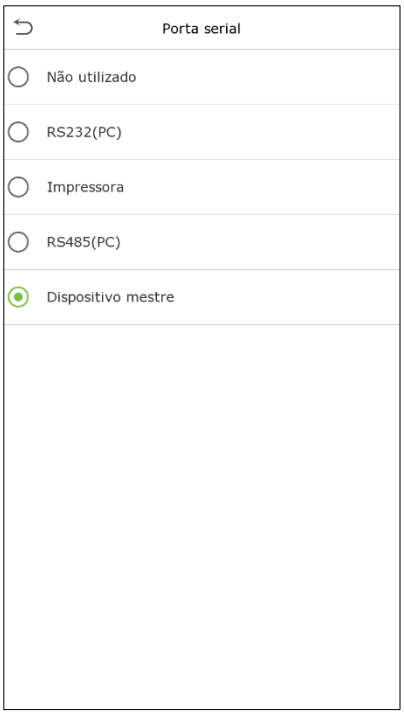
Função	Descrição
Ender. IP	O valor de fábrica é 192.168.1.201 e pode ser editado.
Másc. Rede	O valor de fábrica é 255.255.255.0 e pode ser editado.
Gateway	O valor de fábrica é 0.0.0.0 e pode ser editado.
DNS	O valor de fábrica é 0.0.0.0 e pode ser editado.
DHCP	Ao habilitar esta função, o roteador será responsável por configurar todos os parâmetros de rede automaticamente.

Mostrar na barra status	Para definir se o ícone de rede será exibido na barra de status da tela inicial.

6.2 Comunicação Serial

A função **Comunic. Serial** define outras opções de comunicação com um dispositivo através de uma porta serial (RS232 ou RS485).

Toque em **Comunic. Serial** na tela de **Configurações de Comunicação.**

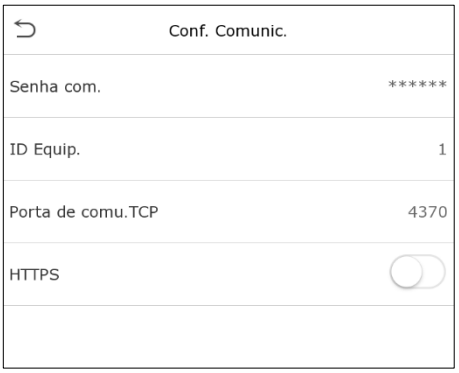


Função	Descrição
Porta Serial	**Não Utilizado**: Não se comunica com o dispositivo através da porta serial. **RS232(PC):** Comunica-se com o PC através da porta serial RS232. **Impressora:** Envia comando para impressora imprimir o ticket com dados da autenticação do usuário. (Ex.: Utilizando impressora térmica). **RS485(PC):** Comunica-se com o PC através da porta serial RS485. **Dispositivo Mestre:** Ao selecionado, permite a comunicação com os leitores auxiliares FR1200 ou FR1500.
Taxa de Transmissão	A taxa na qual os dados são trafegados com dispositivos, possui 4 opções de taxa de transmissão: 115200 (padrão), 57600, 38400 e 19200. Quanto maior a taxa de transmissão, mais rápida é a velocidade de comunicação, mas também menos confiável. Portanto, uma taxa de transmissão mais alta pode ser usada quando a distância de comunicação é curta; quando a distância de comunicação é longa, escolher uma taxa de transmissão mais baixa é recomendável.

6.3 Configuração de Comunicação

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.



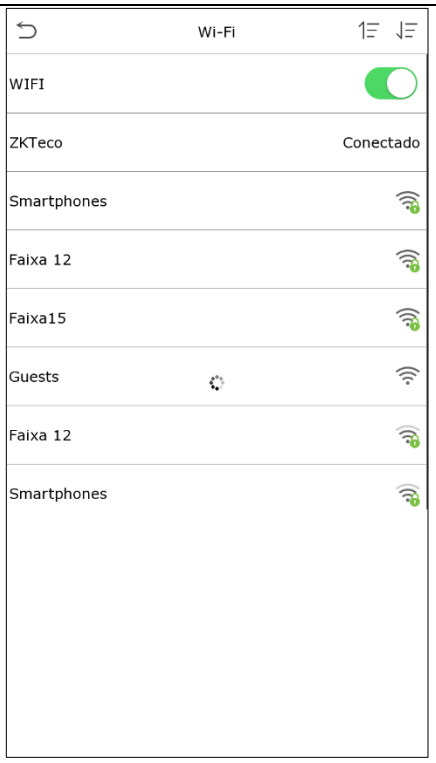
Função	Descrição
Senha Com.	A senha padrão é 0, que pode ser alterada, pode conter de 1 a 6 dígitos.
ID do aparelho	Número de identificação do dispositivo na rede serial, que varia entre 1 e 254, necessário se comunicação for RS232/RS485.
Porta de comu. TCP	O valor predefinido na fábrica é 4370 e pode ser editado
HTTPS	Para aumentar a segurança do acesso do navegador, os usuários podem ativar o protocolo HTTPS para criar uma transmissão de rede segura e criptografada. Necessário o software ser instalado em HTTPS caso isso seja selecionado no dispositivo.

6.4 Rede sem fio (Wi-Fi)

O dispositivo possui um módulo Wi-Fi embutido no dispositivo..

O módulo Wi-Fi permite a transmissão de dados por meio de Wi-Fi (Wireless Fidelity) e estabelece conexão em rede sem fio. O Wi-Fi está ativado por padrão no dispositivo. Se você não precisa usar a rede Wi-Fi, pode desativá-la usando o botão de desativar o Wi-Fi.

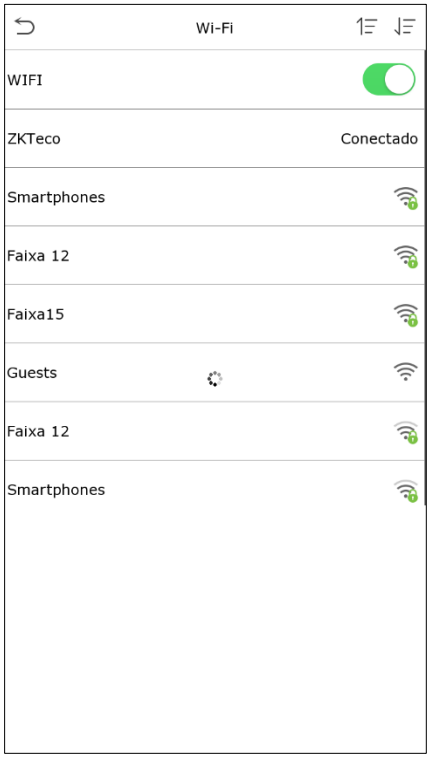
Toque em **Wi-Fi** na interface de **Configurações de Comunicação** para configurar a conexão Wi-Fi.

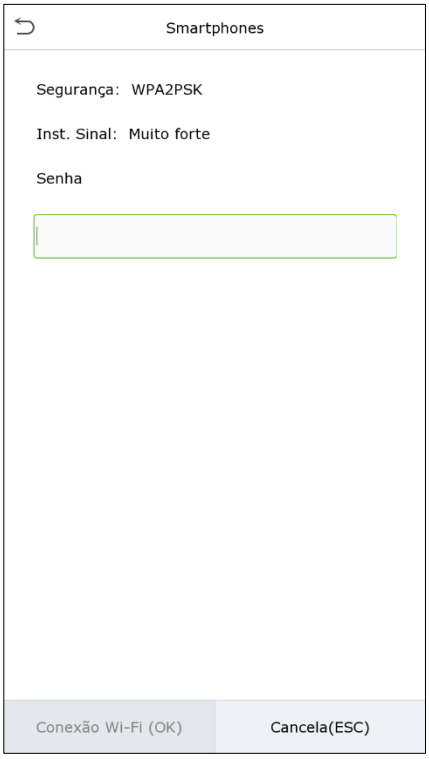


O Wi-Fi está ativado no dispositivo por padrão. Toque para ativar ou desativar o Wi-Fi.

Uma vez que o Wi-Fi esteja ativado, o dispositivo buscará pelas redes Wi-Fi disponíveis dentro do alcance da rede.

Toque na rede Wi-Fi desejada na lista disponível e insira a senha na tela, em seguida, toque em **Conectar ao Wi-Fi (OK).**



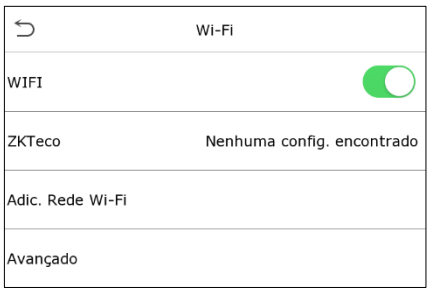


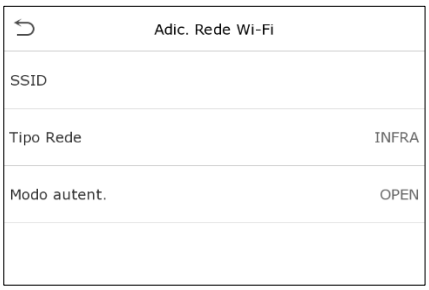
- **Wi-Fi Habilitado**: Toque na rede desejada na lista de redes pesquisadas
- Toque no campo de senha para inserir a senha e, em seguida, toque em **Conectar ao Wi-Fi (OK).**

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

Adicionar Rede Wi-Fi Manualmente:

O Wi-Fi também pode ser adicionado manualmente se a rede Wi-Fi desejada não estiver sendo exibida na lista.



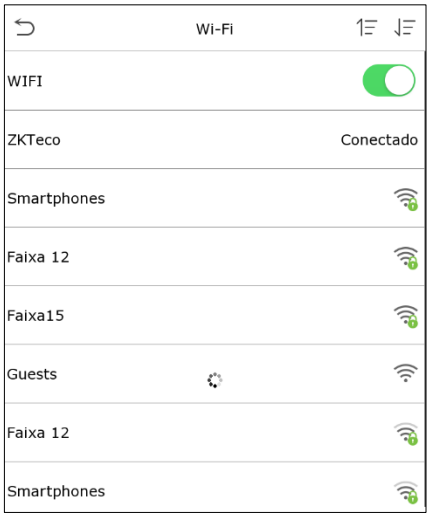


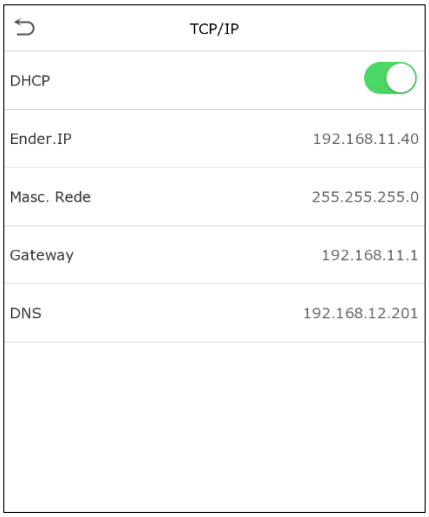
- Clique em Adic. Rede Wi-Fi.
- Na próxima tela, insira os parâmetros da rede Wi-Fi. (A rede adicionada deve existir.)

Observação: Após adicionar com sucesso o Wi-Fi manualmente, siga o mesmo processo para pesquisar o nome do Wi-Fi adicionado.

Configuração Avançada

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



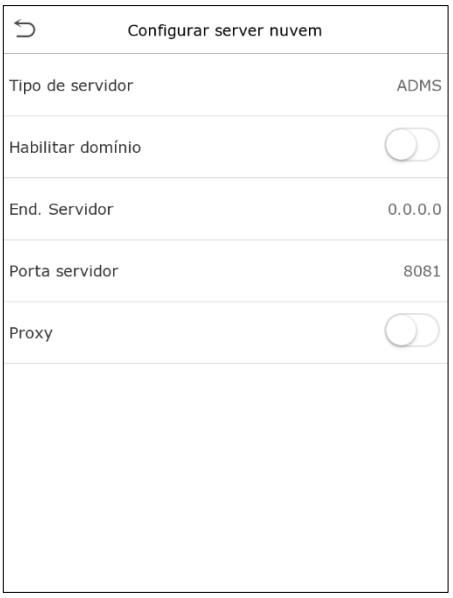


Função	Descrição
DHCP	O protocolo de configuração dinâmica de host (DHCP) aloca dinamicamente endereços IP para clientes de rede. Se o DHCP estiver ativado, o IP não poderá ser definido manualmente.
End. IP	Endereço IP para a rede WIFI, o padrão é 192.168.1.201 (0.0.0.0 caso o DHCP esteja ativado). Pode ser modificado de acordo com a disponibilidade da rede.
Máscara de sub-rede	A máscara de sub-rede padrão da rede WIFI é 255.255.255.0. Pode ser modificado de acordo com a disponibilidade da rede.
Gateway	O endereço de Gateway padrão é 0.0.0.0. Pode ser modificado de acordo com a disponibilidade da rede.
DNS	O valor de fábrica é 0.0.0.0 e pode ser editado.

6.5 Configuração do Servidor em Nuvem

Isso representa as configurações usadas para conectar ao servidor ADMS, necessário para a comunicação do dispositivo com software.

Clique **Configurar servidor nuvem** na tela de **Configurações de Comunicação.**



Função		Descrição
Habilitar 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)
Domínio desabilitado	**Endereço do servidor**	O endereço IP do servidor ADMS.
	Porta do servidor	Porta usada pelo servidor ADMS.
Proxy		Ao optar por habilitar o proxy, você precisa definir o endereço IP e o número da porta do servidor proxy

6.6 Configuração de Wiegand

Este menu é usado para definir os parâmetros de entrada e saída Wiegand.

Toque em Configuração Wiegand na Interface de **Configurações de Comunicação**

6.6.1 Entrada Wiegand

Função	Descrição
Formato Wiegand	Os valores variam de 26 bits, 32 bist, 34 bits, 36 bits, 37 bits e 50 bits e 64 bits
Wiegand bits	Após ativar os formatos Wiegand necessários, selecione a opção de bit de entrada.
Largura do pulso (us)	O valor da largura de pulso enviado pelo Wiegand é de 100 microssegundos por padrão, que pode ser ajustado dentro do intervalo de 120 a 400 microssegundos
Intervalo de pulso (us)	O valor padrão é 1.000 microssegundos, que pode ser ajustado dentro do intervalo de 200 a 20.000 microssegundos.
Tipo de ID	Selecione o que será recebido pela entrada Wiegand, ID do usuário ou o número do cartão.

Descrição dos formatos mais comuns de Wiegand:

Formato Wiegand	Descrição
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCO Consiste em 26 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 13º bits, enquanto o 26º bit é o bit de paridade ímpar do 14º ao 25º bits. O 2º ao 25º bits são os números do cartão
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCO Consiste em 26 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 13º bits, enquanto o 26º bit é o bit de paridade ímpar do 14º ao 25º bits. Os 2º a 9º bits são os site code, enquanto os 10º a 25º bits são os números do cartão.
Wiegand34	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	OFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME 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	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE 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.

6.6.2 Saída Wiegand

Função	Descrição
SRB	Quando o SRB está habilitado, a fechadura é acionada pelo SRB para evitar que a fechadura seja aberta com a remoção do dispositivo da parede
Formato Wiegand	Os valores variam de 26 bits, 32bits, 34 bits, 36 bits, 37 bits, 50 bits e 64bits.
Bits de saída Wiegand	Após ativar os formatos Wiegand necessários, selecione a opção de bit de saída.
Falha ID	Se a verificação falhar, o sistema enviará o ID com falha para o dispositivo ao invés do número do cartão ou ID.

Site Code	O site code pode ser definido manualmente e pode ser repetido em um dispositivo diferente. O valor válido varia de 0 a 256 por padrão.
Largura do pulso (us)	O valor da largura de pulso enviado pelo Wiegand é de 100 microssegundos por padrão, que pode ser ajustado dentro do intervalo de 20 a 400 microssegundos
Intervalo de pulso (us)	O valor padrão é 1.000 microssegundos, que pode ser ajustado dentro do intervalo de 200 a 20.000 microssegundos
Tipo de ID	Selecione o que enviado pela saída Wiegand, ID do usuário ou o número do cartão.

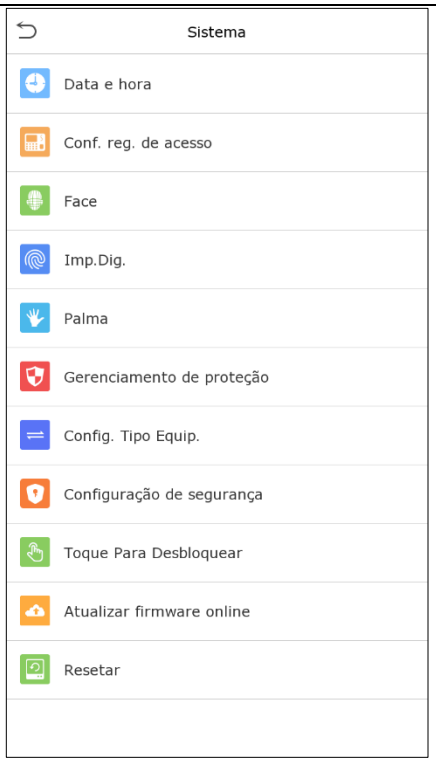
6.7 Diagnóstico de Rede

Clique em **Diagnóstico de Rede** na tela de Configurações de Comunicação. Insira o endereço IP que precisa ser diagnosticado e clique em **Iniciar diagnóstico** para verificar se a rede pode se conectar ao IP inserido.

7 Configurações de Sistema

As configurações do sistema são usadas para definir os parâmetros do sistema, alguns parâmetros são necessários para otimizar o desempenho do dispositivo.

Clique em **Sistema** na interface do menu principal.

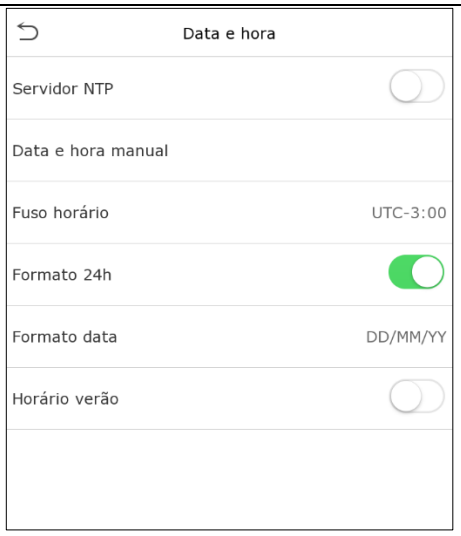


7.1 Data e Hora

Toque em **Data e Hora** na tela de **Sistema** para definir a **Data e a Hora**.

O produto suporta o sistema de sincronização de horário NTP. Essa função entra em vigor depois que a **Servidor NTP** é ativado e o link do endereço do servidor NTP específico é definido.

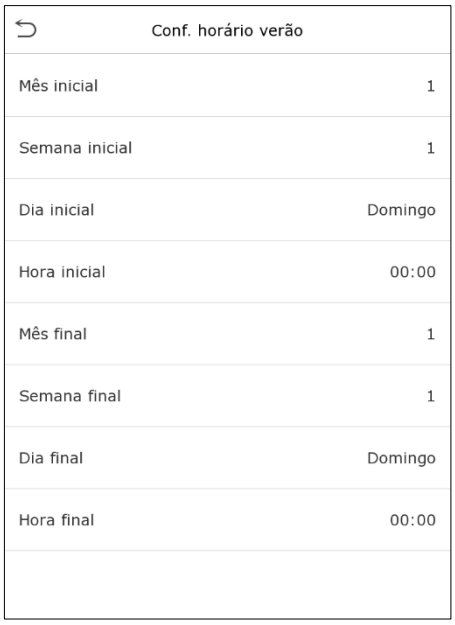
Se os usuários precisarem definir a data e a hora manualmente, primeiro desabilite a **Servidor NTP** e, em seguida, toque em **Data e hora manual** para definir a data/hora e toque em **Confirmar** para salvar.



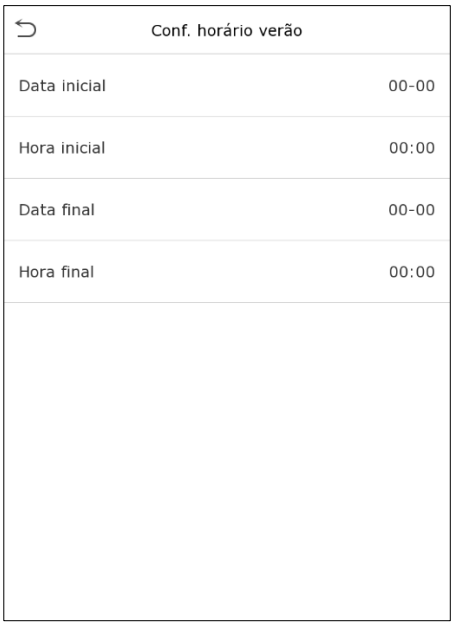
Toque em **Fuso Horário** para escolher um fuso horário e, em seguida, toque no botão de retorno para salvar e sair.

Toque em **Formato 24 Horas** para ativar ou desativar esse formato.

Toque em **Horário de Verão** para ativar ou desativar a função. Se ativado, 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.



Semana/dia



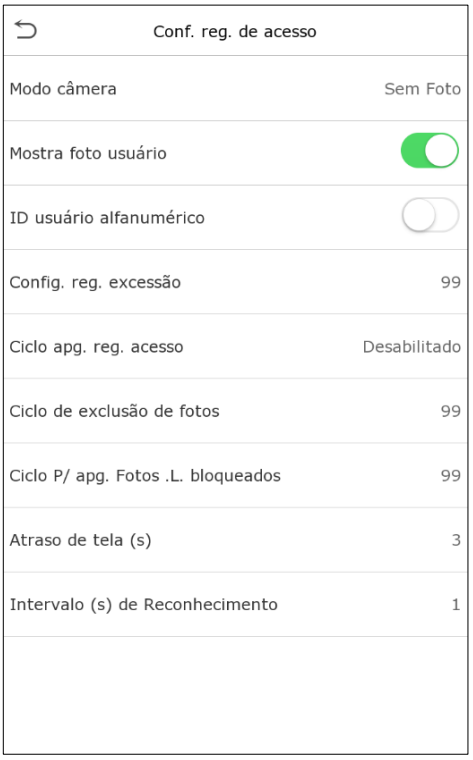
Data/Hora

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 serão restauradas.

Observação: Por exemplo, se um usuário definir a hora do dispositivo para 15:35 em 31 de janeiro de 2024 e, em seguida, alterar para 18:30 em 1º de janeiro de 2025. Após restaurar as configurações de fábrica, a hora do dispositivo permanecerá como 18:30 em 1º de janeiro de 2025.

7.2 Configuração de Registros de Acesso

Clique nas **configurações de registros de acesso** na interface do sistema

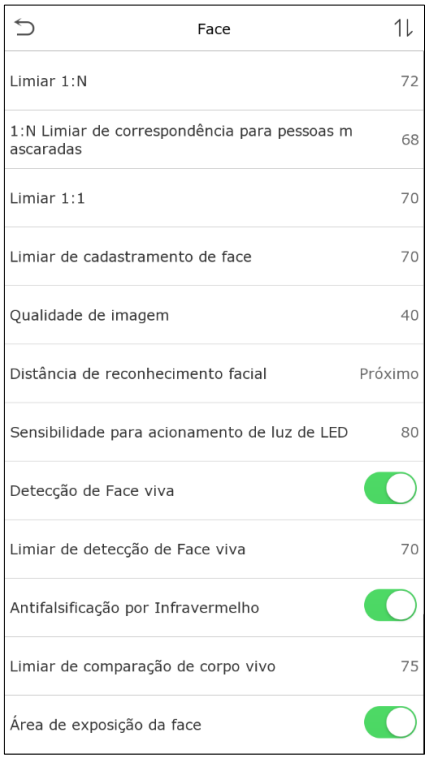


Função	Descrição
Modo de câmera	Esta função está desativada por padrão. Quando ativada, um aviso de segurança será exibido. **Sem Foto:** Nenhuma foto é tirada durante a autenticação do usuário. **Capturar, não salvar:** A foto é tirada, mas não salva durante a autenticação. **Capturar e salvar:** A foto é tirada e salva durante a autenticação. **Salvar após a verificação Ok:** A foto é tirada e salva para cada autenticação bem-sucedida. **Salvar após verificação inválida:** A foto será tirada e salva apenas para a autenticação com falha.
Mostra foto usuário	Esta função está desativada por padrão. Quando ativada, um aviso de segurança será exibido. A foto do usuário será exibida quando o usuário for autenticado com sucesso.
ID usuário alfanumérico	Quando essa opção é ativada, na tela de cadastro de usuário, é possível criar o ID alfanumérico. ***Observação: Ao ativar esta função, na tela de Wiegand, o tipo será apenas de número de cartão, não mais poderá selecionar o ID.***
Config. Reg. Exceção	Quando os registros de erro atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de registros de erros antigos. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 999.
Ciclo apg. Reg. acesso	Quando os registros de acesso atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de registros de acesso antigos. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 999.
Ciclo exclusão de fotos	Quando as fotos de log atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de antigas. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 99

Ciclo p/ apg. Fotos L. bloqueados	Quando as fotos da lista de bloqueados atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de fotos. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 99.
Atraso de tela (s)	Tempo de atraso da exibição da mensagem de verificação bem-sucedida. Valor válido: 1~9 segundos.
Intervalo de comparação de faces (s)	Este parâmetro define o intervalo de comparação entre a mesma face do mesmo usuário, caso ele continue na frente do equipamento após uma autenticação válida. Valor válido: 0 a 9 segundos.

7.3 Parâmetros de Face

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



Função	Descrição
Limiar 1:N	No modo de verificação 1:N, a verificação só será bem-sucedida quando a similaridade entre a imagem facial adquirida e todos os modelos faciais cadastrados for maior que o valor definido. O valor válido varia de 0 a 100. Quanto maior o limiar, menor será a taxa de erro de julgamento e maior será a taxa de rejeição, e vice-versa. É recomendado definir o valor padrão de 72 **neste dispositivo com esta versão de firmware.**
1:N Limiar de correspondência para pessoas mascaradas	Neste parâmetro 1:N, a validação do uso de máscara só será bem-sucedida quando a similaridade entre a imagem da autenticação de face com máscara for comparada com os modelos pré-estabelecidos de máscaras. O valor válido varia de 0 a 100. Quanto maior o limiar, menor será a taxa de erro de julgamento e maior será a taxa de rejeição, e vice-versa. É recomendado definir o valor padrão de 68 **neste dispositivo com esta versão de firmware.**

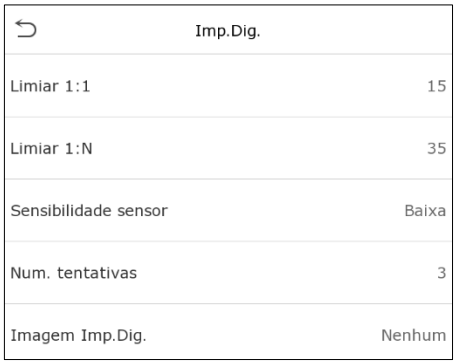
Limiar 1:1	No modo de autenticação 1:1, a autenticação só será bem-sucedida quando a semelhança entre a imagem facial adquirida e os modelos faciais do usuário cadastrados no dispositivo for maior que o valor definido. O valor válido varia de 0 a 100. Quanto maiores os limites, menor a taxa de erro, maior a taxa de rejeição e vice-versa. Recomenda-se definir o valor padrão de 63 **neste dispositivo com esta versão de firmware.**
Limiar de cadastramento de face	Durante o cadastro de face, a comparação 1:N é usada para determinar se o usuário já se cadastrou antes. Quando a semelhança entre a imagem facial adquirida e todos os modelos faciais cadastrados forem maiores que esse limite, indica que a face já foi cadastrada.
Qualidade da imagem	Qualidade de imagem para cadastro e autenticação facial. Quanto maior o valor, mais clara a imagem precisa ser.
Distância de reconhecimento facial	É a distância necessária para que o usuário, ao aproximar do equipamento, seja autenticado caso esteja cadastrado. Os parâmetros podem ser definidos como: Distante: Aproximadamente 2,5 metros -> Valor interno = 80 Mediana: Aproximadamente 1,5 metros -> Valor interno = 105 Próximo: Aproximadamente 0,5 metros -> Valor interno=180
Sensibilidade para acionamento da luz LED	Este valor controla a ativação e desativação da luz LED. Quanto maior o valor, mais frequentemente a luz do LED será ligada. Este parâmetro pode variar de 1 a 200 e por padrão vem como 80.
Detecção de face viva	Detecta a tentativa de falsificação usando imagens de luz visível para determinar se a amostra de fonte biométrica fornecida é realmente uma pessoa (um ser humano vivo) ou uma representação falsa.
Limiar de detecção de face viva	Parâmetro para ajustar a detecção de face viva. Quanto maior o valor, melhor o desempenho anti-falsificação usando luz visível.
Anti-falsificação por infravermelho	Usado para ativar a montagem de imagens infravermelho na autenticação e evitar ataques de fotos e vídeos falsos.
Limiar de comparação de corpo vivo	Quanto maior o valor, melhor o desempenho anti-falsificação usando infravermelho
Área de exposição de face	Quando ativada esta função, melhora a iluminação da face durante reconhecimento facial. Aplicado em cenários em que a luz de fundo sobrepõe e prejudica o reconhecimento facial.
WDR	Ampla Faixa Dinâmica (WDR), que equilibra a luz e amplia a visibilidade da imagem para vídeos de vigilância em cenas de iluminação de alto contraste e melhora a identificação de objetos em ambientes claros e escuros.
Modo anti-pisca	Usado quando o WDR está desligado. Isso ajuda a reduzir a cintilação quando a tela do dispositivo pisca na mesma frequência que a luz.
Algoritmo face	Informações relacionadas ao algoritmo facial e possibilita pausar a atualização do modelo facial.

Observação: O ajuste inadequado dos parâmetros de exposição e qualidade pode afetar gravemente o desempenho do dispositivo. Ajuste o parâmetro de exposição somente sob a orientação do pessoal de suporte pós-venda de nossa empresa

- Para modificar a precisão do reconhecimento facial, na interface do sistema, vá em **Face** e ative a Anti-falsificação por infravermelho para configurar a anti-falsificação.
- Em seguida, no **Menu Principal**, selecione **Autoteste > Teste câmera** e realize o teste facial.
- Toque três vezes nos scores no canto superior direito da tela e uma caixa retangular vermelha aparecerá para iniciar o ajuste do modo.
- Mantenha uma distância de um braço entre o dispositivo e a face. É recomendado não mover a face em uma ampla faixa.

7.4 Parâmetros de impressão digital

Clique em **Impressão Digital** na interface do sistema



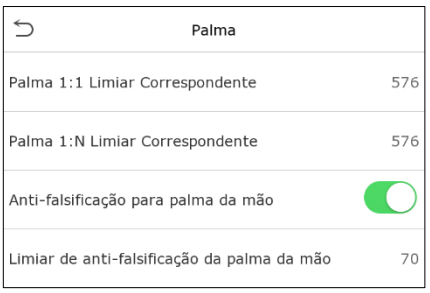
FRR	FAR	Limiares de comparação recomendados	
		1:N	1:1
Alto	Baixo	45	25
Médio	Médio	35	15
Baixo	Alto	25	10

Função	Descrição
Limiar 1:1	No método de autenticação 1:1, a autenticação só será bem-sucedida quando a similaridade entre os dados de impressão digital adquiridos e o modelo de impressão digital associado ao ID de usuário inserido no dispositivo for maior que o valor definido.
Limiar 1:N	No método de autenticação 1:N, a autenticação será bem-sucedida apenas quando a similaridade entre os dados de impressão digital adquiridos e os modelos de impressão digital cadastrados no dispositivo for maior que o valor definido.
Sensibilidade do sensor de impressão digital	Para definir a sensibilidade da coleta de impressões digitais. Recomenda-se usar o nível padrão "Médio". Quando o ambiente está seco, resultando em detecção lenta de impressões digitais, você pode definir o nível como "Alto" para aumentar a sensibilidade; quando o ambiente estiver úmido, dificultando a identificação da impressão digital, pode-se definir o nível para "Baixo".
Núm. tentativas	Na verificação 1:1, os usuários podem esquecer a impressão digital registrada ou pressionar o dedo de forma incorreta. Você pode configurar o número de tentativas erradas.

Imagem de Impressão Digital	Esta função está desativada por padrão. Após desativá-la, a imagem da impressão digital não será exibida ao cadastrar e autenticar por impressão digital. Ao ativar ou desativar essa função, uma tela de aviso será exibida. Quatro opções estão disponíveis: **Mostrar cadast.:** para exibir a imagem da impressão digital apenas durante o cadastro. **Mostrar valor:** para exibir o valor em score da qualidade da impressão digital. **Sempre mostrar:** para exibir a imagem da impressão digital na tela durante a inscrição e verificação. **Nenhum:** não exibir a imagem da impressão digital e em score

7.5 Parâmetros de Palma

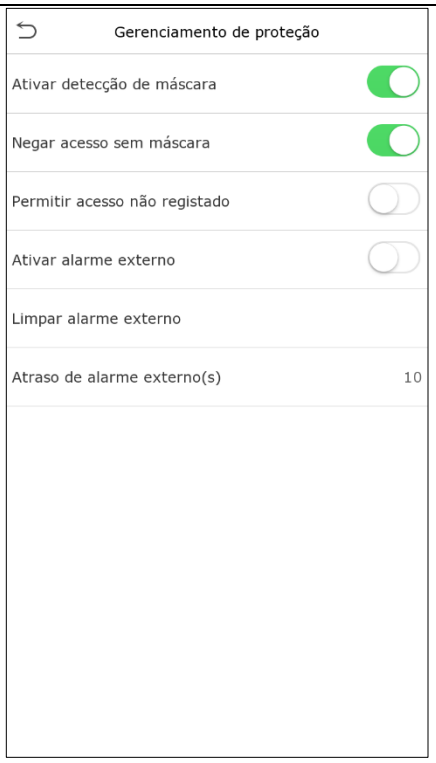
Clique em **Palma** na interface do sistema



Função	Descrição
Palma 1:1 Limiar Correspondente	No método de verificação 1:1, a verificação só será bem-sucedida quando a similaridade entre os dados de palma adquiridos e o modelo de palma associado ao ID de usuário inserido no dispositivo for maior que o valor definido.
Palma 1:N Limiar Correspondente	No método de verificação 1:N, a verificação será bem-sucedida apenas quando a similaridade entre os dados de palma adquiridos e os modelos de palma cadastrados no dispositivo for maior que o valor definido.
Anti-falsificação para palma da mão	Este parâmetro ativa ou desativa a anti-falsificação para a palma da mão, sempre recomendamos deixar este parâmetro ativado.
Limiar de anti-falsificação da palma da mão	Parâmetro para ajustar o limiar de detecção de face viva para palma da mão. Quanto maior o valor, melhor o desempenho anti-falsificação para palma da mão.

7.6 Gerenciamento de Proteção

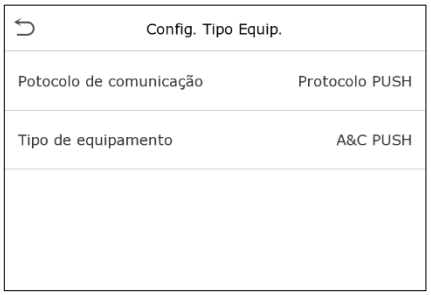
Clique em **Gerenciamento de Proteção** na interface do sistema



Função	Descrição
Ativar Detecção de Máscara	Habilita ou desabilita a função de detecção de máscara. Quando está habilitada, o dispositivo identificará se o usuário está usando uma máscara ou não durante a autenticação.
Negar acesso sem máscara	Habilita ou desabilita a função de negar acesso sem máscara. Quando está habilitada, mesmo que a temperatura corporal esteja normal, a pessoa que não estiver usando uma máscara não será autorizada a entrar.
Permitir acesso a pessoas não registradas	Habilitar ou desabilita a função de permitir acesso a pessoas não cadastradas. Quando habilitada, desde que a pessoa passe pela detecção de máscara, o dispositivo permite que a pessoa entre sem cadastro.
Ativar alarme externo	Quando habilitado e a detecção da máscara estiver habilitada, mas a máscara não for usada pela pessoa, um alarme será acionado.
Limpar Alarme Externo	Limpa os registros de alarmes acionados do dispositivo.
Atraso do Alarme Externo(s)	O tempo de atraso (em segundos) para acionar um alarme externo. Ele pode ser configurado em segundos. Os usuários podem desabilitar a função ou definir um valor entre 1 e 255

7.7 Configuração do tipo de equipamento

Clique em **Configurações do tipo de equipamento** na interface do sistema



Função	Descrição
Protocolo de comunicação	É o protocolo usado para comunicar os dados do terminal facial com o software, pode ser selecionado Protocolo PUSH para comunicar com o ZKBioCVAcces, ZKBioCVSecurity ou ZKBioTime. Para cenários onde existe a necessidade de outras soluções de software da ZKTeco, como o ZLINK ou ZKBioPonto, o protocolo que deve ser selecionado é o BEST.
Tipo de equipamento	**T&A PUSH:** O protocolo de comunicação estará direcionado para controle de presença, que pode ser usado com o ZKBioTime. **A&C PUSH:** O protocolo de comunicação estará direcionado para controle de acesso, que pode ser usado com o ZKBioCVAcces ou ZKBioCVSecurity.

7.8 Configurações de segurança

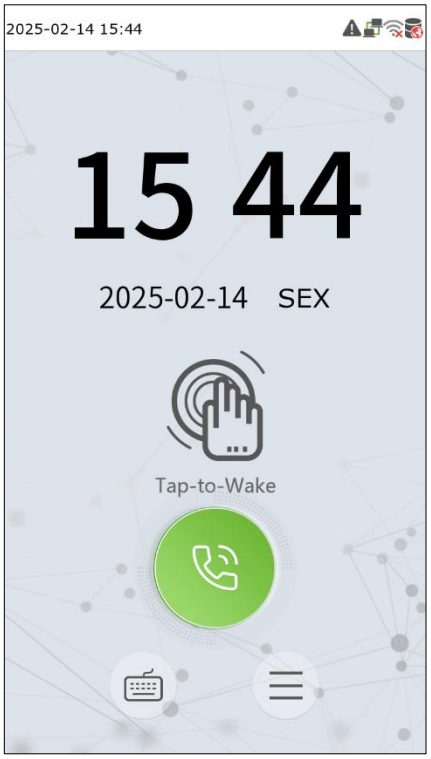
Toque em **Configurações de Segurança** na interface do **sistema**.

Função	Descrição
Comunicação StandAlone	Por padrão, esta função está desativada. Esta função pode ser ativada ou desativada através da interface do menu. Quando é ligada, uma tela de aviso aparece e o dispositivo será reiniciado após a confirmação. Na versão 4.1.14 é necessário criar uma senha para a comunicação StandAlone,

	que deve ser inserida no software de configuração de parâmetros que nossa equipe de suporte técnico utiliza durante um atendimento técnico.
SSH	O dispositivo não oferece suporte ao recurso Telnet, portanto, o SSH é normalmente usado para conexão remota. Por padrão, o SSH está habilitado. A tela do menu permite ativar e desativar o SSH. Quando ativado, haverá uma tela de aviso de segurança, mas o dispositivo não precisará ser reiniciado após a confirmação.
Mascarar ID de Usuário	Depois de habilitado, o ID do usuário será exibido parcialmente após a autenticação válida.
Exibir nome na verificação	Quando habilitada, o nome do usuário será exibido após o resultado da autenticação pessoal. O resultado da verificação não mostrará o nome após a desativação desta opção.
Exibir modo de verificação	Quando habilitada, após a verificação válida, na tela inicial será mostrado o modo de autenticação do usuário.
Salvar foto como Template	Esta função é habilitada por padrão, e na tela do menu é possível desativar. Quando esta função estiver desativada, indicará que há um lembrete de risco: "**É necessário recadastrar a face após uma atualização do algoritmo.**"

7.9 Toque para desbloquear

Quando este parâmetro está ativado a tela inicial do equipamento muda de comportamento, a câmera para realizar o reconhecimento facial não será aberta automaticamente, o usuário terá que clicar na tela para desbloquear a câmera e somente depois realizar a autenticação. A tela inicial também é modificada com um ícone e o texto **Tap-to-Wake,** indicando que o usuário precisa clicar na tela para desbloquear.



Na tela abaixo é possível ajustar dois parâmetros:

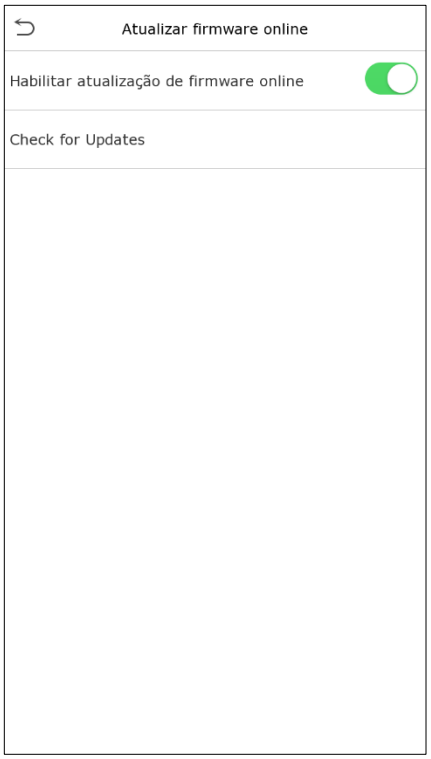
Função	Descrição
Ativar o Toque Para Desbloquear	Neste item você pode ativar ou desativar a função de **Toque Para Desbloquear**.
Período de tempo não habilitado.	Com a função ativada, neste item você pode selecionar faixas horárias para que a função **Toque Para desbloquear** se mantenha ativa.

Observação: Para cada dia da semana é disponibilizado três períodos de tempo, onde é possível configurar o horário de início e horário de fim.

7.10 Atualizar firmware online

Neste menu é possível fazer a atualização de firmware online do repositório da ZKTeco **(Necessário ter internet).**

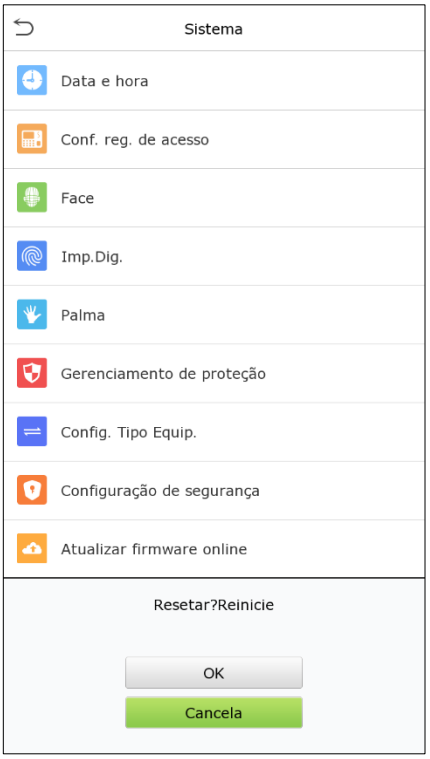
Com a função ativada, clique **em Check for Updates** para checar se a sua versão é a atual, caso contrário, será disponibilizada a versão mais atual para você baixar e instalar.



7.11 Restaurar padrões de fábrica

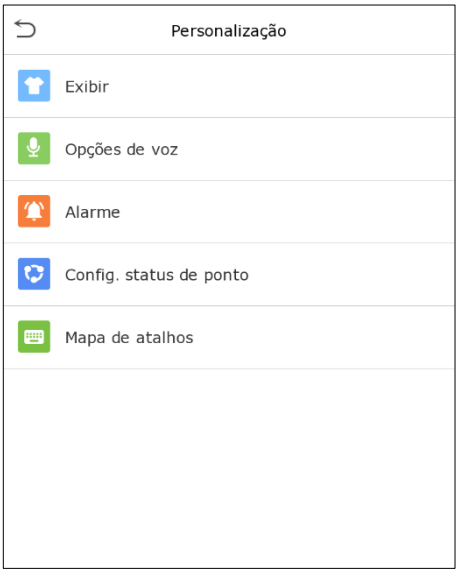
A função de **Restaurar de Fábrica** restaura as configurações do dispositivo, como configurações de comunicação e configurações do sistema para as configurações padrão de fábrica (esta função não limpa os dados de cadastro do usuário e nem logs de acesso).

Toque em **Resetar** na tela de **Sistema** e, em seguida, toque em **OK** para restaurar os padrões de fábrica.



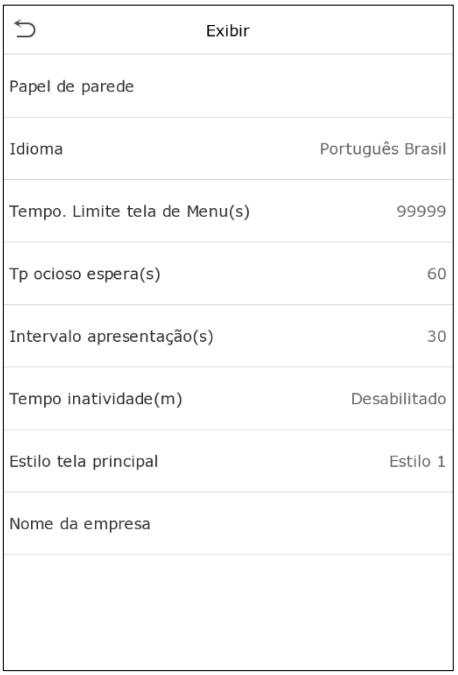
8 Personalização

Toque em **Personalização** na tela do **Menu Principal** para personalizar as configurações, voz, campainha, opções de estado de ponto e mapeamento de teclas de atalho



8.1 Exibir

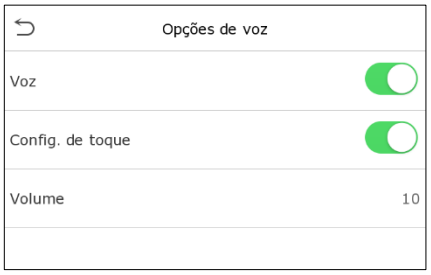
Toque em **Exibir** na tela de **Personalização** para personalizar o estilo de exibição da interface principal.



Função	Descrição
Papel de parede	Permite selecionar o papel de parede da tela principal.
Idioma	Permite selecionar 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.
Tp ocioso 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	Permite selecionar o estilo da tela principal, de acordo com a preferência do usuário.
Nome da empresa	Quando o equipamento está ligado a uma impressora na porta RS232, este nome será impresso no ticket após uma autenticação válida.

8.2 Opção de voz

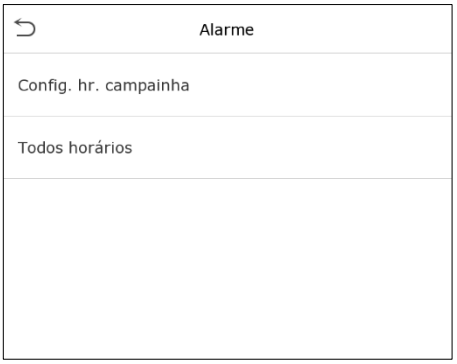
Toque em **Opções de Voz** na interface **Personalização** para definir as configurações de voz.



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

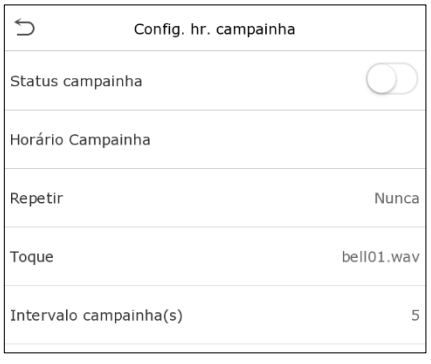
8.3 Alarme

Toque em **Alarme** na tela **Personalização** para definir as configurações de **Alarmes**.



Novo Alarme:

Toque em **Config. hr. campainha** na interface **Alarme** para adicionar uma nova programação de Alarme.



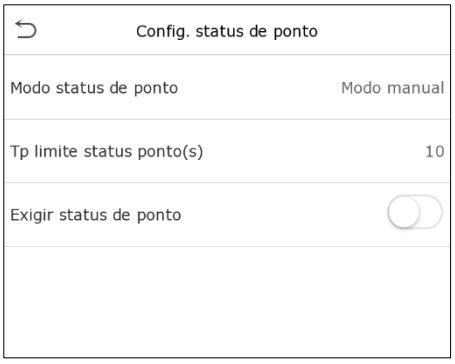
Função	Descrição
Status da campainha	Alterne para ativar ou desativar o status da campainha.
Horário campainha	Uma vez definido o horário, o dispositivo acionará automaticamente para tocar a campainha durante esse tempo.
Repetir	Defina os dias da semana caso seja necessário repetir.
Toque	Selecione um 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:** Assim que a campainha estiver agendada, na interface de **Alarme**, 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 no alarme a ser deletado. Em seguida, toque em **Excluir** e selecione **Sim** para excluir a campainha selecionada.

8.4 Configurações de Status de ponto (presença)

Selecione a opção **Config. Status de ponto** na tela de **Personalização** para ajustar as configurações do estado de ponto/presença.



Função	Função
Modo de Status de ponto	Selecione um Modo de Status de Ponto/Presença: **Desligado:** Isso desabilita a função de registro de presença. E a tecla de registro de presença definida no menu de **Mapeamento de Teclas de Atalho** se torna inválida. **Modo Manual:** Altere manualmente a tecla de registro de presença, e ela desaparecerá após o **Tempo Limite do Estado de Registro de Presença.** **Modo Automático:** A tecla de registro de presença alternará automaticamente para um status de registro de presença específico de acordo com o cronograma predefinido, que pode ser configurado no **Mapeamento de Teclas de Atalho**. **Modo Manual/Automático:** A interface principal exibirá a tecla de registro de presença de alternância automática. No entanto, os usuários ainda poderão selecionar uma alternativa que é o status de presença manual. Após o tempo limite, a tecla de registro de presença manual se tornará uma tecla de registro de presença automática. **Modo Manual Fixo:** Depois que a tecla de registro de presença for configurada manualmente para um status de registro de presença específico, a função permanecerá inalterada até que seja alterada manualmente. **Modo Fixo:** Somente a tecla de registro de presença definida manualmente será exibida. Os usuários não podem alterar o status pressionando outras teclas.
Tp limite status de ponto (s)	É o tempo pelo qual o estado de registro de presença é exibido. O valor varia de 5 a 999 segundos.

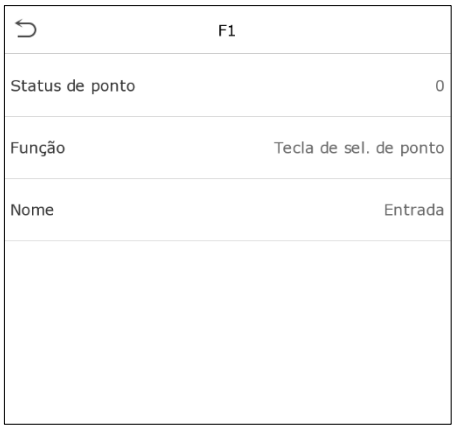
Exigir status de ponto	Escolher se um estado de registro de presença precisa ser selecionado durante a verificação.

8.5 Mapa de Atalhos

Os usuários podem definir teclas de atalho para os status de registro de presença e teclas funcionais na tela principal. Portanto, na tela principal, quando as teclas de atalho são pressionadas, o status de registro de presença ou a tela funcional são exibidos.

Toque em **Mapa de atalhos** na interface de **Personalizar** para configurar as teclas de atalho necessárias.

- Na tela de **Mapeamento de Teclas de Atalho**, toque na tecla de atalho necessária para ajustar as configurações da tecla de atalho.
- No tela da **Tecla de Atalho ("F1")**, toque em função para definir uma ação da tecla de atalho, seja como tecla de status de presença ou como tecla de função.
- Se a tecla de atalho for definida como uma tecla de função (Ex.: Novo usuário, Todos os usuários, etc.), a configuração é feita como mostrado na imagem abaixo.



- Se a tecla de atalho for definida como uma tecla de estado de presença (Ex.: entrada, saída, etc.), então é necessário configurar o valor do estado de presença (valor válido de 0 a 250), o nome e o horário de troca.

9 Gerenciamento de Dados

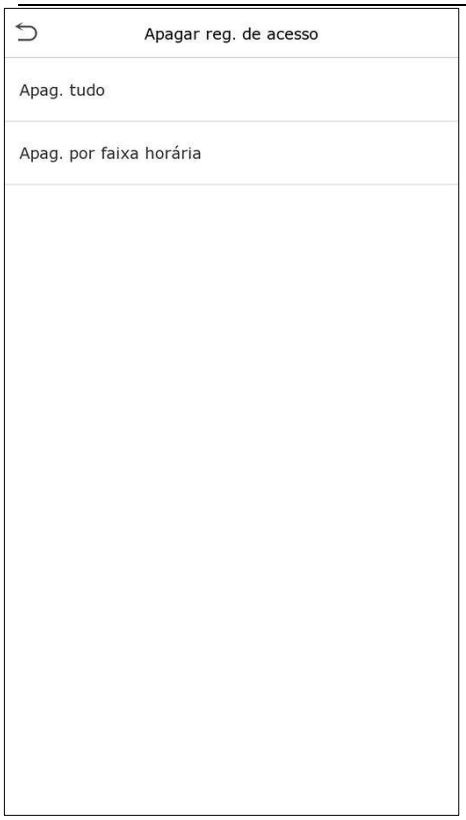
No tela do **Menu Principal**, toque em **Gerenciamento de Dados** acessar as opções disponíveis.

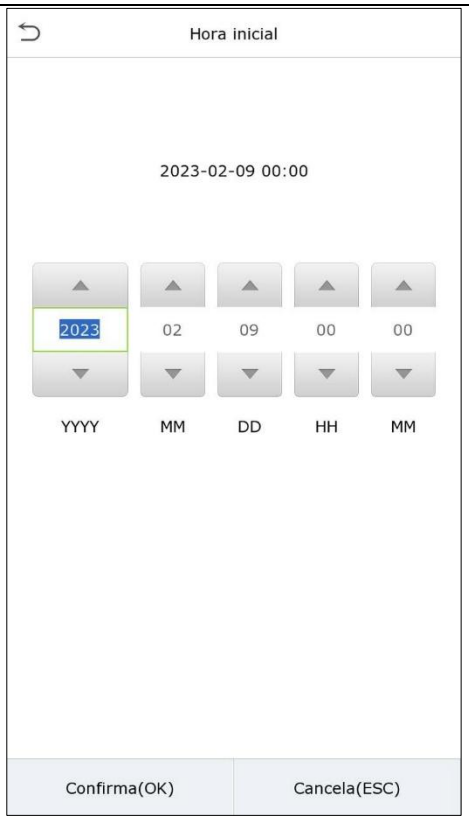
9.1 Apagar Dados

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

Função	Descrição
Apagar reg. de acesso	Para apagar dados de frequência/registros de acesso
Apagar foto ponto	Para apagar fotos de ponto registradas.
Apagar foto lista bloqueados	Para apagar as fotos tiradas durante verificações com falha.
Apagar tudo	Para apagar informações e registros de presença/registros de acesso de todos os usuários registrados.
Apagar priv. Admin	Para remover todos os privilégios de administrador (não apagar usuários).
Apag. dados de acesso	Para apagar todos os dados de acesso.
Excluir Templates de Fotos de Usuário	Para excluir templates de fotos do usuário no dispositivo. Ao excluir templates, uma tela de aviso será exibida: "**Um novo cadastro facial será necessário após atualização do algoritmo**".
Apagar foto do usr.	Para apagar todas as fotos do usuário no dispositivo.
Apagar papel de parede	Para apagar todos os papéis de parede no dispositivo.
Apagar proteção de tela	Para apagar os protetores de tela no dispositivo
Apagar lista de contatos	Apaga a lista de contatos do menu **Interfone>Config. SIP>Lista de contatos.**

O usuário poderá selecionar **Apagar Tudo** ou **Apagar por Faixa de Horário** quando quiser apagar os registros de acesso, fotos de ponto ou fotos listas de bloqueio. Para mostrar a opção **Apagar por intervalo de tempo**, você precisa ativar as funções de exclusões cíclicas em **Menu>Sistema>Config. reg. De acesso.**



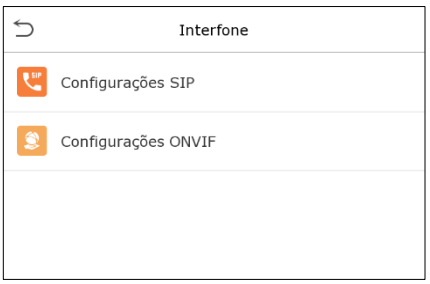


Selecione Apagar por intervalo de tempo.

Defina o intervalo de tempo e clique em OK.

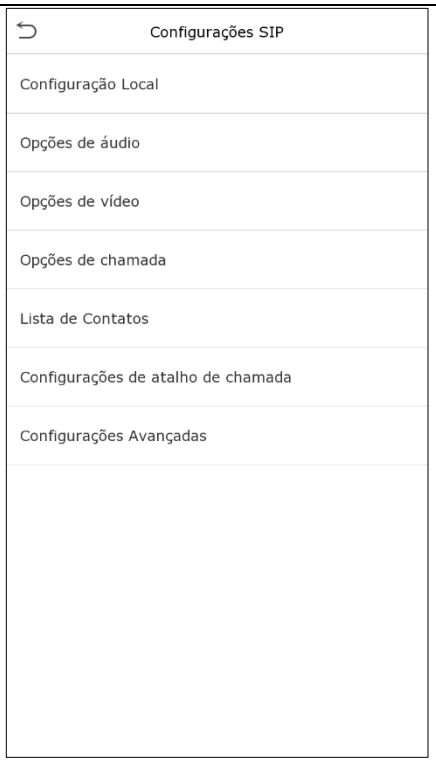
10 Interfone

Na tela do **Menu Principal**, toque em **Interfone** você poderá definir todos os parâmetros para a **Configuração SIP** e **Configuração ONVIF**.

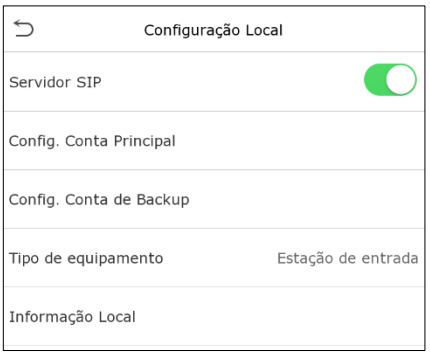


10.1 Configurações SIP

Dentro de **Configurações SIP**, as opções de são mostradas abaixo:



10.1.1 Configuração Local

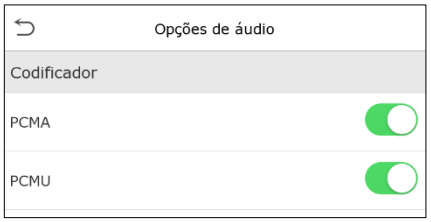


Função	Descrição
Servidor SIP	Ativa ou desativa a função de SIP
Config. Conta Principal	**Config. Conta Principal:** Ativa ou desativa a conta principal. **Habilita nome domínio:** Se ativada, é possível colocar o domínio ao invés do IP. **End. Servidor:** Endereço do servidor SIP (IP ou domínio). **Porta Servidor:** Porta do servidor SIP. **Nome Exibição:** Nome do ramal SIP. **Usuário:** Usuário do ramal SIP. **Verificar ID:** ID do ramal SIP. **Senha:** Senha do ramal SIP. **Servidor STUN:** Ativa ou desativa a função STUN **End. Servidor:** Se a função STUN for ativada, permite configurar o endereço do servidor STUN. **Usuário:** Se a função STUN for ativada, permite configurar usuário do servidor STUN. **Senha:** Se a função STUN for ativada, permite configura a senha do servidor STUN. **OutBund:** Se a função STUN for ativada, permite configurar o OutBund. **Protocolo de Transmissão:** Permite trabalhar com UDP, TCP ou TLS.

Config Conta de Backup	Permite configurar uma segunda conta de servidor SIP, caso a conta principal fique inativa, não será necessário mudar os parâmetros da conta principal. As configurações desta tela são as mesmas da conta principal.
Tipo de equipamento	Permite selecionar as opções: **Estação de entrada, Terminal Cont. de Acesso ou Terminal de Portão**.
Informação Local	Permite configurar o número do **Bloco, Unidade, Piso e Porta**.

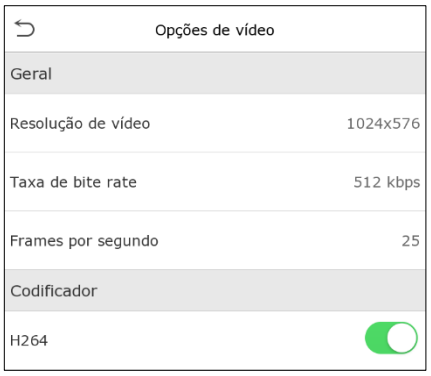
10.1.2 Opções de áudio

Permite configurar qual será o codec de áudio usado durante a chamada SIP, as opções são **PCMA** e **PCMU**.



10.1.3 Opções de vídeo

Permite configurar as opções de vídeo durante a chamada SIP.



Função	Descrição
Resolução de vídeo	Permite alterar entre 1024x576 ou 720x1280
Taxa de bit rate	Permite selecionar as opções 128kbps, 256kbps, 512kbps, 800kbps ou 1024kbps.
Frames por segundo	Esta opção é fixada em 25fps
H264	Permite ativar ou desativar a codificação H64

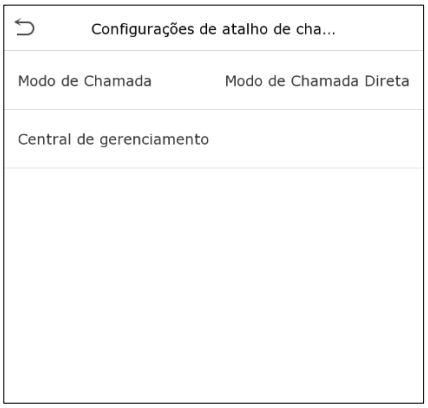
10.1.4 Opções de chamada

Função	Descrição
Atraso (s) de chamada	Permite configurar o tempo que o equipamento irá tocar para o ramal se não houver atendimento. Finalizado este tempo sem o ramal atender, esta solicitação de chamada é encerrada. Pode ser configurado entre 30s~60s.
Atraso (s) para falar	Permite configurar o tempo de chamada ativa, finalizado este tempo, a chamada será automaticamente encerrada. Pode ser configurado entre 60s~120s.
Confi. Vol. Chamada	Permite configurar o volume do alto falante do dispositivo durante uma chamada SIP. Pode ser configurado entre 0~100.
Tipo de chamada	**Voz:** Realiza apenas a chamada SIP com voz. **Voz+Vídeo:** Realizar a chamada SIP com voz e vídeo.
Estilo do botão de chamada	Permite escolher entre as opções **Campainha** ou **Telefone**, a mudança será aplicada no ícone flutuante de chamada SIP na tela principal.
Config. Resposta Auto.	Permite ativar ou desativar o atendimento automático.
Atraso da Resposta Auto.	Se **Config. Resposta Auto.** estiver ativada, possibilita configurar o atraso para o atendimento automático.
Intervalo de Autenticação	Durante uma chamada SIP ativa o usuário pode clicar no ícone de face para mudar para o reconhecimento facial, este parâmetro permite configurar o atraso para que automaticamente a tela retorne para a de chamada SIP.
Criptografia	Permite ativar a criptografia SRTP (Secure Real-Time Transport Protocol) é um protocolo que protege o tráfego de áudio e vídeo em tempo real.

10.1.5 Configurações de atalho de chamada

Permite selecionar o **Modo Padrão** ou **Modo de chamada Direta**

Modo Padrão

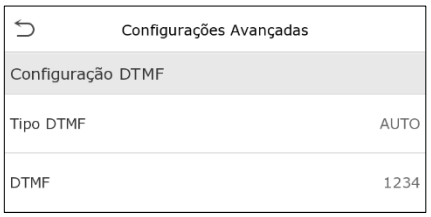


Modo de chamada Direta

- **Modo Padrão:** Permite criar teclas de atalho com números de ramais pré-definidos, de forma que o usuário ao clicar no ícone da tela principal, abra o teclado para digitar e seja exibida as teclas de atalhos pré-definidas.
- **Modo de chamada direta:** Permite configurar um ramal para fazer a chamada direta, de forma que o usuário ao clicar no ícone da tela principal, faça a chamada direta para o ramal pré-definido.

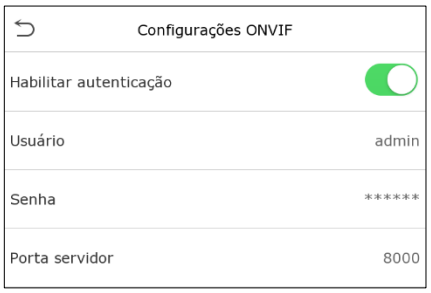
10.1.6 Configurações Avançadas

Em **Configuração DTMF** é possível configurar o tipo de DTMF e a senha para o DTMF.



Função	Descrição
Tipo DTMF	Permite alterar entre SIP INFO, RFC2833 ou AUTO.
DTMF	A configuração da senha DTMF será para que, durante uma chamada SIP, se o atendente digitar a senha pré-definida, o relé de saía para fechadura seja acionado.

10.2 Configurações ONVIF



Função	Descrição
Habilitar autenticação	Permite ativar ou desativar a autenticação por usuário e senha.
Usuário	Caso a autenticação esteja ativada, é necessário inserir o usuário.
Senha	Caso a autenticação esteja ativada, é necessário inserir a senha.

Porta servidor	Porta para comunicação do ONVIF.

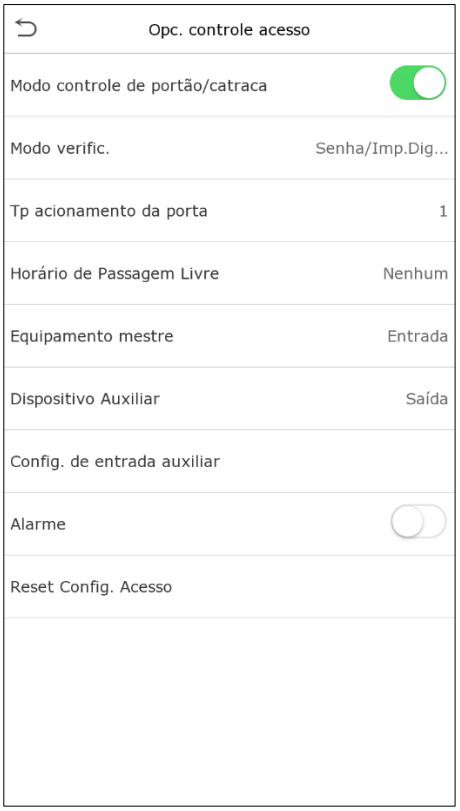
11 Controle de acesso

Na tela do **Menu Principal**, toque em **Controle de acesso** você poderá definir o tempo de abertura de portas, controle de fechaduras e configurar outros parâmetros relacionados ao controle de acesso.

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

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

11.1 Opções de controle de acesso



Função	Descrição
Modo de controle de portão/catraca	Alterne entre **ON** ou **OFF** para entrar no modo de controle do portão/catraca ou não. Quando definido como **LIGADO**, nesta tela as opções de tempo de relé, sensor de porta e tipo de sensor de porta serão removidos.
Tempo do relé (s)	Tempo de acionamento do relé após uma autenticação válida. Valor válido: 1~99 segundos; 0 segundo representa função desativada.
Atraso do sensor da porta (s)	Se a porta não estiver travada e for deixada aberta por um determinado período (Atraso do sensor da porta), um alarme será acionado. O valor válido do Atraso do Sensor da Porta varia de 1 a 255 segundos
Tipo de sensor de porta	Existem três opções de Sensores: **Nenhum, Normal Aberto e Normal Fechado.** **Nenhum**: significa que o sensor da porta não está em uso. **Normal Aberta**: Com a porta fechada, o equipamento espera um sinal aberto. **Normal Fechado**: Com a porta fechada, o equipamento espera um sinal fechado
Modo de verificação	O modo de verificação suportado inclui Senha/Impressão Digital/Face, Apenas Impressão Digital, Apenas ID de Usuário, Senha, ID de Usuário + Impressão Digital, Impressão Digital + Senha, ID de Usuário + Impressão Digital + Senha, Apenas Face, Face + Impressão Digital, Face + Senha, Face + Impressão Digital + Senha.
Tempo de disponibilidade da porta	Para definir o período de tempo para a porta, para que a porta esteja disponível apenas durante esse período.
Horário de passagem livre	Período de tempo programado para o modo "Normal Aberto", para que a

	porta fique sempre aberta durante este período.
Equipamento mestre	Ao configurar o equipamento mestre, o status pode ser definido para sair ou entrar. **Saída:** O registro no relatório do software será feito como saída. **Entrada:** O registro no relatório do software será feito como entrada.
Dispositivo auxiliar	Ao configurar o dispositivo auxiliar, o status pode ser definido para sair ou entrar. **Saída:** O registro no relatório do software será feito como saída. **Entrada:** O registro no relatório do software será feito como entrada.
Configuração de entrada auxiliar	• A entrada auxiliar pode ser configurada para não fazer nada se marcada como "**Nenhum**". • Se marcada a opção "**Acionamento de porta**", ao acionar a entrada • auxiliar, a saída a relé de porta será acionada. • Se marcada a opção de "**Acionamento de alarme**", ao acionar a entrada auxiliar, a saída de alarme será acionada e o software recebe um evento de alarme. • Se marcada a opção "**Acionamento de porta e Alarme**", ao acionar a entrada auxiliar, a saída a relé de porta será acionada e a saída de alarme, além disso, o software recebe um evento de alarme. Se marcada a opção "**Tocar a campainha**", ao acionar a entrada auxiliar, a chamada SIP será efetuada para o ramal definido na chamada direta em **Interfone>Configurações SIP>Configurações de atalho>Modo de chamada**
Alarme	Emite um alarme sonoro quando a porta estiver fechada ou a verificação for bem-sucedida, o sistema cancelará o alarme do local.
Reset das configurações de acesso	O reset dos parâmetros de controle de acesso inclui tempo de relé, tempo de atraso do sensor, tipo de sensor, modo de verificação, Tempo de disponibilidade da porta, Horário de passagem livre, dispositivo mestre/auxiliar e alarme. Esta função não apaga dados de logs de acesso, par isso, utilize a opção do menu principal **Ger. Dados**.

11.2 Configuração de regra de tempo

Toque em Configuração de Regra de Tempo na tela de controle de acesso para definir as configurações de tempo

- O equipamento permite definir até 50 períodos de tempo.
- Cada período de tempo representa 10 faixas horárias, ou seja, 1 semana e 3 feriados, e cada faixa horária possui um período padrão de 24 horas por dia. O usuário só pode verificar dentro do período de tempo válido**.**

Pode-se definir um máximo de 3 intervalos de tempo para cada faixa horária. A relação entre esses intervalos de tempo é "OU". Assim, quando uma autenticação cair em qualquer um desses intervalos de tempo, a autenticação será válida.

- O formato de faixa horária para cada intervalo de tempo é: **HH:MM-HH:MM**, de acordo com o relógio de 24 horas.

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

Para ajustar uma faixa horária, clique sobre a faixa horária desejada e ajuste os horários conforme tela abaixo:

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

Observação:

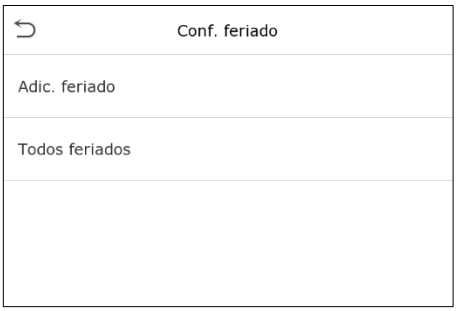
- Quando o horário de término é menor que o horário de início (Ex.: 23:57~23:56), indica que o acesso está proibido o dia todo.
- Quando a hora de término for maior que a hora de início (como 00:00~23:59), isso indica que o intervalo é válido.

- O período de tempo efetivo para manter a porta desbloqueada ou aberta o dia todo é (00:00~23:59) ou também quando a hora de término é posterior à hora de início (como 08:00~23:59).

11.3 Configurações de Feriado

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 autenticar como válido nos feriados.

Toque em **Conf. Feriado** na tela de **Controle de Acesso** para definir o acesso em **Feriados**.



- **Adicionar um novo feriado:**

Toque em **Adic. Feriado** na tela de **Feriados** e defina os parâmetros

- **Editar um feriado:**

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

- **Excluir um feriado:**

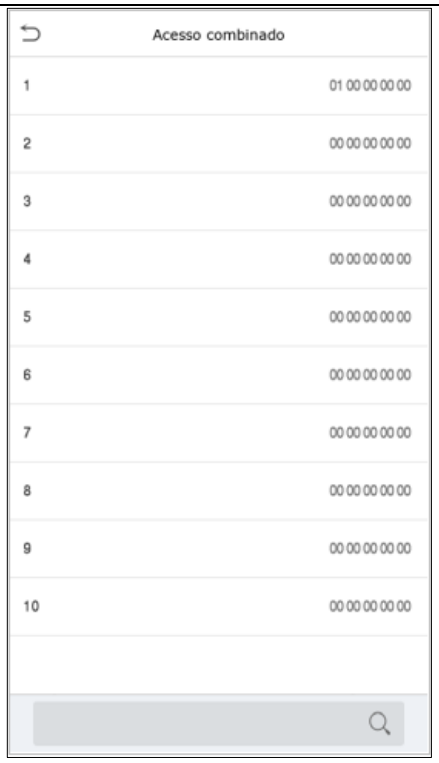
Na tela de **Feriados**, selecione um item de feriado a ser excluído e toque em **Apagar**. Pressione **OK** para confirmar a exclusão. Após a exclusão, este feriado não é mais exibido na interface **Todos os feriados**.

11.4 Acesso combinado

Os grupos de acesso são organizados em diferentes combinações de desbloqueio de portas para obter várias verificações e aumentar a segurança.

Em uma combinação de destravamento de porta, a faixa do número combinado N é: $0 \le N \le 5$, o número de membros N pode pertencer a um grupo de acesso ou pode pertencer a cinco grupos de acesso diferentes.

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



- Se a **combinação de desbloqueio da porta 3** for configurada como (09 09 09 09 09), isso indica que existem 5 pessoas nesta combinação; todas elas são do Grupo AC 9.
- Se a **combinação de desbloqueio da porta 4** for configurada como (03 05 08 00 00), isso indica que a combinação de desbloqueio 4 é composta apenas por três pessoas. A primeira pessoa é do Grupo AC 3, a segunda pessoa é do Grupo AC 5 e a terceira pessoa é do Grupo AC 8.

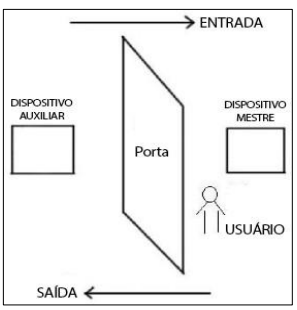
Observações:

- Para excluir a combinação de desbloqueio da porta, configure todas as combinações de desbloqueio da porta para 0.
- Se a lista de Acesso Combinado estiver vazia, acesse **Ger. Dados>Apagar dados>Apag. Dados Acesso** para restaurar a configuração padrão.

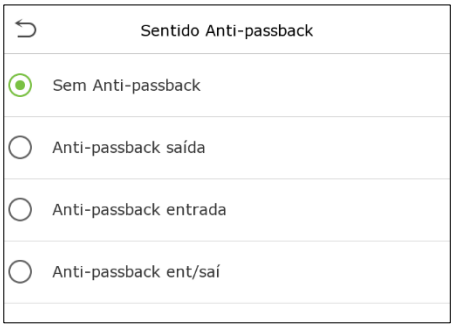
11.5 Configuração Anti-Passback

É possível que os usuários sejam seguidos por algumas pessoas para entrar sem autenticação, resultando em uma violação de segurança. Para evitar tal situação, foi desenvolvida a opção Anti- Passback. Uma vez habilitado, a autenticação de entrada deve alternar com a autenticação de saída (ou vice-versa) para garantir uma autenticação válida. Evitando desta forma duas ou mais autenticações válidas para entrada sequenciadas ou para saída sequenciadas, obrigando o usuário que entrou, a próxima ação seja a saída (e vice-versa)!

Esta função requer que dois dispositivos funcionem juntos: um é instalado dentro da porta (dispositivo mestre) e o outro é instalado fora da porta (dispositivo auxiliar). Os dois dispositivos se comunicam através do sinal Wiegand. O formato Wiegand e o tipo de saída (ID do usuário / número do cartão) precisa estar configurado de forma igual no dispositivo mestre e no dispositivo auxiliar.



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

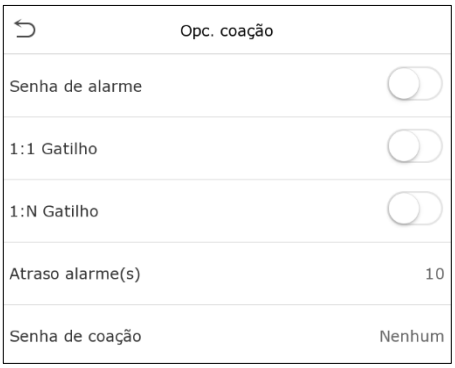


Função	Descrição
Direção Anti-Passback	**Sem Anti-Passback:** A função Anti-Passback está desativada, o que significa que a verificação bem-sucedida através do dispositivo mestre ou do dispositivo auxiliar pode desbloquear a porta. O status de entrada ou saída não é salvo nesta opção para o próximo desbloqueio. **Anti-Passback saída**: depois que um usuário faz a saída, somente se o último registro for um registro de entrada que o usuário poderá fazer saída novamente; caso contrário, o alarme será acionado. No entanto, o usuário pode fazer a entrada normalmente. **Anti-Passback entrada:** Após a entrada de um usuário, somente se o último registro for um registro de saída que o usuário poderá fazer a entrada novamente; caso contrário, o alarme será acionado. No entanto, o usuário pode fazer a saída normalmente. **Anti-Passback de entrada/saída:** Após um usuário fazer entrada/saída, somente se o último registro for um registro de saída, o usuário poderá fazer entrada novamente; ou se for um registro de entrada, o usuário pode fazer saída novamente; caso contrário, o alarme será acionado.

11.6 Opções de Coação

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

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



Função	Descrição
Senha de alarme	Quando um usuário usa o método de verificação de senha, um sinal de alarme será gerado somente quando a autenticação por senha for bem-sucedida, caso contrário não haverá sinal de alarme.
1:1 Gatilho	Quando um usuário utiliza o método de autenticação por impressão digital 1:1, um sinal de alarme será gerado; caso contrário, não haverá sinal de alarme.

Alarme em Caso de Autenticação 1:N	Quando um usuário utiliza o método de autenticação por impressão digital 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 tenha decorrido. O valor varia de 1 a 999 segundos
Senha de coação	Defina a senha de coação de 6 dígitos. Quando o usuário insere esta senha de coação para autenticação, um sinal de alarme é gerado.

12 Procurar registros

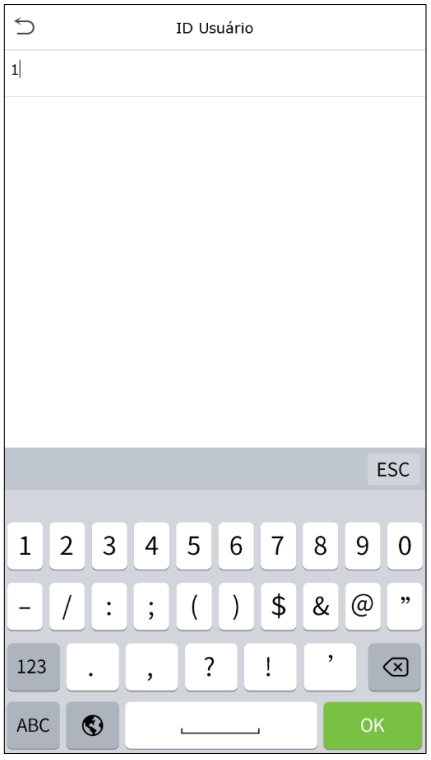
Assim que a autenticação de um usuário for validada, os logs de eventos serão salvos no dispositivo. Esta função permite que os usuários consultem seus registros de acesso.

Clique em **Procurar Registros** na tela do **Menu Principal** para pesquisar o registro de Acesso/Presença desejado.

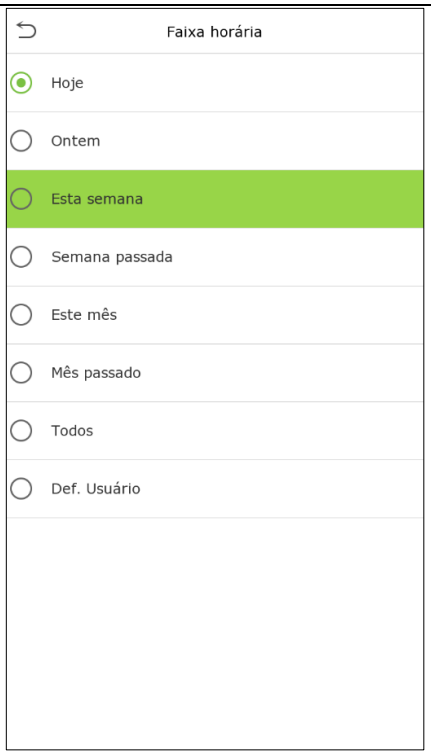
O processo de pesquisa de fotos de presença e lista de bloqueados é semelhante ao da pesquisa de logs de eventos. Veja a seguir um exemplo de pesquisa de logs de eventos.

Na tela de **Reg. acesso**, toque em **Logs de eventos** para pesquisar o registro desejado.

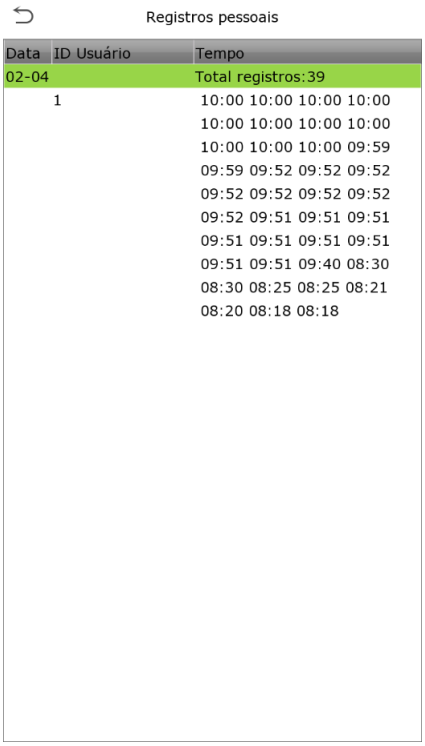
- Insira **o ID do usuário** a ser pesquisado e clique em **OK**. Se desejar pesquisar logs de todos os usuários, clique em **OK** sem inserir nenhum **ID de usuário**.



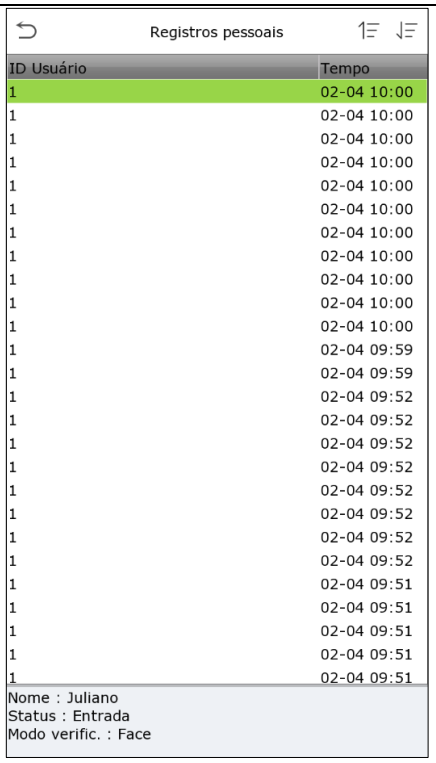
- Selecione o intervalo de tempo em que os logs precisam ser pesquisados



- Depois que a pesquisa de log for bem-sucedida, toque desejado para visualizar seus detalhes.

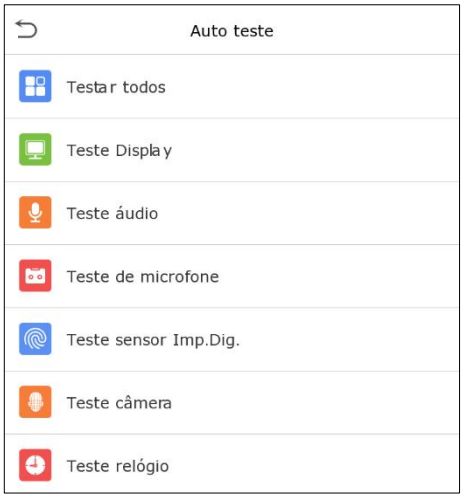


- A figura abaixo mostra os detalhes do log selecionado.



13 Autoteste

No Menu Principal, toque em **Autoteste** para testar automaticamente se todos os módulos do dispositivo funcionam corretamente, incluindo Display, áudio, microfone, sensor de impressão digital, câmera e relógio.

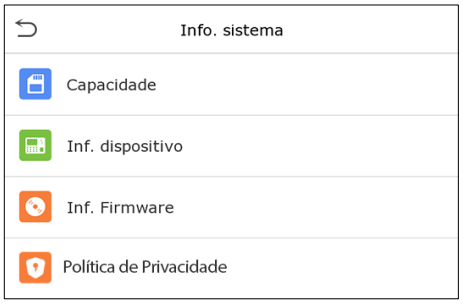


Função	Descrição
Testar todos	Para testar automaticamente se o display, áudio, microfone, sensor digital, câmera e relógio estão normais.
Teste Display	Para testar automaticamente o display exibindo cores diferentes, para verificar se a tela exibe as cores normalmente.
Teste áudio	Para testar automaticamente se os arquivos de áudio armazenados no dispositivo estão completos e se a qualidade da voz é boa
Teste de Microfone	Para testar se o microfone está funcionando corretamente (Fale no microfone).

Testar o Sensor de Impressão Digital	Testa o sensor de impressão digital, pressionando um dedo no scanner para verificar se a imagem da impressão digital adquirida está clara.
Teste câmera	Para testar se a câmera funciona corretamente, checando as imagens para ver se elas estão suficientemente nítidas.
Teste relógio	Para testar o RTC. O dispositivo testa se o relógio funciona normalmente e com precisão com um cronômetro. Toque na tela para começar a contar e pressione-o novamente para parar de contar.

14 Informação do sistema

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

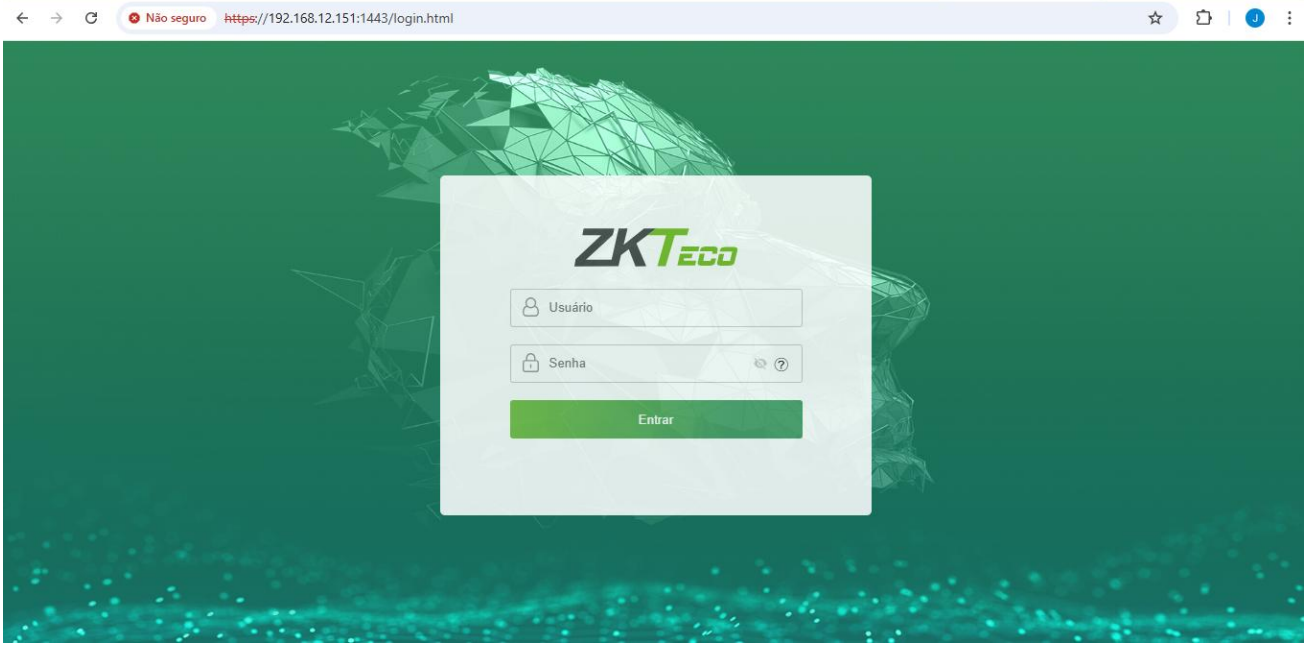


Menu	Descrição
Capacidade do dispositivo	Exibe o armazenamento do dispositivo atual, palma, senha, face, cartão, administradores, registros de acesso, fotos de presença e lista de bloqueio e fotos do usuário.
Informação do dispositivo	Exibe o nome do dispositivo, número de série, endereço MAC, algoritmo de palma e face, informações de versão, informações de plataforma e fabricante e data de fabricação.
Informações de firmware	Exibe a versão do firmware e outras informações de versão do dispositivo.
Política de Privacidade	O controle da política de privacidade aparecerá quando o dispositivo for ligado pela primeira vez. Depois de clicar em "**Eu li**", o cliente pode usar o produto regularmente. Clique em I**nformações do sistema -> Política de privacidade** para visualizar o conteúdo da política de privacidade. O conteúdo da política de privacidade não permite a exportação de discos U. **Nota**: O texto da política de privacidade atual está disponível apenas em chinês simplificado/inglês. No entanto, a tradução do conteúdo em vários idiomas está em andamento, com mais iterações.

15 Webserver

O speedface possui uma interface web para fazer configurações, para acessar esta interface web use a URL:

https://IP_DO_DISPOSITVO:1443 (Ex.: https://192.168.12.151:1443/), a tela abaixo será exibida:



Para realizar o login use a credencial abaixo:
Usuário: admin
Senha: admin@123

No primeiro acesso, o webserver solicita a troca da senha de fábrica para uma senha que o usuário irá criar, conforme mostrado na tela abaixo:

Para mais informações sobre as funcionalidades do webserver consulte no nosso manual no LINK.

16 Apêndice 1

16.1 Requisitos para cadastro de face diretamente pelo dispositivo.

1) É recomendado realizar o cadastro em um ambiente interno com uma fonte de luz adequada, sem subexposição ou superexposição no rosto.
2) Não posicione o dispositivo em direção a fontes de luz externas, como portas, janelas ou outras fontes de luz intensa.
3) Roupas de cor escura, diferentes da cor de fundo, são recomendadas para o cadastro.
4) Exponha adequadamente sia face e testa, não cubra a face e as sobrancelhas com o cabelo.
5) É recomendado mostrar uma expressão facial normal. (Um leve sorriso é aceitável, mas não feche os olhos ou incline a cabeça para qualquer direção).
6) Durante o cadastro da face, para pessoas com óculos, tire e coloque antes de terminar o tempo.
7) Não use acessórios como lenço ou máscara que possam cobrir a boca ou o queixo.
8) Posicione-se diretamente em direção ao dispositivo durante o cadastro e posicione sua face na área de captura de imagem.
9) Não inclua mais de uma face na área de captura.
10) É recomendada uma distância de 50cm a 80cm para capturar a imagem. (A distância é ajustável, dependendo da altura do usuário).

Telefone: (31) 3055-3530
Endereço: Rodovia MG-010, KM 26
Loteamento 12 - Bairro Angicos
Vespasiano - MG - CEP: 33.206-240
www.zkteco.com.br

16.2 Requisitos para cadastro de face através de uma foto

A foto digital ter bordas retas, ser colorida, um pouco retratada, com apenas uma pessoa, e essa pessoa deve estar com expressão facial normal e vestindo roupas casuais. As pessoas que usam óculos devem permanecer com os óculos ao serem fotografadas.

Distância dos olhos

São recomendados 200 pixels ou mais e não menos de 115 pixels de distância.

Expressão Facial

Face neutra ou sorriso simples. Os olhos devem estar naturalmente abertos.

Gesto e ângulo

O ângulo de rotação horizontal não deve exceder ±10° e a elevação e 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

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

Formato de imagem

Os formatos permitidos são BMP, JPG ou JPEG.

Outros Requisito

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 no mesmo nível horizontal.
7) Os olhos da pessoa capturada devem estar abertos e com a íris claramente visível.
8) 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 na face ou no fundo. O nível de contraste e luminosidade deve ser adequado.

17 Apêndice 2

17.1 Política de Privacidade

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

I. Informações coletadas

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

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

II. Segurança e gerenciamento de produtos

1. Ao usar nossos produtos pela primeira vez, você deve definir o privilégio de administrador antes de executar operações específicas. Caso contrário, você será frequentemente lembrado de definir o privilégio de administrador quando entrar na tela do menu principal. Se você não definir o privilégio de administrador após receber o aviso do sistema, você deve estar ciente do possível risco de segurança (por exemplo, os dados podem ser modificados manualmente).
2. Todas as funções de exibição de informações biométricas estão desativadas em nossos produtos por padrão. Você pode em **Menu > Configurações do sistema** definir se deseja exibir as informações biométricas. Se você habilitar essas funções, assumimos que você está ciente dos riscos de segurança especificados na política de privacidade.
3. Apenas seu ID de usuário é exibido por padrão. Você pode definir se deseja exibir outras informações de verificação do usuário (como Nome, Departamento, Foto, etc.) sob o privilégio de Administrador.

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

4. A função de captura de foto da câmera está desativada em nossos produtos por padrão. Se você deseja habilitar esta função para tirar fotos de usuários para registro de acesso ou tirar fotos de estranhos para controle de acesso, o produto ativará o som de alerta da câmera. **Depois de habilitar esta função, presumimos 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 carregados pelo Administrador em nossos produtos são criptografados automaticamente usando o algoritmo AES 256 e armazenados com segurança. Se o administrador baixar dados de nossos produtos, presumimos que você precisa processar os dados e conhece o risco potencial de segurança. Nesse caso, você assumirá a responsabilidade pelo armazenamento dos dados. Você deve saber que alguns dados não podem ser baixados por questões de segurança de dados.
6. Todas as informações pessoais em nossos produtos podem ser consultadas, modificadas ou excluídas. Se você não for usar mais nossos produtos, limpe seus dados pessoais.

III. Como lidamos com informações pessoais de menores

Nossos produtos, site e serviços são projetados principalmente para adultos. Sem o consentimento dos pais ou responsáveis, os menores não devem criar a sua própria conta. Se você for menor de idade, é recomendável que você peça a seus pais ou responsáveis que leiam atentamente esta Política, e somente use nossos serviços ou informações fornecidas por nós com o consentimento de seus pais ou responsáveis.

Só usaremos ou divulgaremos informações pessoais de menores coletadas com o consentimento de seus pais ou responsáveis se e na medida em que tal uso ou divulgação for permitido por lei ou obtivermos o consentimento explícito de seus pais ou responsáveis, sendo tal uso ou divulgação para fins de proteção de menores.

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

IV. Outros

Você pode visitar o site https://www.zkteco.com/en/privacy_policy para obter mais informações sobre como coletamos, usamos e armazenamos com segurança suas informações pessoais. Para acompanhar o rápido desenvolvimento da tecnologia, ajustar as operações comerciais e atender às necessidades dos clientes, iremos constantemente deliberar e otimizar nossas medidas e políticas de proteção de privacidade.

17.2 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)	Cádimio (Cd)	Crómio hexavalente (Cr6+)	Bifenilos Polibromados (PBB)	Éteres de Difenila 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

18 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.

Unidade Vespasiano:
Rodovia MG-010, KM 26 - Loteamento 12 - Bairro Angicos,
Vespasiano - MG | CEP: 33.206-240
Unidade São Paulo:
Rua Cubatão, 86 – 18º andar (Cjs 1802 e 1803) - Bairro Vila Mariana,
São Paulo - SP | CEP: 04013-000
Entre em contato com a ZKTeco
comercial.brasil@zkteco.com
(31) 3055-3530