Manual do Usuário

Série SpeedFace-V5L

Data: Agosto de 2023

Versão do documento: 1.0

Português

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

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

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

Marca registrada

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

Responsabilidade

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

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

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

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

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

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

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

ZKTeco Filial Brasil

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

Telefone (31) 3055-3530

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

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

ANATEL 01094-23-12720

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

ANATEL 07935-23-12720

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

ANATEL 07937-23-12720

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

ANATEL 12509-20-12720

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

ANATEL 14815-21-12720

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

ANATEL 11891-22-11470

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

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

Sobre o Manual

Este manual apresenta as operações 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 com ★ não estão disponíveis em todos os dispositivos.

Convenções do Documento

As convenções utilizadas neste manual estão listadas abaixo:

Convenções de Interface Gráfica do Usuário:

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

Símbolos

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

Conteúdos

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

A série 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.

A série SpeedFace-V5L adota tecnologia de reconhecimento sem contato e identificação individual com máscara, eliminando efetivamente preocupações de higiene. Ela também está equipada com um algoritmo antifraude definitivo para reconhecimento facial, contra quase todos os tipos de ataques com fotos e vídeos falsos. Além disso, sua câmera facial suporta QR Code, PDF417, Data Matrix, MicroPDF417, Aztec, entre outros, com suporte do aplicativo móvel ZKBioAccess IVS para QR Code dinâmico para controle de acesso e presença.

A versão TD/TI com detecção de máscara ajuda a reduzir a propagação de germes e prevenir infecções diretamente em cada ponto de acesso de qualquer local, como hospitais, fábricas, escolas, edifícios comerciais e estações, durante o recente problema global de saúde pública, com sua função de identificação individual com máscara durante a verificação facial.

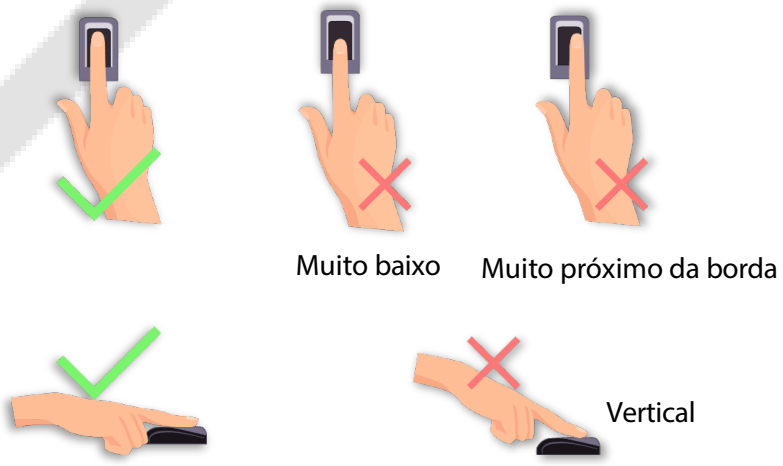
A série SpeedFace-V5L oferece suporte a videoporteiro tanto pelo aplicativo móvel ZSmart quanto pelo software para PC ZKBioTalk, além de serem integrados ao protocolo de vídeo ONVIF, permitindo que se conectem a NVRs Onvif para vigilância e gravação de vídeo.

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

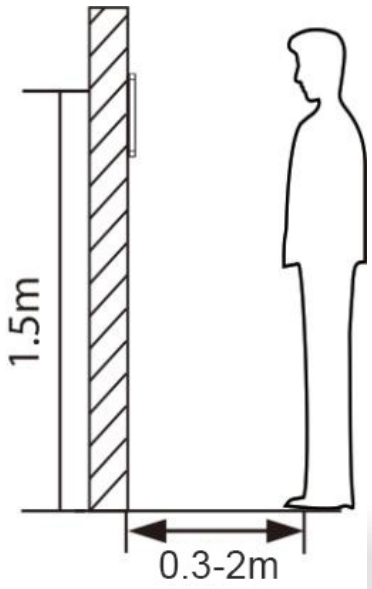
Dedos recomendados: Indicador, médio ou anelar; evite usar o polegar ou o mindinho, pois é difícil pressioná-los com precisão no leitor de impressões digitais.



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

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 naturais durante o registro ou verificação.

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 método de autenticação

Recomendações para cadastro de face

- Ao cadastrar uma face, mantenha uma distância de 40 cm a 80 cm entre o dispositivo e a face.
- Tenha cuidado para não mudar sua expressão facial. (Ex.: sorriso, etc.)
- Se você não seguir as instruções na tela, o cadastro de face pode demorar mais ou pode falhar.
- Tenha cuidado para não cobrir os olhos ou as sobrancelhas.
- Não use chapéus, bonés, máscaras, óculos de sol.
- Tenha cuidado para não exibir duas faces na tela. Cadastre uma pessoa por vez.
- Recomenda-se que um usuário que utilize óculos cadastre ambas as faces, com e sem óculos.

Recomendações para autenticar uma face

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

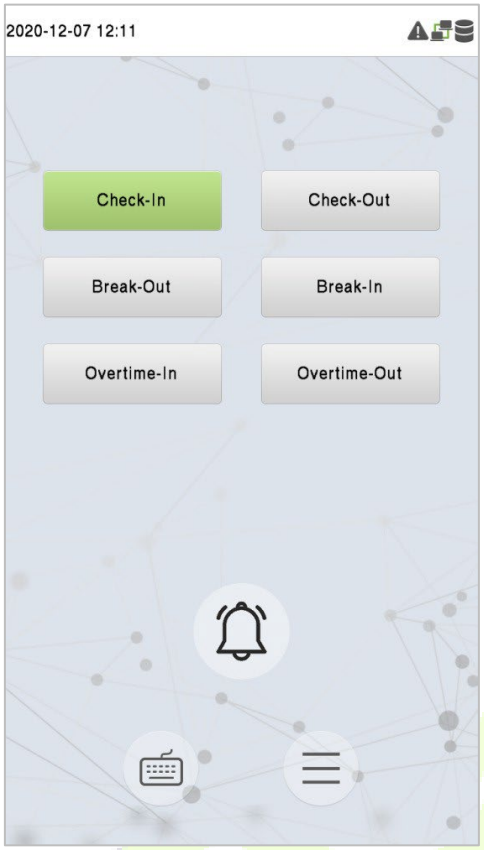
- Se uma parte do rosto estiver coberta com um chapéu, boné, máscara, tapa-olho ou óculos de sol, a autenticação pode falhar. Não cubra a face, permita que o dispositivo veja as sobrancelhas e a face.

1.4 Tela principal

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

Nota:

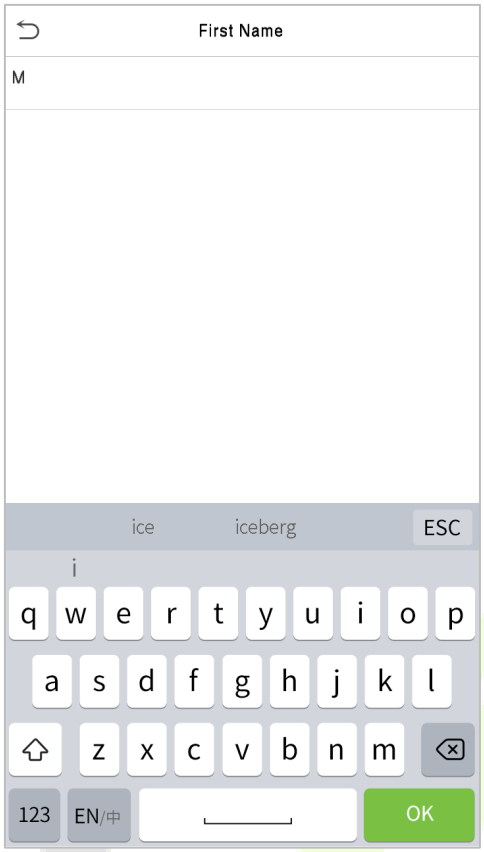
- Clique em para autenticar com ID do usuário.
- Quando não houver um super administrador cadastrado no dispositivo, clique em para ir ao menu.
- Após adicionar um Super Administrador no dispositivo, é necessário a verificação do Super Administrador antes de abrir as funções de menu.
  Observação: Para a segurança do dispositivo, é recomendado registrar 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 interface 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 correspondente ao estado de presença desejado para selecionar o seu estado de presença atual, que será exibido em verde. Consulte "Mapeamento de Teclas de Atalho" para obter o método de operação específico.

  Observação: As opções de status de registro de presença estão desativadas por padrão e é necessário selecionar outras opções de modo em "Opções de status de registro de presença" 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.

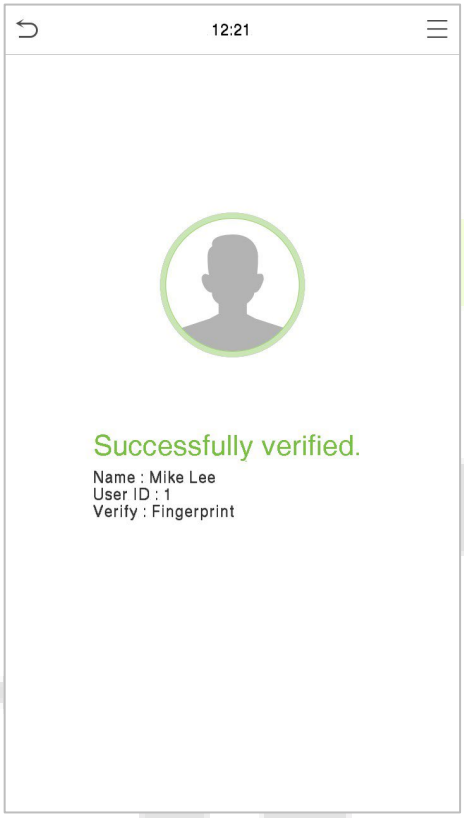
2.6 Modo de autenticação

2.6.1 Autenticação de impressão digital

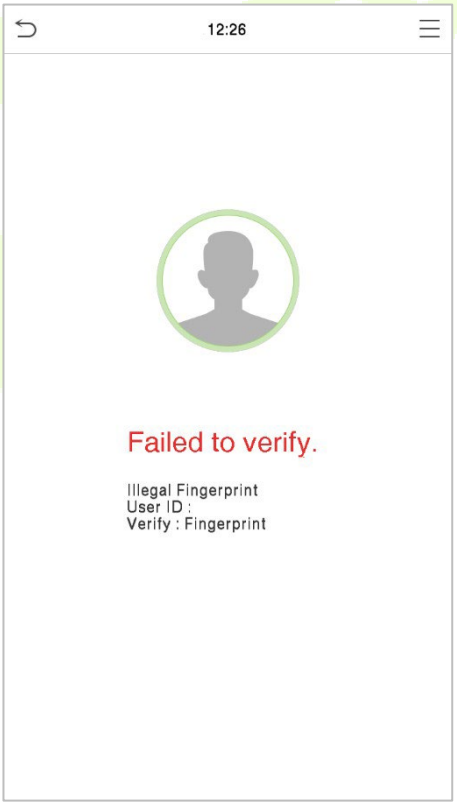
- **Modo de autenticação de impressão digital 1: N**

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

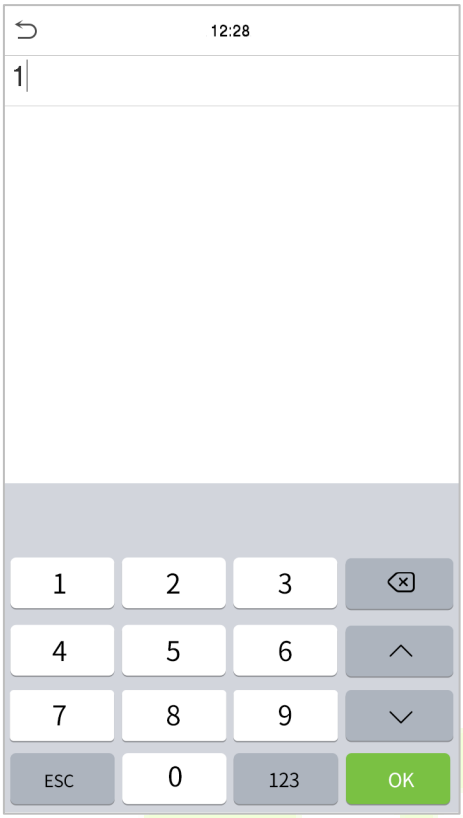


- **Modo de autenticação de impressão digital 1:1**

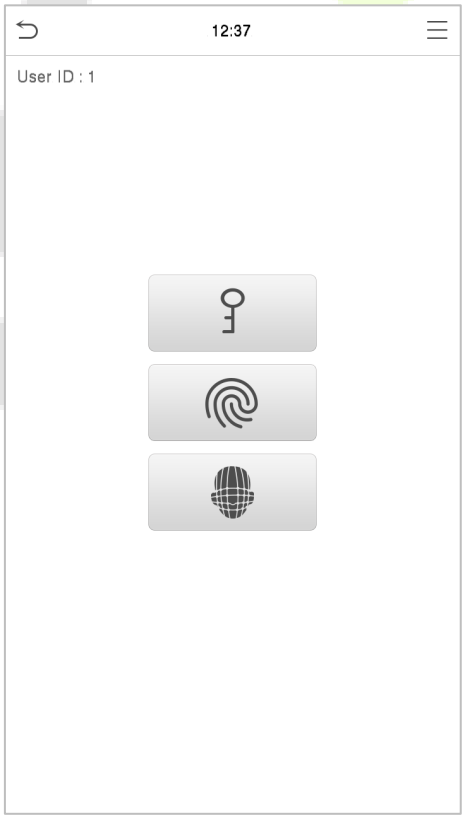
Compara a impressão digital que está sendo pressionada no leitor de impressão digital com as impressões digitais vinculadas à entrada do ID do usuário por meio do teclado virtual.
Os usuários podem verificar suas identidades no modo de verificação 1:1 quando não conseguem ter acesso com o método de autenticação 1: N.

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

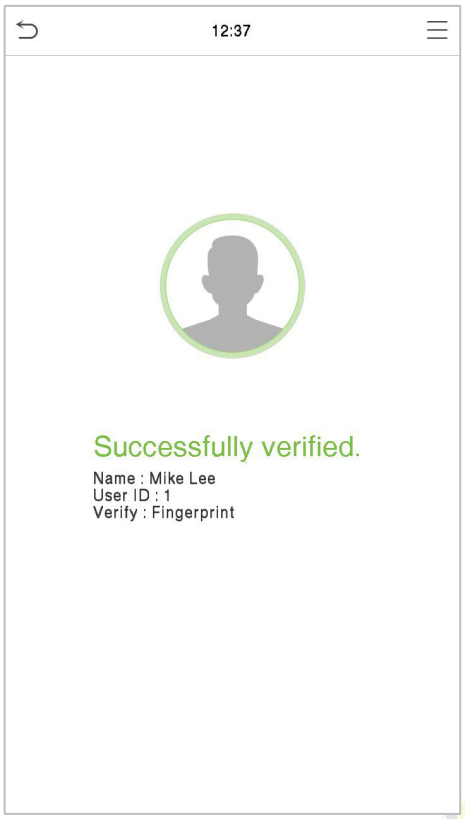
Digite o ID do usuário e clique em **[OK].**



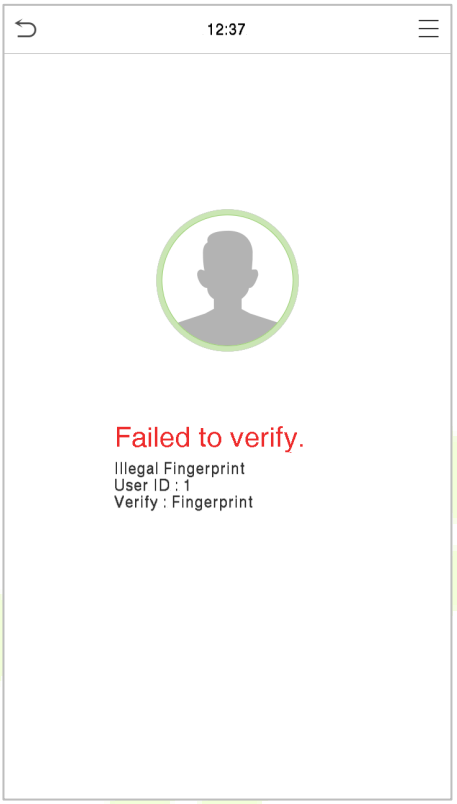
Se o usuário tiver registrado o rosto e a senha, além das impressões digitais, e o método de verificação estiver definido como verificação de senha/impressão digital/rosto, a seguinte tela aparecerá. Selecione o ícone de impressão digital para entrar no modo de verificação de impressão digital.



Pressione a impressão digital para verificar.



Autenticação bem-sucedida

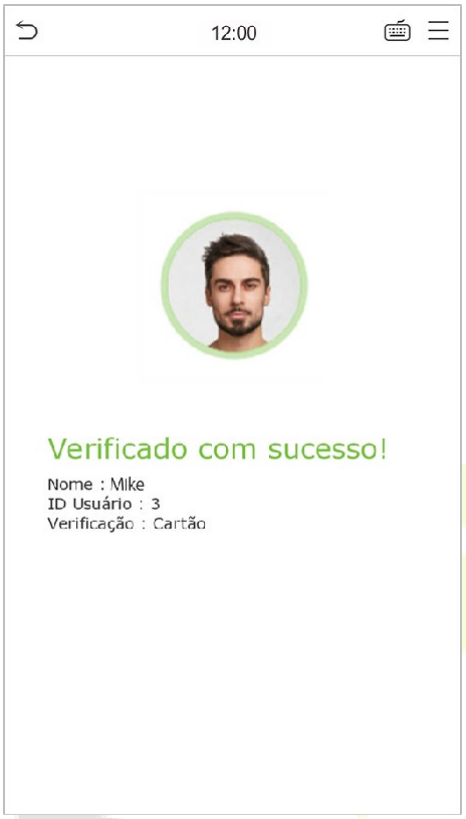


Autenticação falhou

2.6.2 Autenticação de cartão

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

O modo de autenticação de 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.

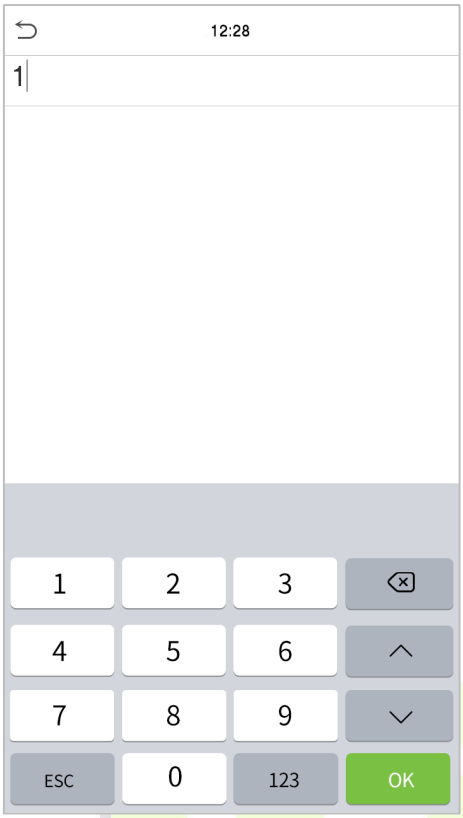


- **1:1 Modo de autenticação de cartão 1:1**

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

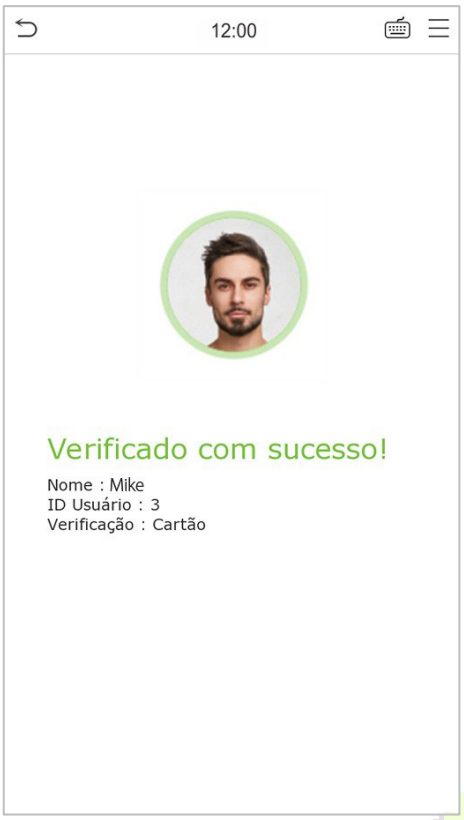
Selecione na tela principal para abrir o modo de autentificação de cartão 1:1.

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

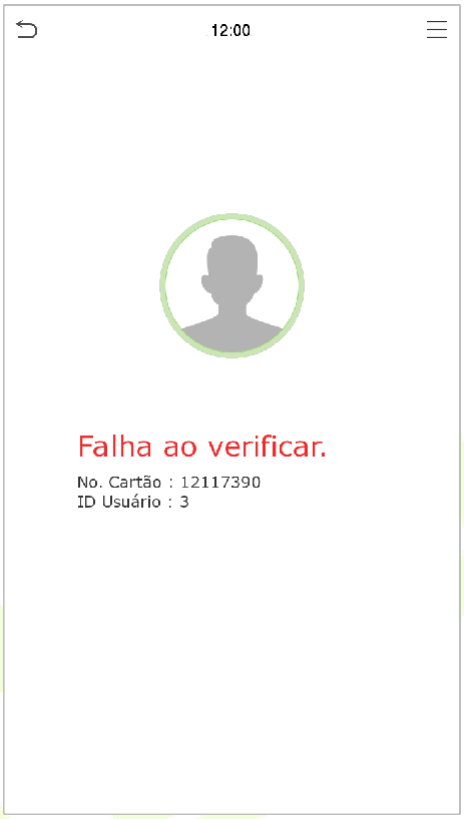


Se um funcionário registrar uma impressão digital além do cartão, a seguinte tela aparecerá. Selecione o ícone para entrar no modo de verificação do cartão.

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



Autenticação bem-sucedida



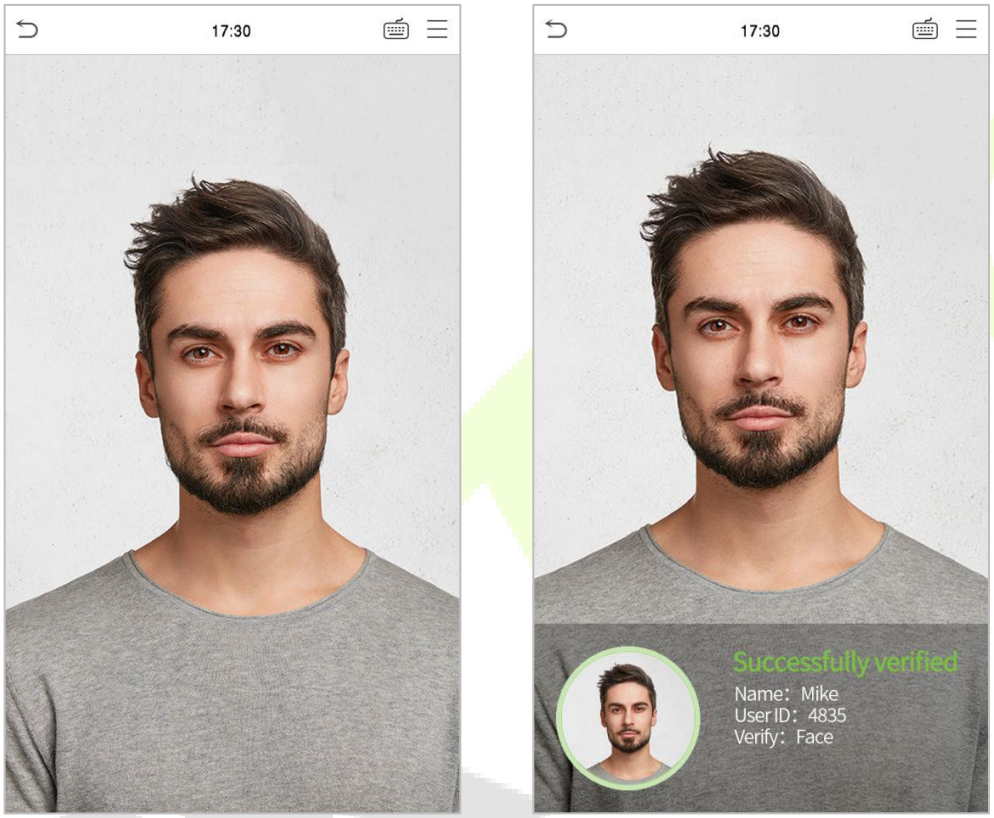
Autenticação falhou

2.6.3 Autenticação facial

- **Modo de autenticação facial 1:N**

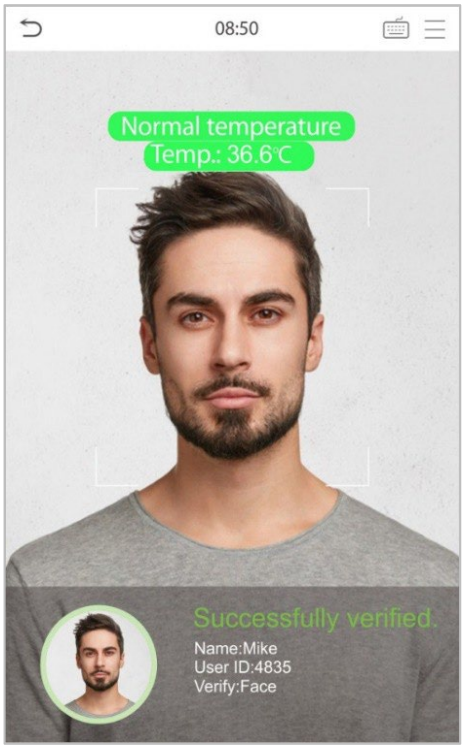
Verificação convencional

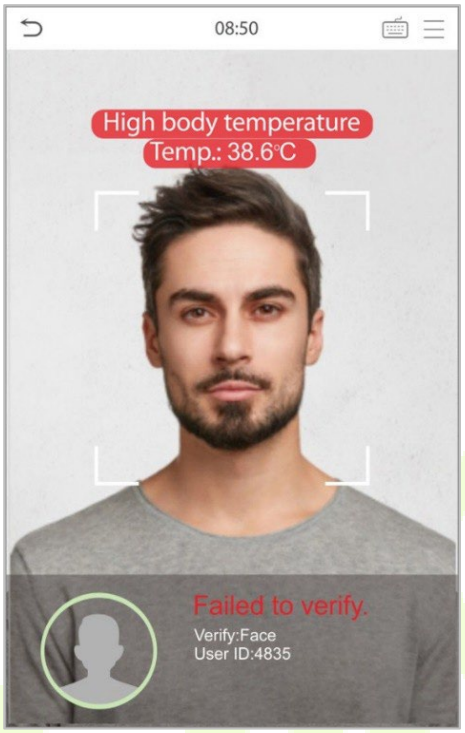
Neste modo de verificação, o dispositivo compara as imagens faciais coletadas com todos os dados faciais registrados no dispositivo. A seguir está o prompt pop-up de um resultado de comparação bem-sucedido.



Ative a triagem de temperatura com infravermelho.

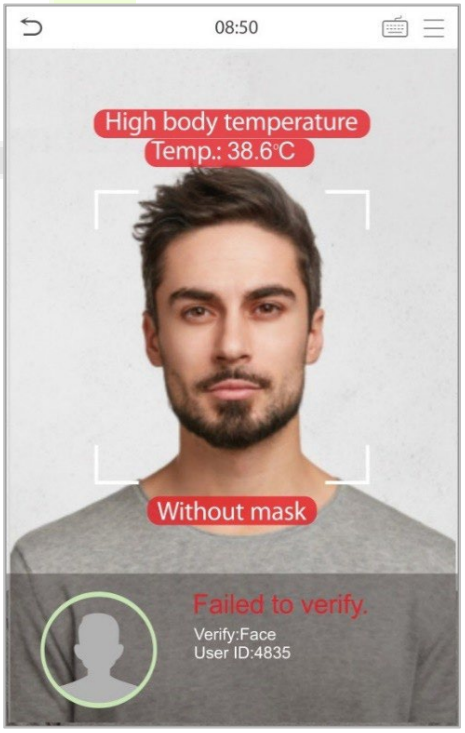
Quando o usuário habilita a **função de triagem de temperatura com infravermelho**, durante a verificação do usuário, além do método de verificação convencional, o rosto do usuário deve estar alinhado com a área de medição de temperatura para medir a temperatura corporal antes que a verificação possa ser realizada. A seguir estão os pop-ups da interface de prompt de resultado de comparação. (Observação: essa função é aplicável apenas a produtos com módulo de medição de temperatura.)





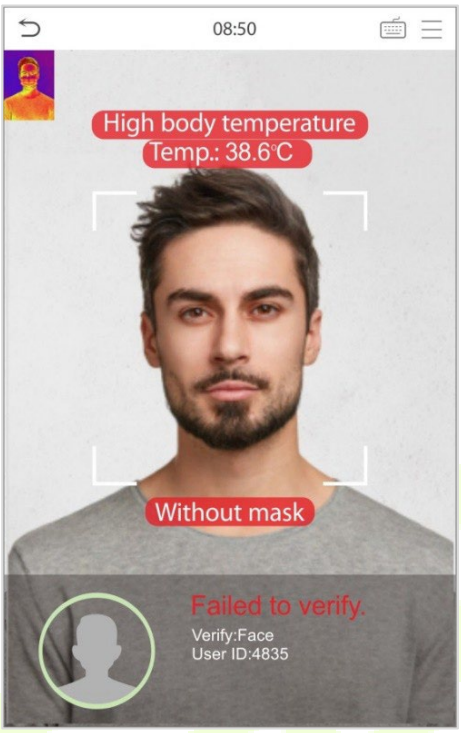
Ative a detecção de máscara

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 os pop-ups da interface de resultado de autenicação. (Observação: essa função é aplicável apenas a produtos com módulo de medição de temperatura.)



Exibir figura termodinâmica

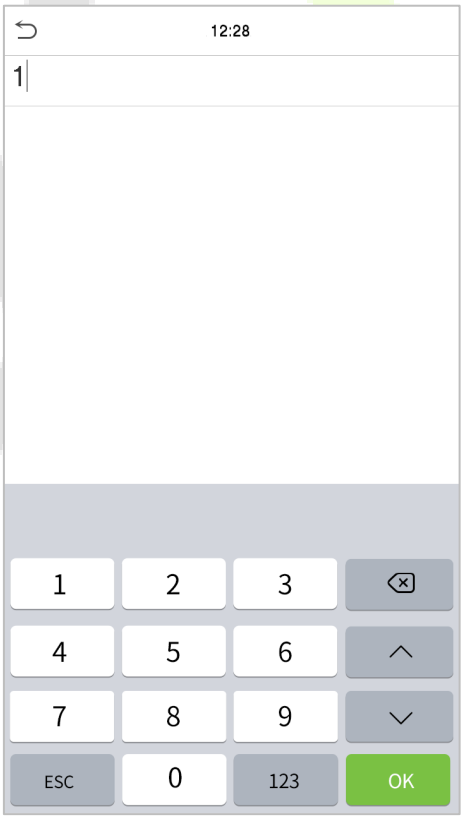
Quando o usuário habilita a função de **exibição da figura termodinâmica**, a imagem térmica da pessoa é exibida no canto superior esquerdo do dispositivo durante a verificação. Como mostrado nas imagens abaixo:



- **Modo de autenticação facial 1:1**

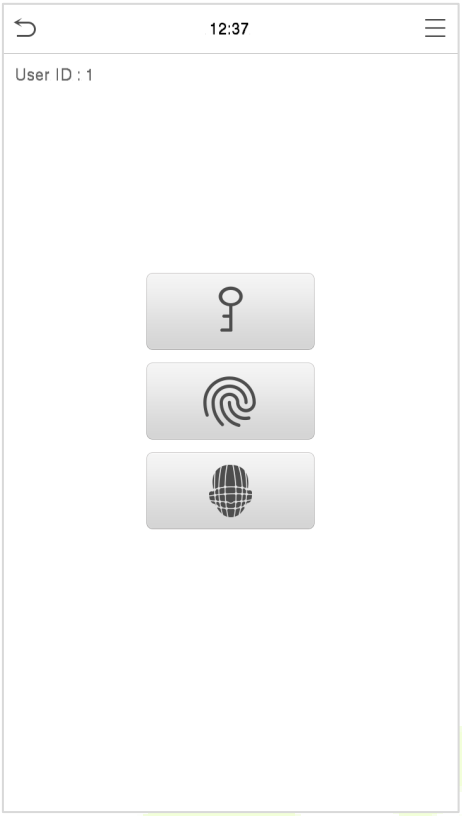
Compare a face capturada pela câmera com o template facial relacionado ao ID do usuário inserido. Pressione na interface principal e entre no modo de verificação facial 1:1.

Digite o ID do usuário e clique em OK.



Se um funcionário registrar uma impressão digital e uma senha, além do rosto, a seguinte tela aparecerá.

Selecione para entrar no modo de verificação facial.



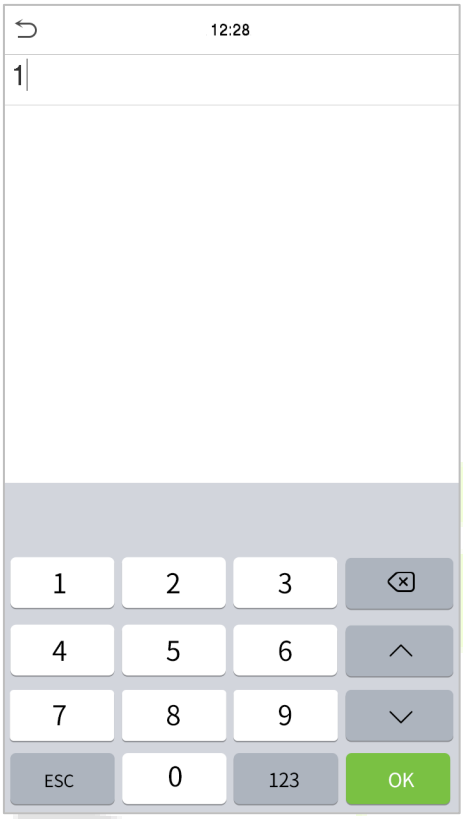
Após a verificação bem-sucedida, será exibida a mensagem "**Verificado com sucesso**", conforme mostrado abaixo:

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

2.6.4 Verificação de senha

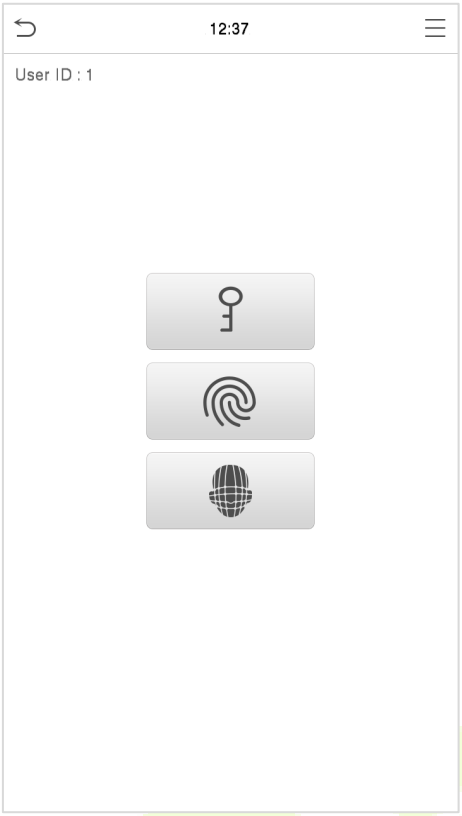
O dispositivo compara a senha inserida com a senha registrada do ID do usuário fornecido.

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.

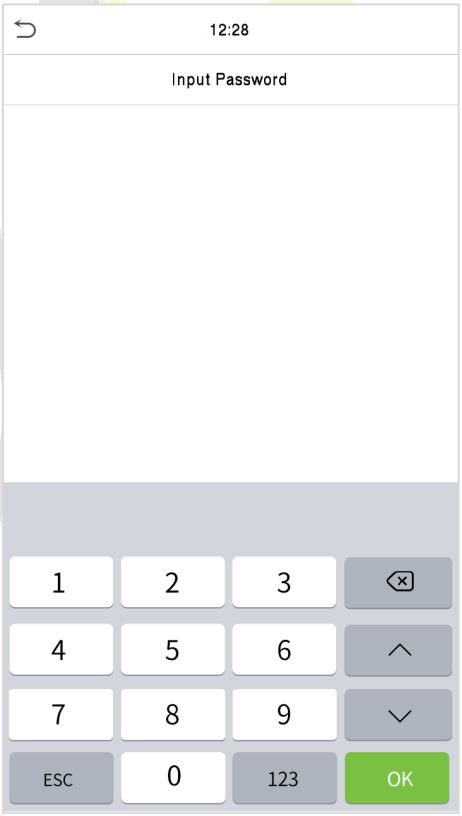


Se um funcionário registrar a impressão digital e o rosto, além da senha, a seguinte tela aparecerá.

Selecione para entrar no modo de verificação de senha

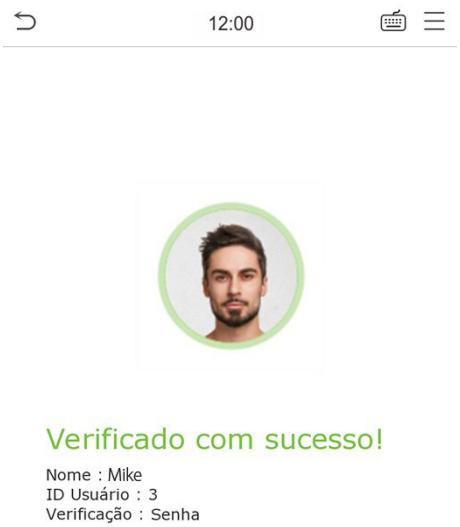


Digite a senha e pressione **OK**.

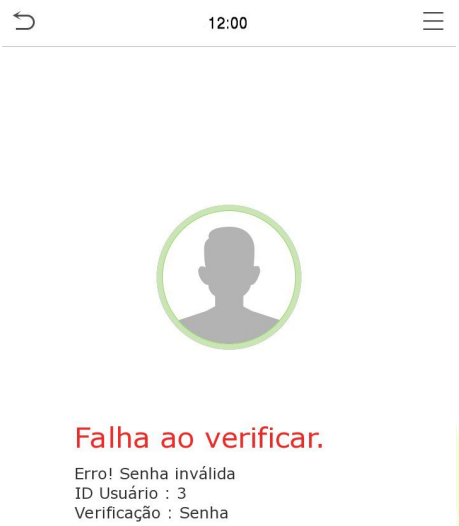


Aqui estão as telas de exibição após inserir uma senha correta e uma senha incorreta, respectivamente:

A autenticação foi bem-sucedida:

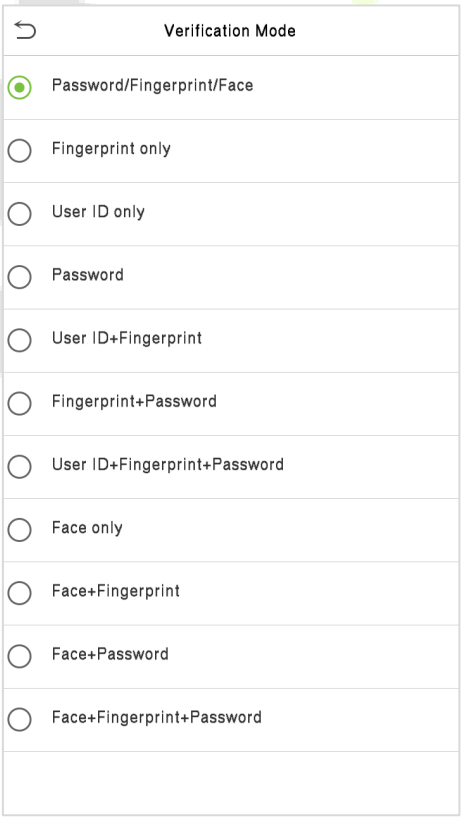


A autenticação falhou:



2.6.5 Verificação combinada

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



Procedimento para configurar o modo de verificação combinada.

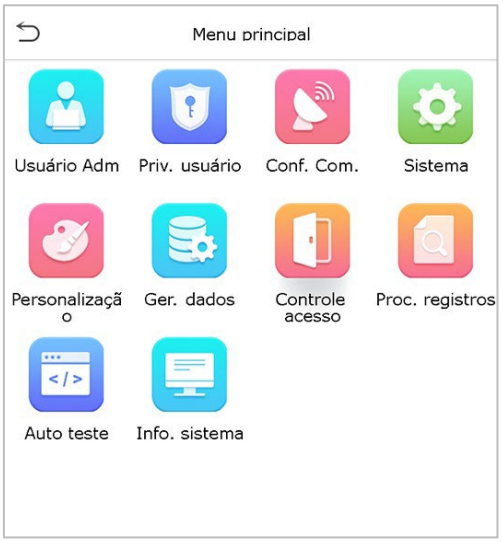
- A verificação combinada requer que os funcionários registrem todos os métodos de verificação diferentes. Caso contrário, os funcionários podem não conseguir verificar com sucesso por meio do processo de verificação combinada.
- Por exemplo, quando um funcionário registra apenas os dados faciais, mas o modo de verificação do dispositivo está configurado como "Rosto + Senha", o funcionário não conseguirá concluir com sucesso o processo de verificação.
- Isso ocorre porque o dispositivo compara o modelo facial escaneado da pessoa com o modelo de verificação registrado (tanto o rosto quanto a senha) armazenado anteriormente naquele ID de pessoal no dispositivo. No entanto, como o funcionário registrou apenas o rosto e não a senha, a verificação não será concluída e o dispositivo exibirá "Verificação falhou".

Observação:

- "**/**" significa "**ou**" e "**+**" significa "**e**".
- Você deve registrar as informações de verificação necessárias antes de usar o modo de autenticação combinada, caso contrário, a verificação poderá falhar. Por exemplo, se um usuário usa o Registro Facial, mas o modo de verificação é Rosto + Senha, esse usuário nunca passará na verificação.

3 Menu Principal

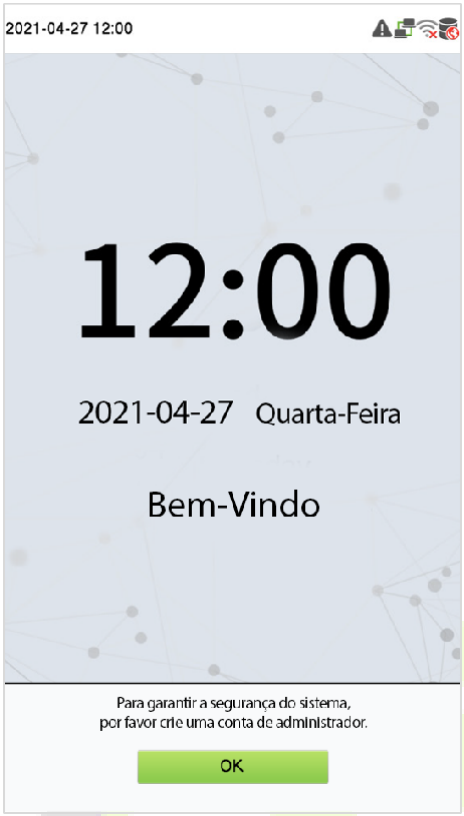
Selecione na tela de espera para entrar no menu principal, a seguinte tela será exibida:



Menu	Descrição
Usuário Adm.	Para adicionar, editar, visualizar e excluir informações básicas de um usuário
Priv. Usuário	Para definir o escopo de permissão da função personalizada e de cadastrador para os usuários, ou seja, os direitos para utilizar o sistema.
Conf. Com.	Para definir os parâmetros de rede, comunicação serial, conexão de PC, rede sem fio, servidor de nuvem, Wiegand e diagnóstico de rede.
Sistema	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.
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 superadministrador.

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



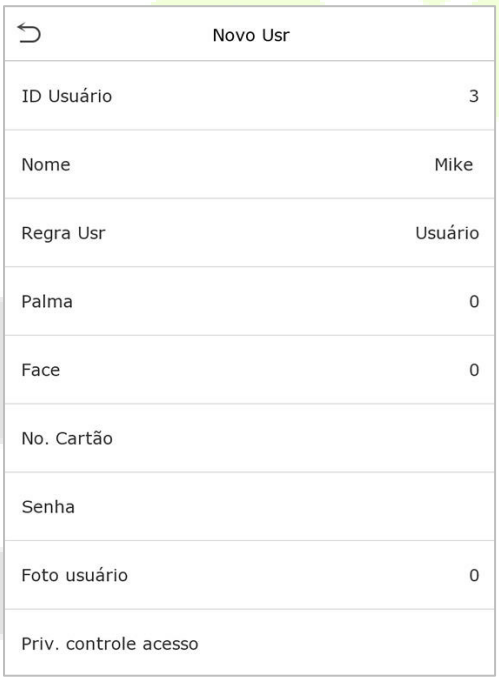
4 Gestão de Usuários

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.



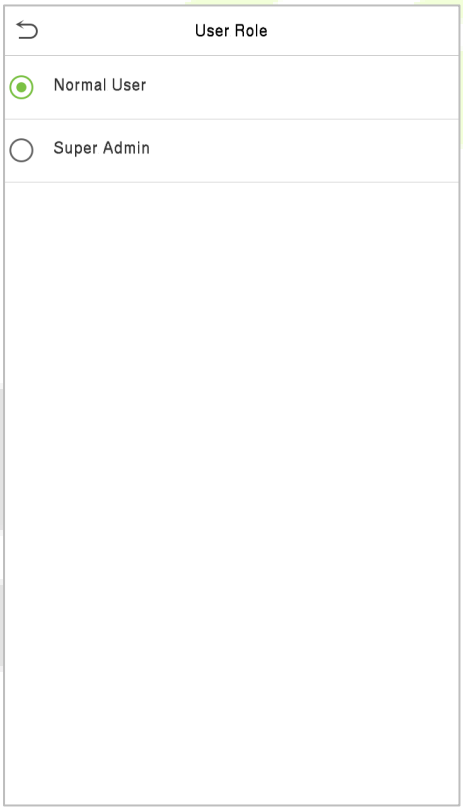
Observação:

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

3.1.2 Privilégio do usuário

Existem dois tipos de contas de usuário: **usuário normal** e **superadministrador**. Caso já exista um administrador cadastrado, os usuários normais não possuem direitos de gerenciamento do sistema, podendo apenas acessar verificações de 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.

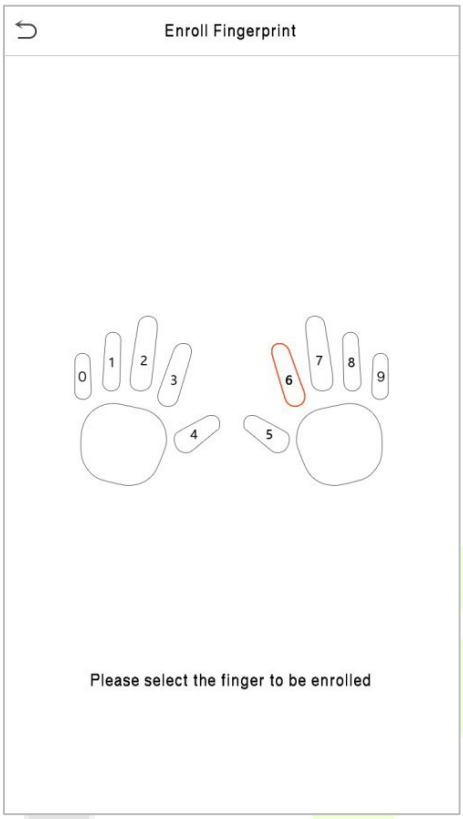
Toque em **Priv. Usuário** para definir a função do usuário como Usuário Normal ou Super Admin.



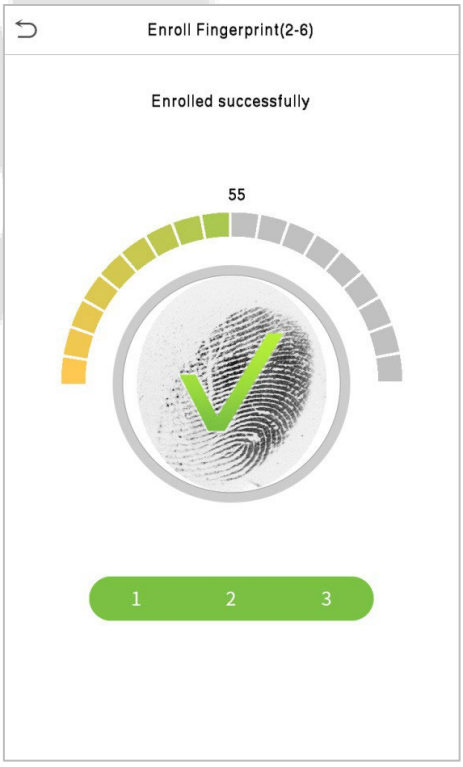
Observação: Se a função de usuário selecionada for o Super Admin, o usuário deverá fazer a autenticação para acessar o menu principal. A autenticação é baseada no(s) método(s) de autenticação que o super administrador cadastrou. Por favor, consulte "Modos de Autenticação".

4.1.3 Registrar Impressão Digital

Clique em **Impressão Digital** para acessar a página de registro 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 Registrar Face

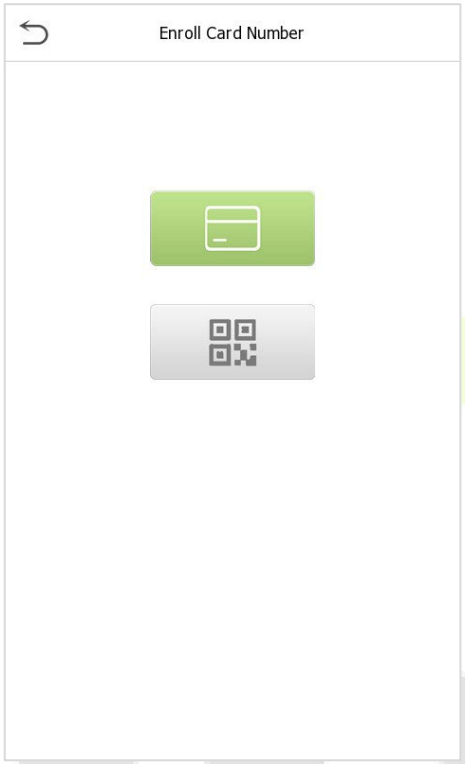
Clique em "**Face**" para acessar a página de registro facial. Por favor, posicione-se em frente à câmera e mantenha-se imóvel durante o registro facial. A interface de registro é a seguinte:

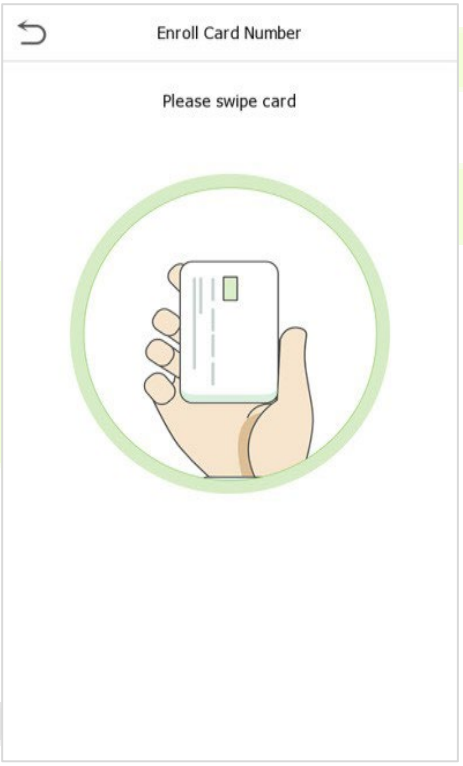
4.1.5 Registrar Número do Cartão

- **Registrar Cartão**

Toque em **Cartão** na interface 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 bem-sucedido.
- Se o cartão já estiver registrado, a mensagem "Cartão Duplicado" aparecerá.
- A interface de registro é a seguinte:

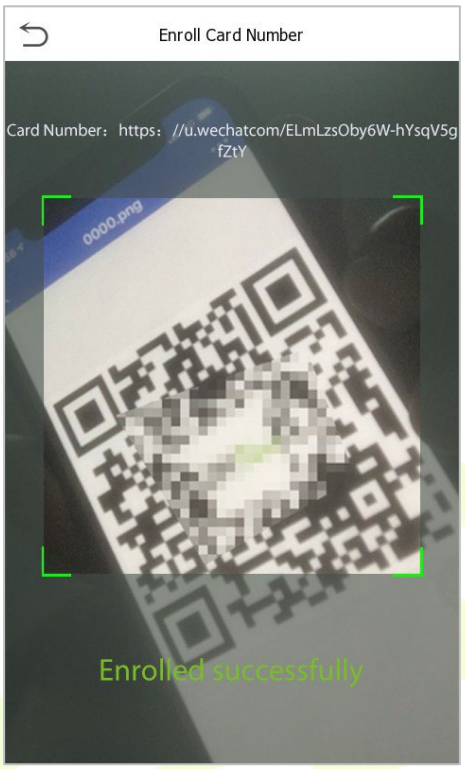




- **Cadastrar QR Code do Cartão**

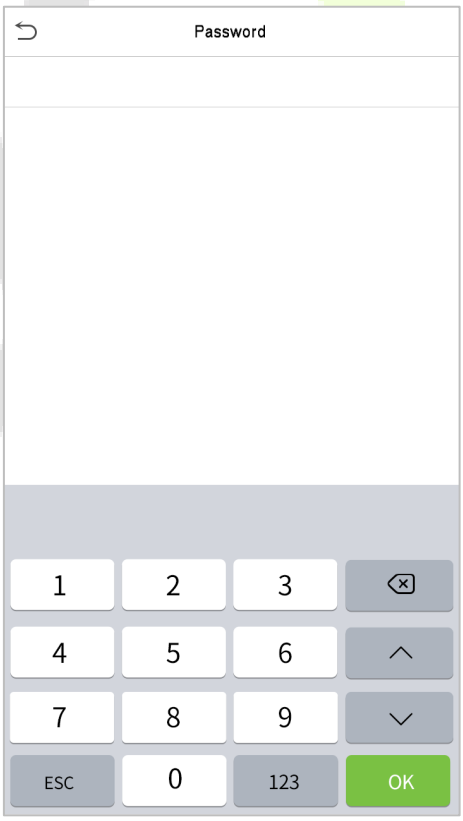
Toque em **Cartão** na interface de **Novo Usuário** para acessar a página de registro do cartão.

- Na interface do Cartão, mostre o QR Code em frente à câmera. O registro do QR Code será bem-sucedido.
- Se o QR Code já estiver registrado, a mensagem "Erro! Cartão já cadastrado" será exibida. A interface de registro é a seguinte:



4.1.6 Registrar Senha

Toque em **Senha** para acessar a página de registro 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 Registrar Foto do Usuário

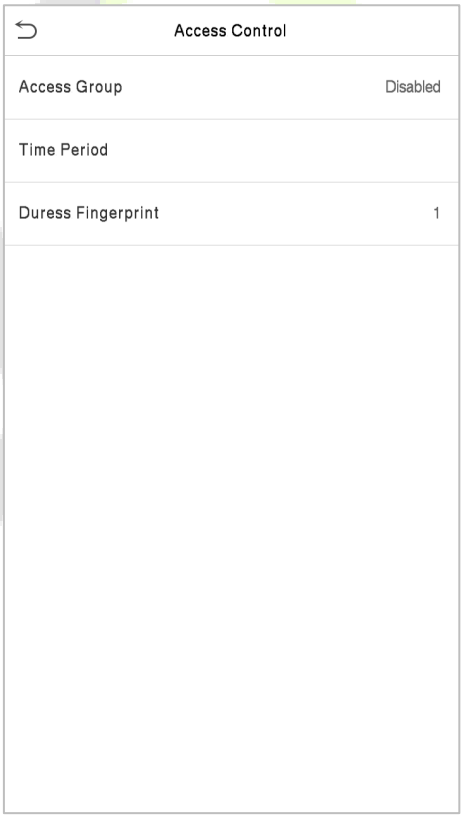
Quando um usuário registrado com uma foto passa pela autenticação, a foto registrada será exibida.
Clique em **Foto do Usuário**, clique no ícone da câmera para tirar uma foto. O sistema retornará à interface de **Novo Usuário** após tirar a foto.
Observação: Ao registrar um rosto, o sistema capturará automaticamente uma imagem como foto do usuário. Se você não deseja registrar uma foto do usuário, o sistema definirá automaticamente a imagem capturada como foto padrão.

4.1.8 Função 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 período de tempo ao qual o usuário pertence.

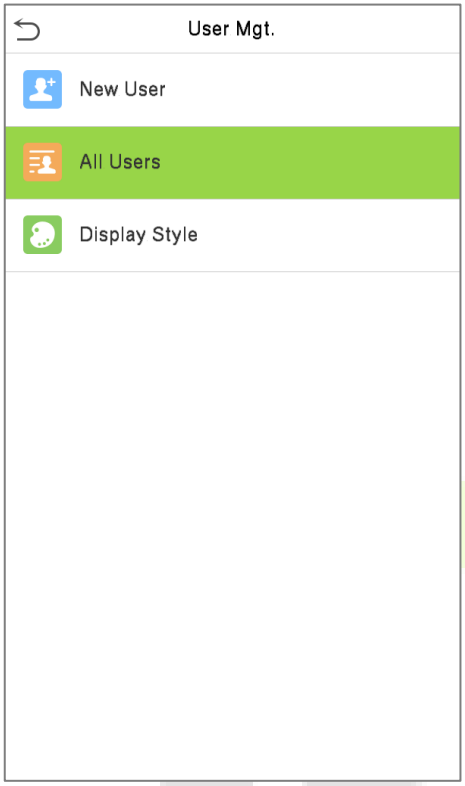
Clique em **Função de controle de Acesso** > **Grupo de Acesso**, atribua os usuários registrados a diferentes grupos para uma melhor gestão. Os novos usuários pertencem ao Grupo 1 por padrão e podem ser realocados para outros grupos. O dispositivo suporta até 99 grupos de controle de acesso.

Clique em **Período de Tempo**, selecione o período de tempo a ser utilizado.



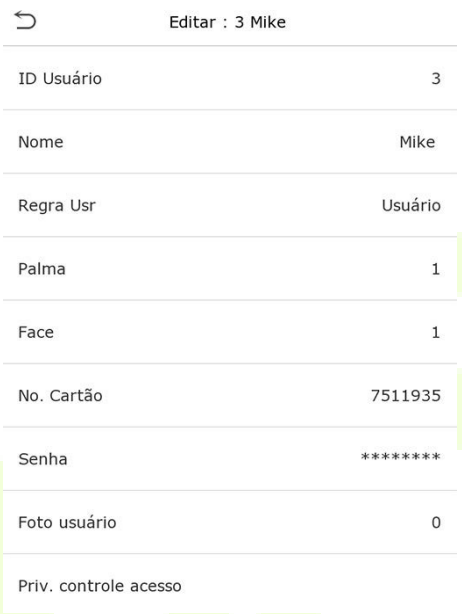
4.2 Procura de Usuários

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



4.3 Editar Usuário

Na interface **Todos os Usuários**, toque no usuário necessário 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 um usuário. Para o processo detalhado, veja "Registro de Usuário".

4.4 Excluir Usuário

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

- **Operações de Exclusão**

Excluir Usuário: Exclui todas as informações do usuário (exclui o usuário selecionado como um todo) do dispositivo.

Excluir Apenas Face: Exclui as informações faciais do usuário selecionado.

Excluir Apenas Senha: Exclui as informações de senha do usuário selecionado.

Excluir Apenas Impressão Digital: Exclui as informações de impressão digital do usuário selecionado.

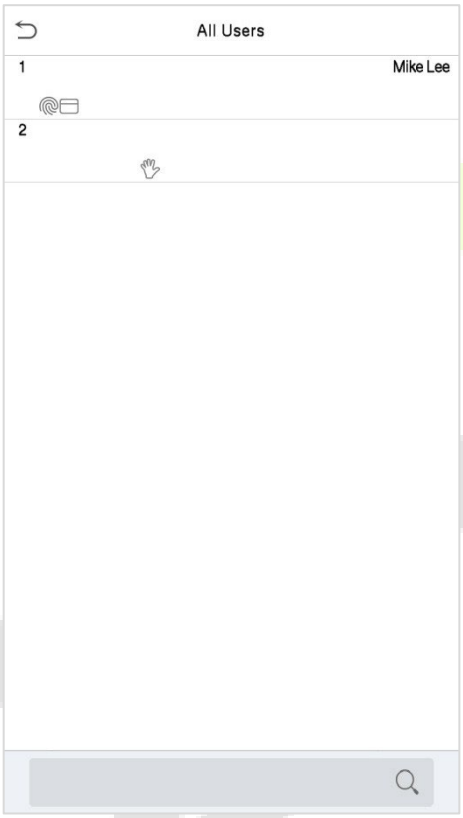
Observação: Se você selecionar Excluir Usuário, todas as informações do usuário serão excluídas.

4.5 Estilo de Display

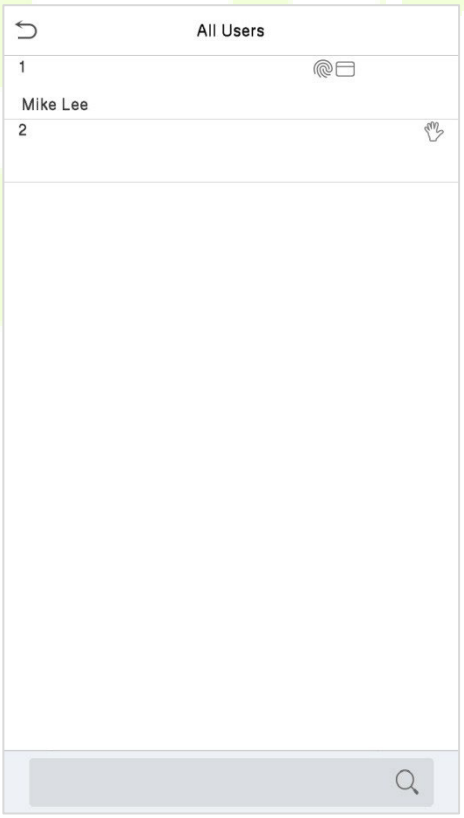
No menu principal, clique em **Usuário Adm.** e, em seguida, clique em **Estilo de exibição** para entrar na interface de **configuração do Estilo de exibição**.

Todos os estilos de exibição são mostrados como abaixo:

Múltiplas Linhas



Linha Mista



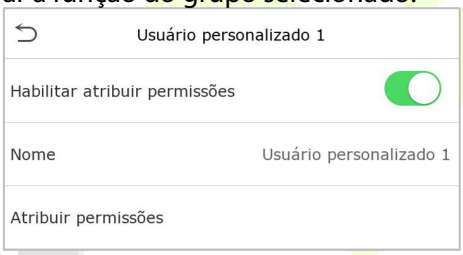
5 Privilégio do Usuário

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

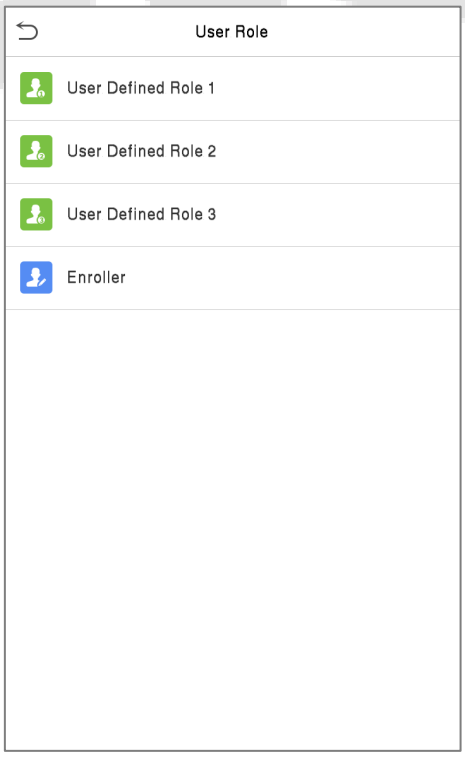
You may set the permission scope of the custom role (up to 3 roles) and enroller, that is, the permission scope of the operation menu.

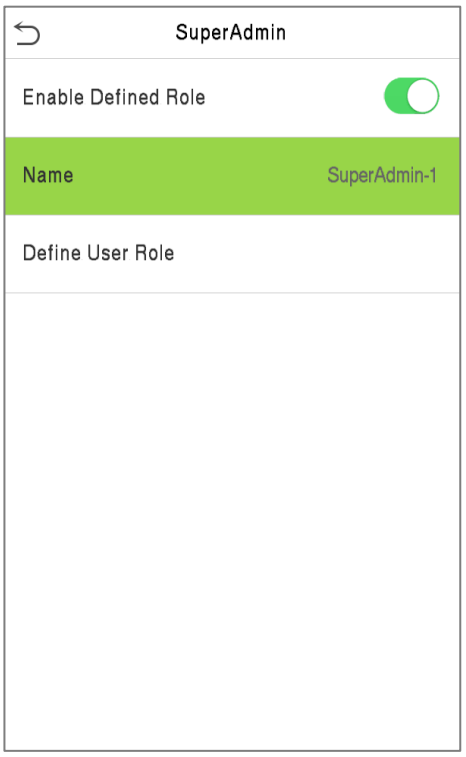
Clique em **Priv. Usuário** na interface do menu principal.

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.

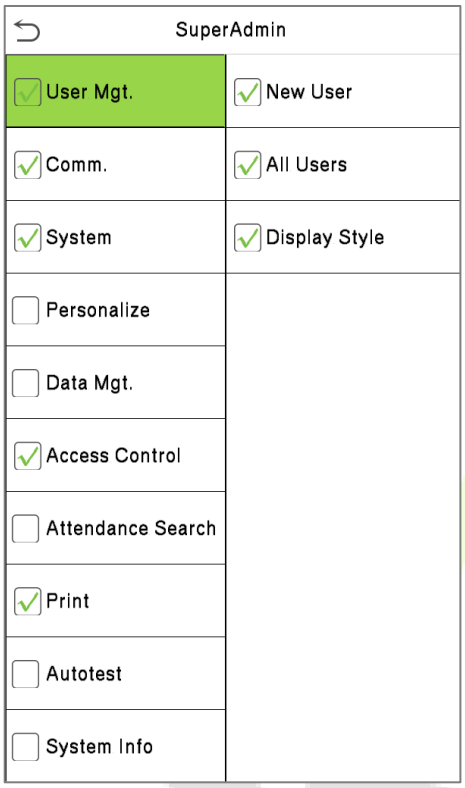


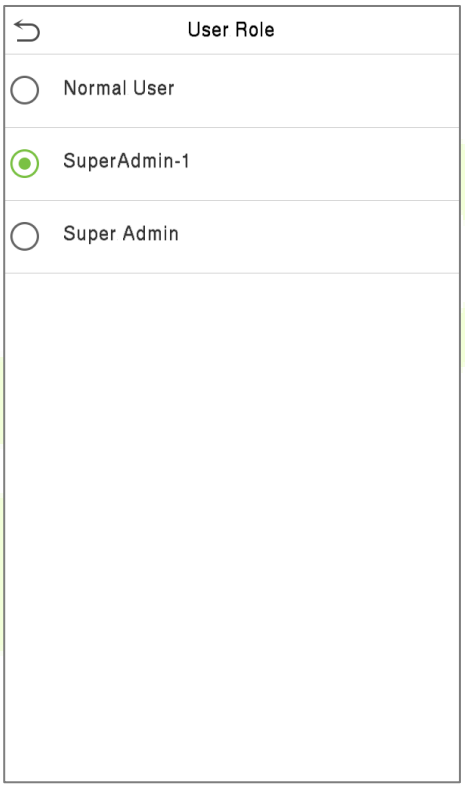


Em seguida, toque em **Definir Função do Usuário** e selecione os privilégios necessários para atribuir ao novo papel e, em seguida, toque no botão **Retornar**.

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

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

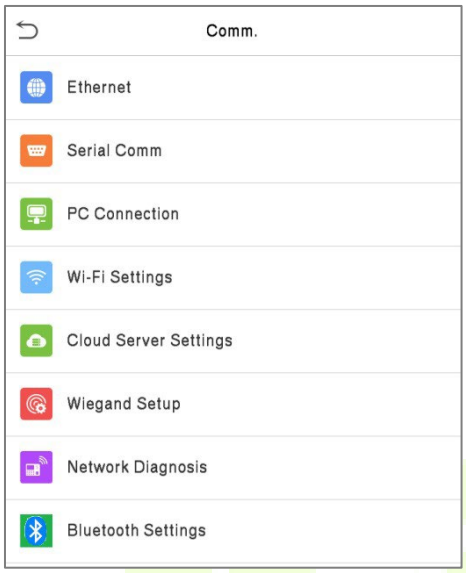




Observação: Se a Função do Usuário estiver habilitada no dispositivo, toque em **Gerenciamento de Usuários** > **Novo Usuário** > **Função do** Usuário para atribuir os papéis criados aos usuários necessários. No entanto, se não houver um superadministrador registrado no dispositivo, o dispositivo exibirá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

6 Configurações de Comunicação

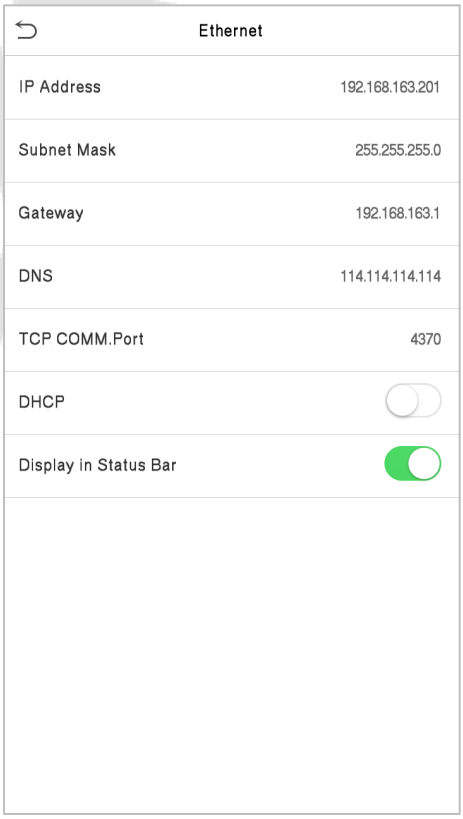
As **configurações de comunicação** são utilizadas para definir os parâmetros de rede, comunicação serial, conexão de PC, rede sem fio, servidor de nuvem, Wiegand e diagnóstico de rede.
Toque em Conf. Com. no Menu Principal.



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.

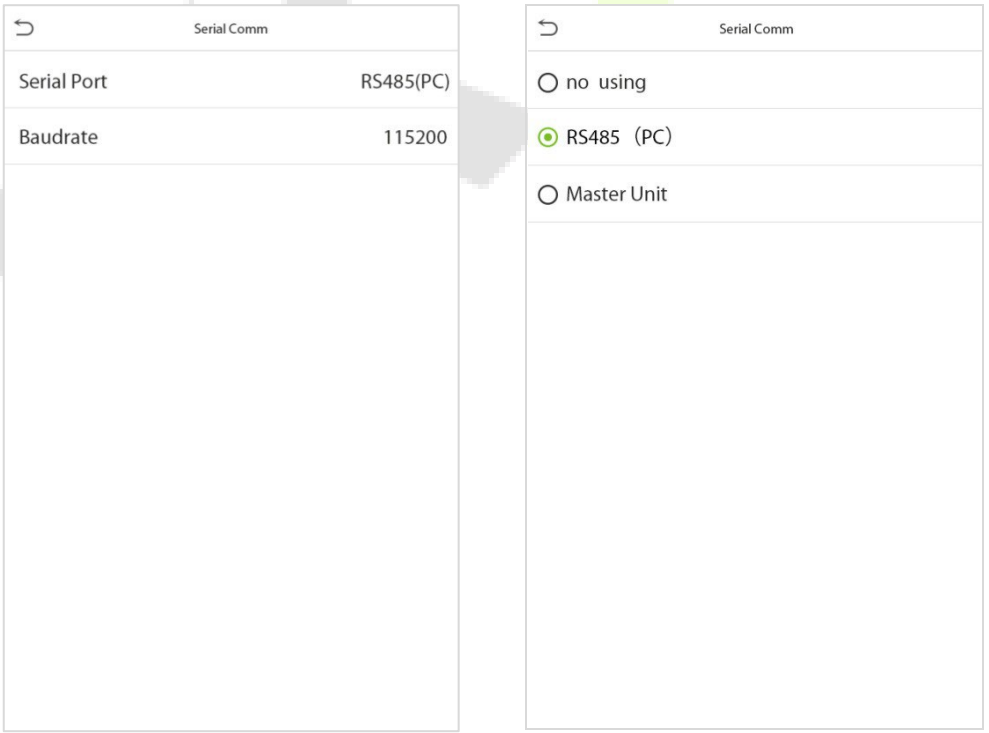


Função	Descrição
TCP/IP	O valor de fábrica é 192.168.1.201 e pode ser editado.
Máscara de Rede	O valor de fábrica é 255.255.255.0 e pode ser editado.
Gateway	O valor de fábrica é 0.0.0.0 e pode ser editado.
DNS	O valor de fábrica é 0.0.0.0 e pode ser editado.
Porta de Com. TCP	O valor predefinido na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

6.2 Comunicação Serial★

A função Serial Comm facilita o estabelecimento de comunicação com um dispositivo através de uma porta serial (/RS485/ Unidade Mestre).

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

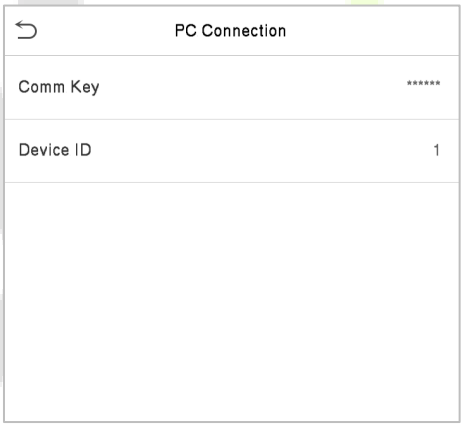


Função	Descrição
Porta Serial	**Desativar:** Não se comunicar com o dispositivo através da porta serial. **RS485(PC):** Comunica-se com o dispositivo através da porta serial RS485. **Unidade Mestre:** Quando o RS485 é usado como função de "Unidade Mestre", o dispositivo atuará como uma unidade mestre e poderá ser conectado a um leitor de impressões digitais e cartões RS485.
Taxa de Transmissão	A taxa na qual os dados são comunicados com o PC 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 seria mais confiável.

6.3 Conexão com o PC

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

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



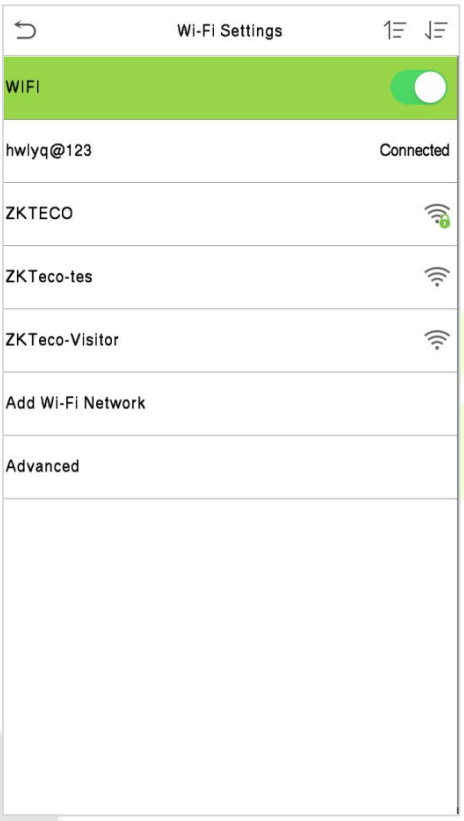
Função	Descrição
Senha de Comunicação	A senha padrão é 0, que pode ser alterada. A senha de comunicação pode conter de 1 a 6 dígitos.
ID do aparelho	Número de identificação do dispositivo na rede serial, que varia entre 1 e 254. Se o método de comunicação for RS232/RS485, você precisa inserir este ID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

6.4 Rede sem fio (Wi-Fi)

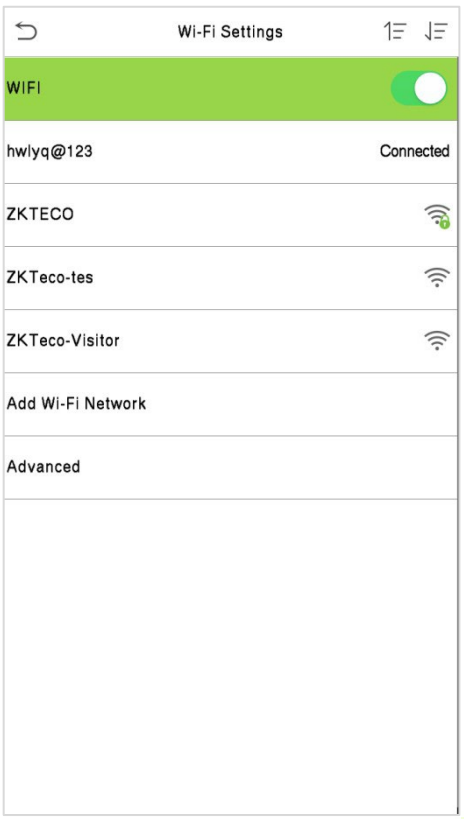
O dispositivo possui um módulo Wi-Fi, que pode ser incorporado ao molde do dispositivo ou conectado externamente.

O módulo Wi-Fi permite a transmissão de dados por meio de Wi-Fi (Wireless Fidelity) e estabelece um ambiente de 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 desativação do Wi-Fi.

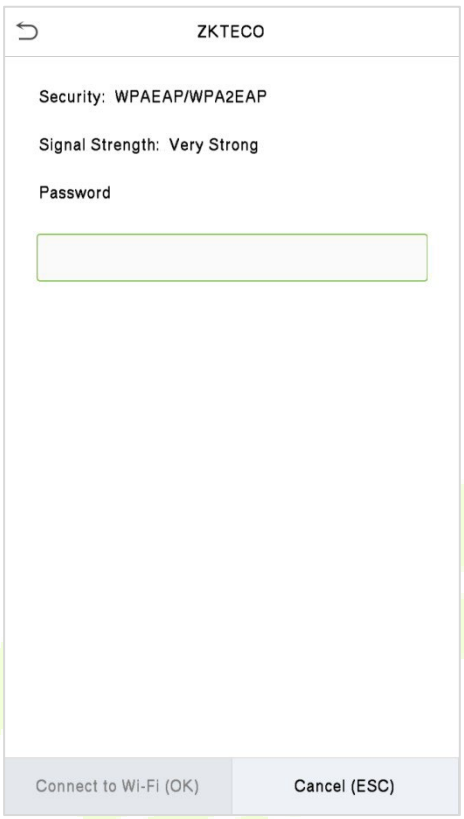
Toque em **Wi-Fi** na interface de **Configurações de Comunicação** para configurar a conexão Wi-Fi.



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 no nome apropriado da rede Wi-Fi na lista disponível e insira a senha correta na interface de senha e, em seguida, toque em **Conectar ao Wi-Fi (OK)**.



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

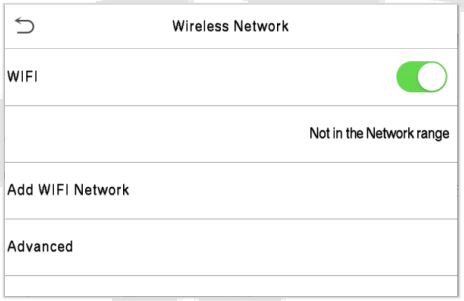


Toque no campo de senha para inserir a senha e, em seguida, toque em **Conectar ao Wi-Fi (OK).**

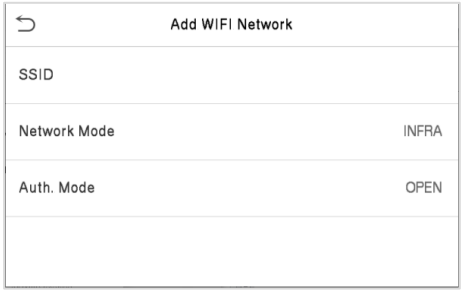
Quando o Wi-Fi for conectado com sucesso, a interface inicial exibirá o logotipo do Wi-Fi.

- **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.**

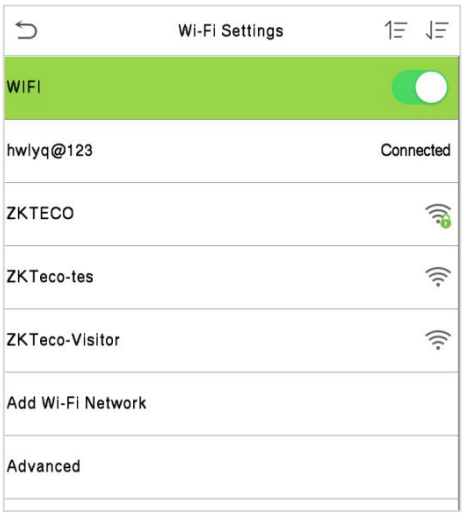


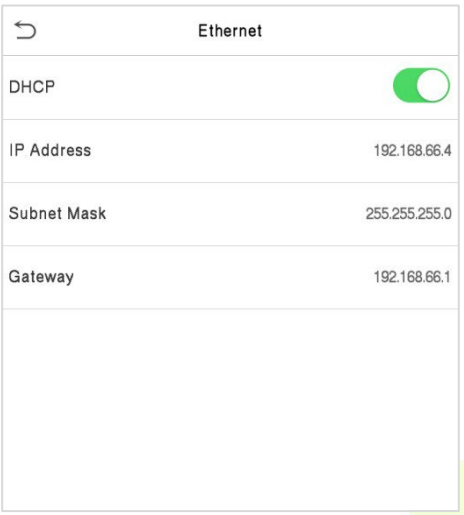
Nesta interface, insira os parâmetros da rede Wi-Fi. (A rede adicionada deve existir.)

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.

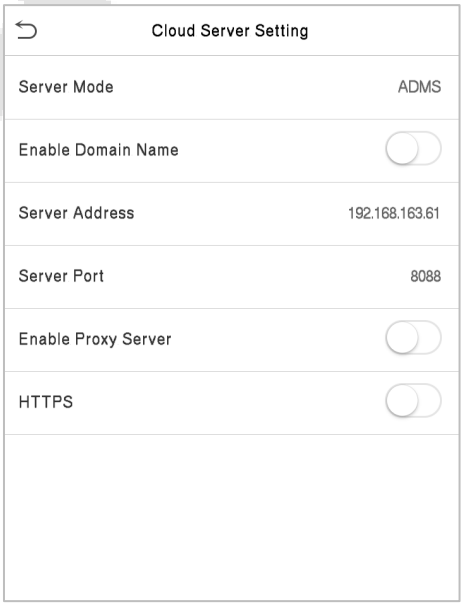




Função	Descrição
DHCP	O protocolo de configuração dinâmica de host (DHCP) aloca dinamicamente endereços IP para clientes de rede. Se o DHCP estiver ativado, o IP não poderá ser definido manualmente.
IP Address	Endereço IP para a rede WIFI, o padrão é 192.168.1.201 (0.0.0.0 caso o DHCP esteja ativado). 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.

6.5 Configuração do Servidor em Nuvem

Isso representa as configurações usadas para conectar o servidor ADMS.
Clique **Configurar servidor de nuvem** na interface de **Configurações de Comunicação**.



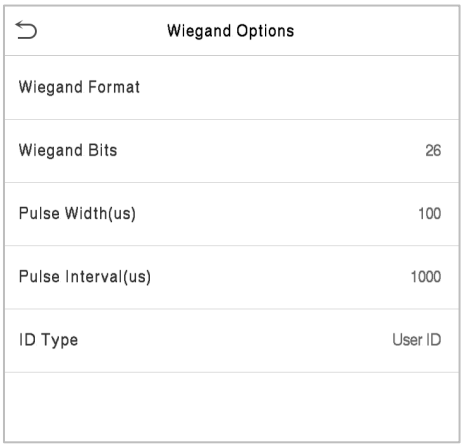
Menu		Descrição
Ativar nome de domínio	**Endereço do servidor**	Uma vez habilitada esta função, será utilizado o modo de nome de domínio "http://..." como http:www.XYZ.com, enquanto "XYZ" será o nome de domínio (quando este modo está LIGADO)
Desativar nome de domínio	**Endereço do servidor**	O endereço IP do servidor ADMS.
	Porta do servidor	Porta usada pelo servidor ADMS.
Ativar servidor proxy		Ao optar por habilitar o proxy, você precisa definir o endereço IP e o número da porta do servidor proxy
HTTPS		Para aumentar a segurança do acesso do navegador, os usuários podem ativar o protocolo HTTPS para criar uma transmissão de rede segura e criptografada e garantir a segurança dos dados enviados por meio de autenticação de identidade e comunicação criptografada. Esta função está habilitada por padrão. Esta função pode ser ativada ou desativada através da interface do menu e, ao alterar o status do HTTPS, o dispositivo exibirá um prompt de segurança e reiniciará após a confirmação.

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



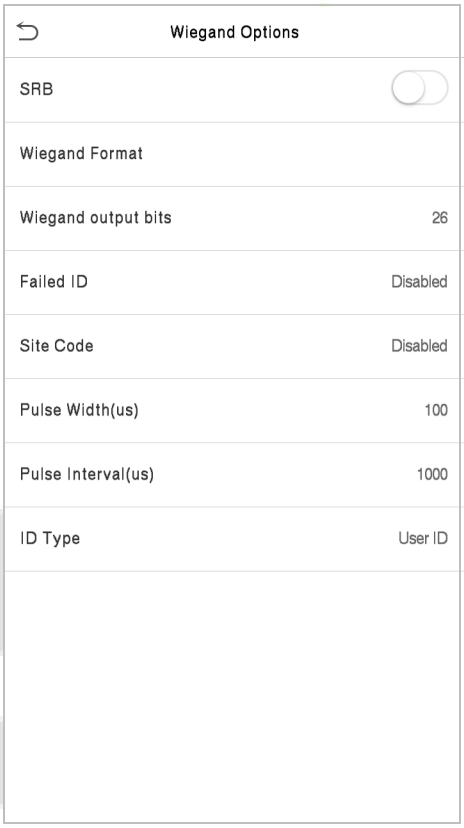
Função	Descrição
Formato Wiegand	Os valores variam de 26 bits, 34 bits, 36 bits, 37 bits e 50 bits.
Bits de saída Wiegand	Após selecionar o formato Wiegand necessário, selecione os dígitos de bit de saída correspondentes do formato Wiegand
Largura do pulso (us)	O valor da largura de pulso enviado pelo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

Descrição dos formatos mais comuns de Wiegand:

Formato Wiegand	Descrição
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCO Consiste em 26 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 13º bits, enquanto o 26º bit é o bit de paridade ímpar do 14º ao 25º bits. O 2º ao 25º bits são os números do cartão
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCO Consiste em 26 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 13º bits, enquanto o 26º bit é o bit de paridade ímpar do 14º ao 25º bits. Os 2º a 9º bits são os site code, enquanto os 10º a 25º bits são os números do cartão.
Wiegand34	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	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCE Consiste em 37 bits de código binário. O 1º bit é o bit de paridade ímpar do 2º ao 18º bits, enquanto o 37º bit é o bit de paridade par do 19º ao 36º bits. O 2º ao 4º bits são os códigos do fabricante. O 5º ao 16º bits são os site code e os 21º ao 36º bits são os números do cartão.

Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCO Consiste em 37 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 18º bits, enquanto o 37º bit é o bit de paridade ímpar do 19º ao 36º bits. O 2º ao 4º bits são os códigos do fabricante. O 5º ao 14º bits são os códigos do dispositivo, e o 15º ao 20º bits são os site code e os 21º ao 36º bits são os números do cartão.
Wiegand50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consiste em 50 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 25º bits, enquanto o 50º bit é o bit de paridade ímpar do 26º ao 49º bits. O 2º ao 17º bits são os site code e os 18º ao 49º bits são os números do cartão.
"C" Número do cartão; **"E"** Paridade par; **"O"** Paridade ímpar; **"F"** Facility code; **"M"** Código do fabricante; **"P"** Paridade; and **"S"** Site code.	

6.6.2 Saída Wiegand



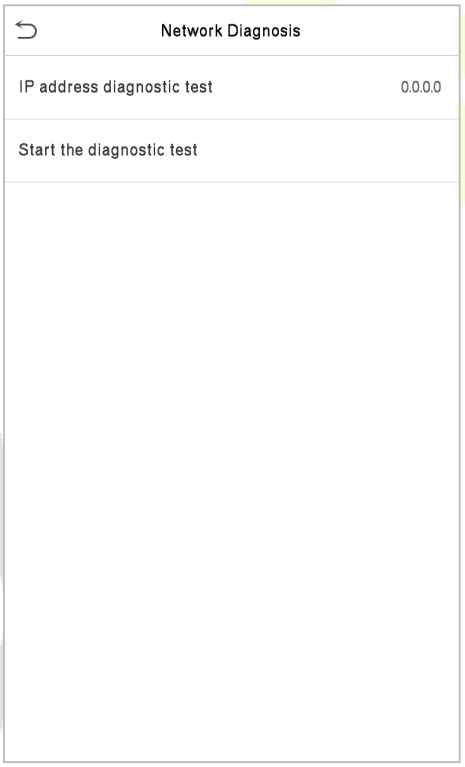
Função	Descrição
SRB	Quando o SRB está habilitado, a fechadura é acionada pelo SRB para evitar que a fechadura seja aberta com à remoção do dispositivo da parede
Formato Wiegand	Os valores variam de 26 bits, 34 bits, 36 bits, 37 bits e 50 bits.
Bits de saída Wiegand	Após selecionar o formato Wiegand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

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

6.7 Diagnóstico de Rede

Para configurar os parâmetros de diagnóstico de rede.

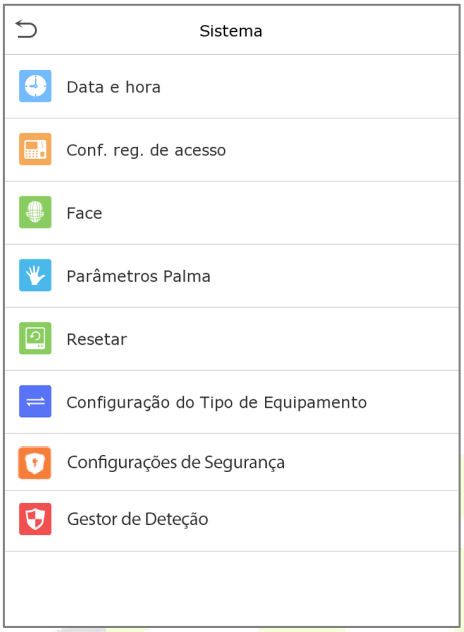
Clique em **Diagnóstico de Rede** na interface de Configurações de Comunicação. Insira o endereço IP que precisa ser diagnosticado e clique em **Iniciar teste de diagnóstico** para verificar se a rede pode se conectar ao dispositivo.



7 Configurações de Sistema

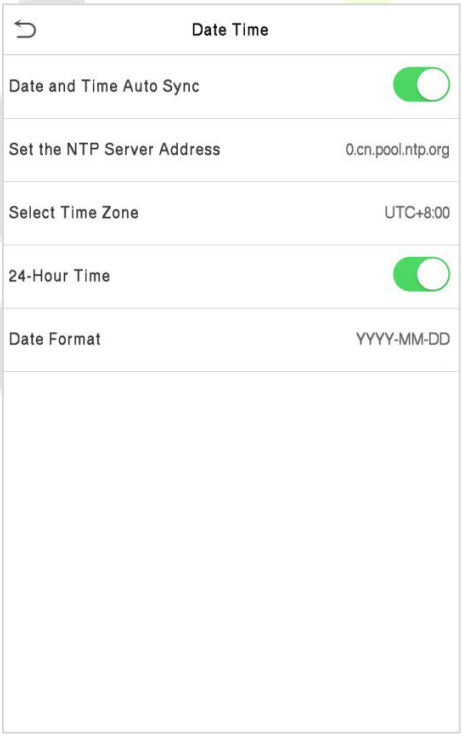
As configurações do sistema são usadas para definir os parâmetros do sistema relacionados para otimizar o desempenho do dispositivo.

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



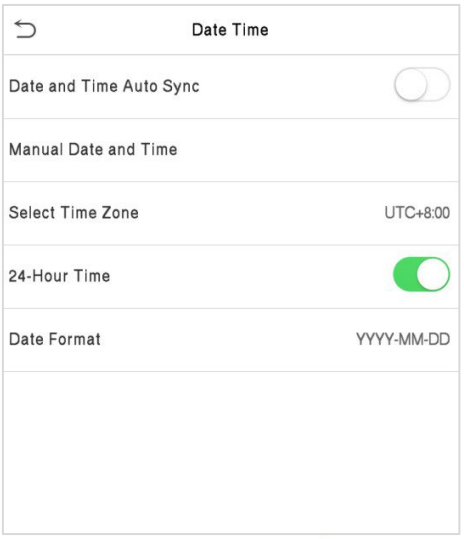
7.1 Data e Hora

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



O produto suporta o sistema de sincronização de horário NTP por padrão. Essa função entra em vigor depois que a **sincronização automática de data e hora** é ativada e o link do endereço do servidor NTP correspondente é definido.

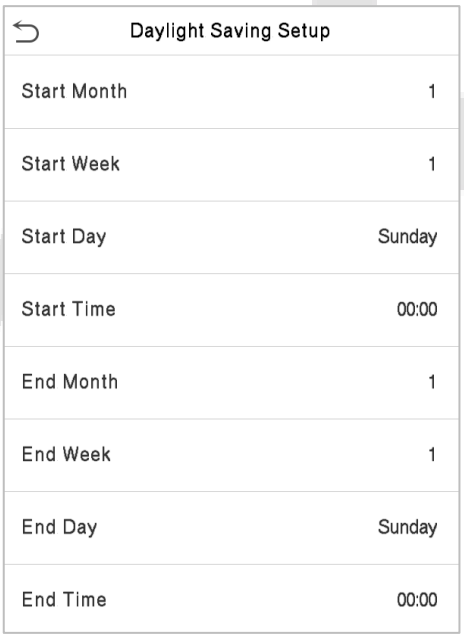
Se os usuários precisarem definir a data e a hora manualmente, primeiro desabilite a **Data e hora automática** e, em seguida, toque em **Data e hora manual** para definir a data e a hora e toque em **Confirmar** para salvar.



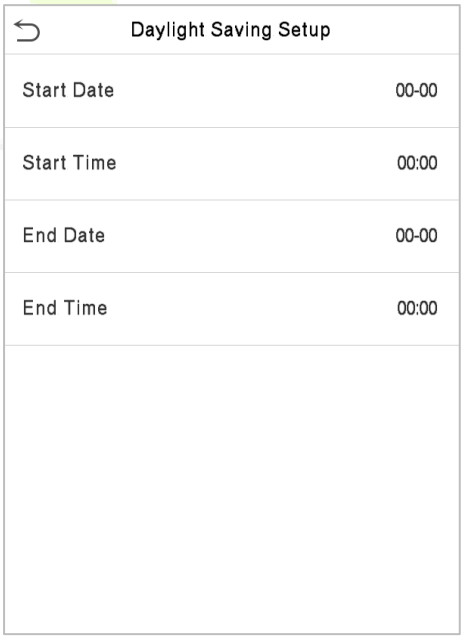
Toque em **Selecionar Fuso Horário** para escolher um fuso horário e, em seguida, toque no botão de retorno para salvar e sair.

Toque em **Formato de Hora de 24 Horas** para ativar ou desativar esse formato. Se ativado, selecione o **Formato de Data** para definir o formato da data, ou seja, como a data deve ser exibida no dispositivo.

★ 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.



Modo de Semana



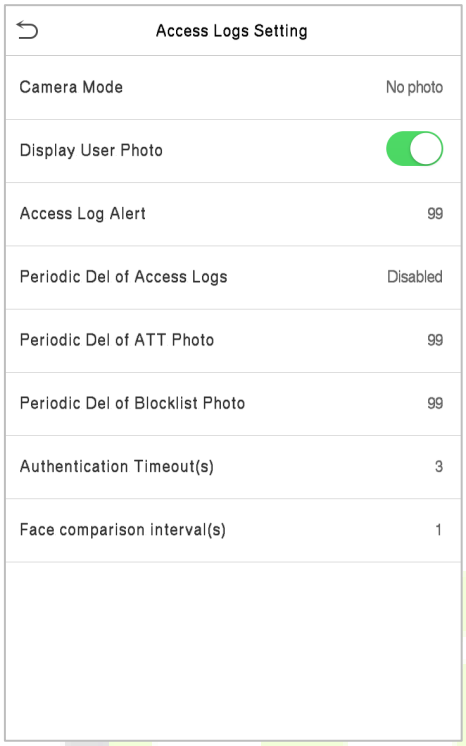
Modo de Data

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

Observação: Por exemplo, se um usuário definir a hora do dispositivo para 18:35 em 15 de março de 2019 e, em seguida, alterar para 18:30 em 1º de janeiro de 2020. Após restaurar as configurações de fábrica, a hora do dispositivo permanecerá como 18:30 em 1º de janeiro de 2020.

7.2 Configuração de Registros de Acesso

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

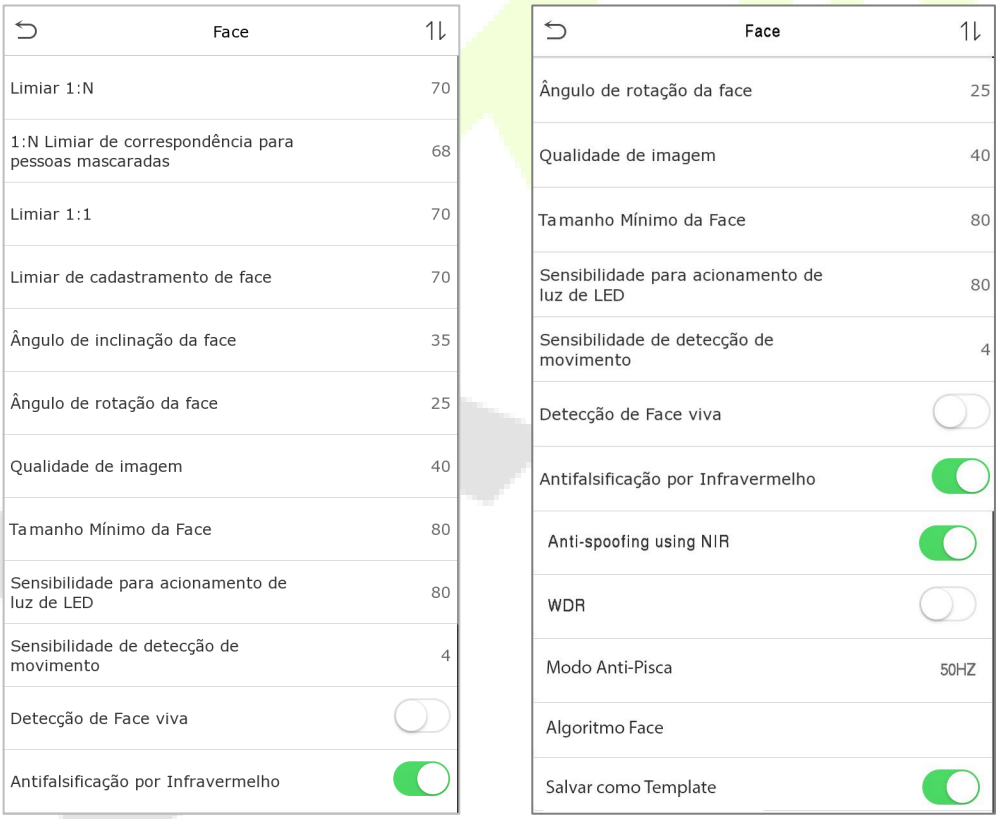


Função	Descrição
Modo de câmera	Esta função está desativada por padrão. Quando ativado, um prompt de segurança será exibido e o som do obturador na câmera será ativado. Existem 5 modos: **Sem Foto:** Nenhuma foto é tirada durante a autenticação do usuário. **Capturar, não salvar:** A foto é tirada, mas não salva durante a autenticação **Capturar e salvar:** A foto é tirada e salva durante a autenticação. **Salvar na verificação bem-sucedida** A foto é tirada e salva para cada autenticação bem-sucedida. **Salvar na verificação com falha:** A foto será tirada e salva apenas para a autenticação com falha.
Exibir foto do usuário	Esta função está desativada por padrão. Quando ativada, um prompt de segurança será exibido. A foto do usuário é exibida quando o usuário for autenticado com sucesso.
Aviso de logs de acesso	Quando os registros de acesso atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de registros de acesso antigos. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 999.
Exclusão cíclica dos registros de acesso	Quando as fotos de ponto atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de fotos de ponto antigas. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 99.

Exclusão cíclica de fotos de presença	Quando as fotos de presença atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de fotos de presença antigas. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 99
Exclusão cíclica de fotos da lista de restrições	Quando as fotos da lista de restrições atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de fotos antigas da lista de restrições. 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)	A quantidade de tempo necessária para comparar modelos faciais. 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 registrados for maior que o valor definido. O valor válido varia de 65 a 120. 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 75.

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.
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 maior que esse limite, indica que a face já foi cadastrada.
Ângulo de inclinação da face	É a tolerância de ângulo de inclinação de um rosto para o registro e comparação de modelos faciais. Se o ângulo de inclinação de um rosto exceder o valor definido, ele será filtrado pelo algoritmo, ou seja, será ignorado pelo terminal e nenhuma interface de registro e comparação será acionada.
Ângulo de rotação da face	É a tolerância de ângulo de rotação de um rosto para o registro e comparação de modelos faciais. Se o ângulo de rotação de um rosto exceder o valor definido, ele será filtrado pelo algoritmo, ou seja, será ignorado pelo terminal e nenhuma interface de registro e comparação será acionada.
Qualidade da imagem	Qualidade de imagem para cadastro e autenticação facial. Quanto maior o valor, mais clara a imagem precisa ser.
Tamanho mínimo da face	Necessário para registro facial e comparação. Se o tamanho de um objeto for menor que o valor definido, o objeto será filtrado e não será reconhecido como um rosto. Este valor pode ser entendido como a distância de comparação facial. Quanto mais longe a pessoa estiver, menor será o rosto e menor será o pixel facial obtido pelo algoritmo. Portanto, ajustar esse parâmetro pode ajustar a distância de comparação mais distante das faces. Quando o valor é 0, a distância de comparação da face não é limitada.
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.
Sensibilidade de detecção de movimento potencial	É definir o valor da mudança no campo de visão de uma câmera, que é conhecido como detecção de movimento. Isto irá despertar o equipamento do modo de espera para a tela de autenticação. Quanto maior o valor, mais sensível será, ou seja, se um valor maior for definido mais frequentemente será acionada a tela de autenticação.
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 antifalsificação usando luz visível.

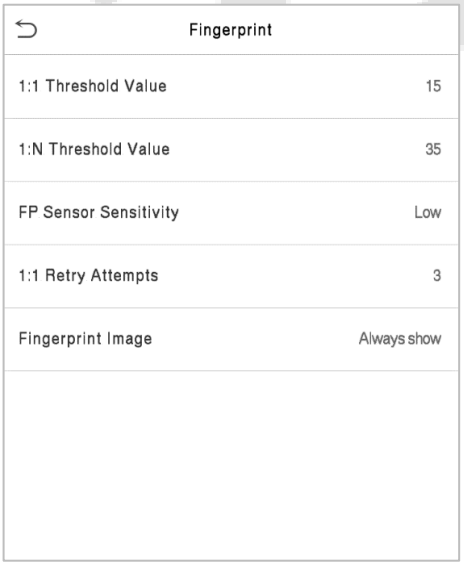
Antifalsificação por infravermelho	Usado para ativar a montagem de imagens infravermelho na autenticação e evitar ataques de fotos e vídeos falsos.
WDR	Ampla Faixa Dinâmica (WDR), que equilibra a luz e amplia a visibilidade da imagem para vídeos de vigilância em cenas de iluminação de alto contraste e melhora a identificação de objetos em ambientes claros e escuros.
Modo Antioscilação	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 facial	Informações relacionadas ao algoritmo facial e pausar a atualização do modelo facial.
Salvar foto como Template	Esta função é habilitada por padrão, e a interface do menu suporta a habilitação ou desabilitação dessa função e existe um prompt de segurança ao alternar. Quando esta função estiver desativada, indicará que há um lembrete de risco: "**É necessário recadastrar o rosto após uma atualização do algoritmo.**"

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 **Antifalsificação por infravermelho** para configurar a antifalsificação.
- Em seguida, no Menu Principal, selecione **Auto-Teste > Teste de Rosto** 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 o rosto. É recomendado não mover o rosto em uma ampla faixa.

7.4 Parâmetros de impressão digital

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

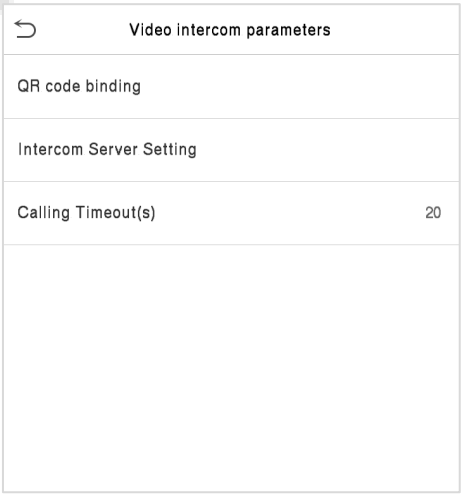


FRR	FAR	Limiares de correspondência recomendados	
		1:N	1:1
Alto	Baixo	45	25
Médio	Médio	35	15
Baixo	Alto	25	10

Função	Descrição
Limiar 1:1	No método de verificação 1:1, a verificação 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 verificação 1:N, a verificação será bem-sucedida apenas quando a similaridade entre os dados de impressão digital adquiridos e os modelos de impressão digital cadastrados no dispositivo for maior que o valor definido.
Sensibilidade do sensor de impressão digital	To set the sensibility of fingerprint acquisition. It is recommended to use the default level "**Medium**". When the environment is dry, resulting in slow fingerprint detection, you can set the level to "**High**" to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "**Low**".
Tentativas de repetição 1:1	Na verificação 1:1, os usuários podem esquecer a impressão digital registrada ou pressionar o dedo de forma incorreta. Para reduzir o processo de reinscrição do ID do usuário, é permitida a tentativa de repetição.
Imagem de Impressão Digital	Esta função está desativada por padrão. Após desativá-la, a imagem da impressão digital não será exibida ao registrar e verificar as impressões digitais. A interface do menu permite ativar ou desativar essa função, e há prompts de segurança ao alternar. Quatro opções estão disponíveis: **Mostrar para inscrição:** para exibir a imagem da impressão digital apenas na tela durante a inscrição. **Mostrar para verificação:** para exibir a imagem da impressão digital apenas na tela durante a verificação. **Sempre mostrar:** para exibir a imagem da impressão digital na tela durante a inscrição e verificação. **Nenhum:** não exibir a imagem da impressão digital.

7.5 Parâmetros de SIP

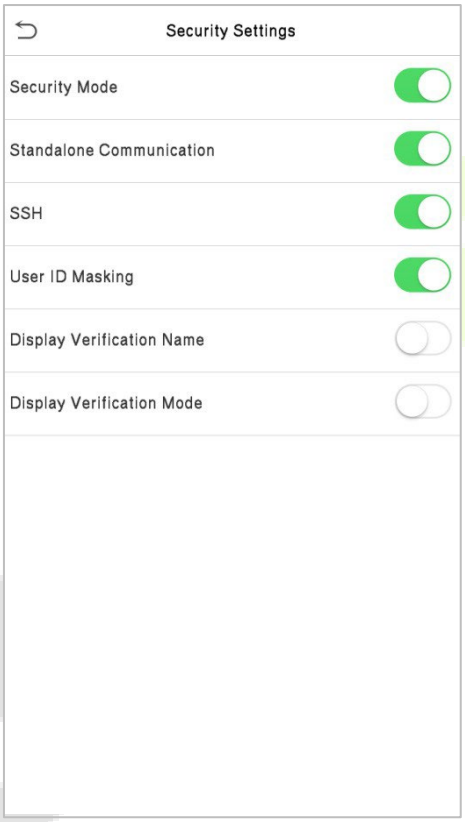
Clique em **Parâmetros de SIP** na interface do sistema.



Função	Descrição
Associação de QR Code	Utilize o aplicativo cliente ZSmart para escanear o código QR e conectar e associar o dispositivo.
Configurações do Servidor SIP	Configure o endereço IP e o número da porta do servidor. **Endereço do servidor:** Insira o endereço IP da instalação do servidor. **Porta do servidor:** É a porta de serviço configurada durante a instalação (não a porta ADMS).
Timeout de chamada (s)	Se a chamada não for atendida dentro de um tempo especificado, o dispositivo retorna para a interface principal.

7.6 Configurações de segurança

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



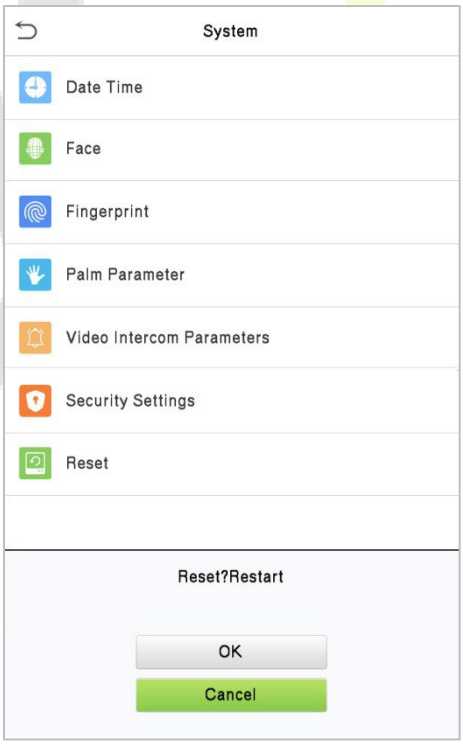
Função	Descrição
Modo de Segurança	Quando habilitada, a verificação de informações do usuário tem um alto nível de segurança. Esta função pode ser ativada ou desativada através da interface do menu. Ao ligar e desligar, há avisos de segurança. Todos os dados serão excluídos e o dispositivo será reiniciado após a confirmação. **Observação**: Depois de ativar o modo de segurança, o produto ativará forçosamente a função de retornar à interface de espera por padrão quando o menu expirar (60s por padrão). Ele não oferece suporte à desativação no modo de segurança, mas oferece suporte à desativação no modo sem segurança. Para configurar, vá para: **Personalizar > Interface do usuário > Tempo(s) limite da tela do menu.**

Comunicação autonôma	Por padrão, esta função está desativada. Esta função pode ser ativada ou desativada através da interface do menu. Quando é ligada, um prompt de segurança aparece e o dispositivo será reiniciado após a confirmação.
SSH	O dispositivo não oferece suporte ao recurso Telnet, portanto, o SSH é normalmente usado para depuração remota. Por padrão, o SSH está habilitado. A interface do menu permite ativar e desativar o SSH. Quando ativado, haverá um prompt de segurança, mas o dispositivo não precisará ser reiniciado após a confirmação.
Máscara de ID de Usuário	Depois de habilitado, o ID do usuário será exibido parcialmente após o resultado da autenticação pessoal e é habilitado por padrão. Para que possa ser mascarado, um ID de usuário precisa ter mais de 2 dígitos.
Exibir nome na autenticação	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 autenticação	Quando habilitada, resultado da verificação pessoal mostrará o modo de verificação do usuário. O resultado da verificação não mostrará o modo de verificação após a desativação desta opção.

7.7 Restauração dos padrões de fábrica

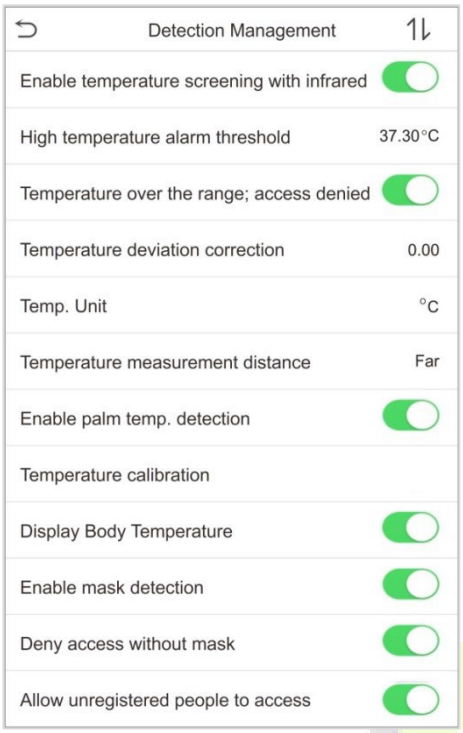
A função de Restauração de Fábrica restaura as configurações do dispositivo, como configurações de comunicação e configurações do sistema para as configurações padrão de fábrica (esta função não limpa os dados de cadastro do usuário e nem logs de acesso).

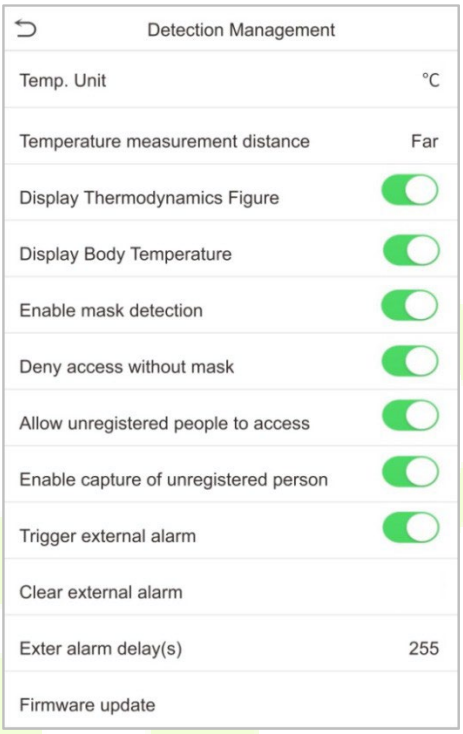
Toque em **Resetar** na interface do sistema e, em seguida, toque em **OK** para restaurar os padrões de fábrica.



7.8 Gestão de Detecção★

Toque em **Gestão de Detecção** na interface do Sistema





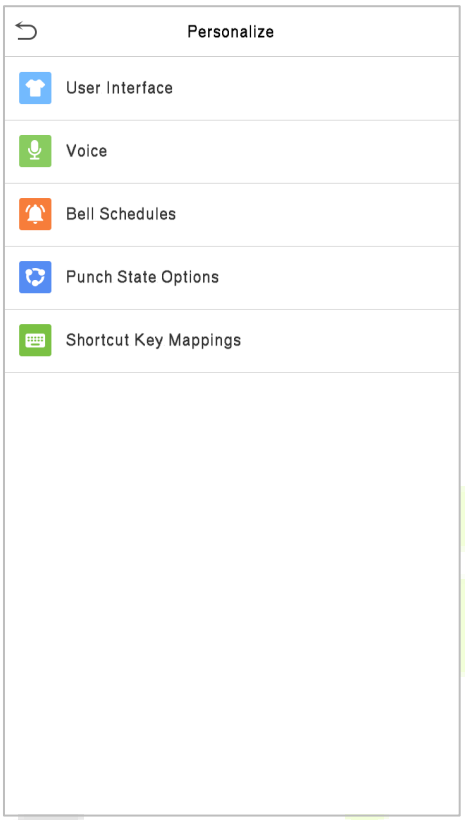
Função	Descrição
Ativar triagem de temperatura com infravermelho	Para habilitar ou desabilitar a função de medição de temperatura por infravermelho. Quando essa função está habilitada, os usuários devem passar pela triagem de temperatura além da verificação de identidade antes de terem acesso permitido. Para medir a temperatura corporal, os rostos dos usuários devem estar alinhados com a área de medição de temperatura.
Limiar de Alarme de Alta Temperatura	Para definir o valor do limiar de alarme de alta temperatura corporal. Quando a temperatura medida durante a verificação for maior que o valor definido, o dispositivo emitirá um aviso e um alarme sonoro. O limiar de alarme padrão é de 37,30℃.
Temperatura acima do intervalo; Acesso negado.	Quando essa função está ativada, se a temperatura corporal do usuário medida estiver acima (ou abaixo) do limite do alarme, o acesso do usuário não será concedido, mesmo que sua identidade seja verificada. Se essa função estiver desativada, o usuário poderá acessar a área restrita quando sua identidade for verificada, independentemente de sua temperatura corporal.
Correção de Desvio de Temperatura	Como o módulo de medição de temperatura permite uma pequena faixa de erros (distúrbios) de um valor observado em diferentes ambientes (umidade, temperatura ambiente, entre outros), os usuários podem definir o valor de desvio aqui.
Unidade de Temperatura	A unidade de temperatura corporal pode ser alternada entre Celsius (℃) e Fahrenheit (°F).

Distância de Medição de Temperatura	Ao medir a temperatura durante o processo de verificação, existem três modos: Próximo, Perto e Distante.
Exibir Figura Termodinâmica ★	Para habilitar ou desabilitar a exibição da imagem térmica de uma pessoa. Quando habilitada, a imagem térmica da pessoa será exibida no canto superior esquerdo do dispositivo durante o processo de detecção.
Habilitar a detecção de temperatura da palma da mão. ★	Para habilitar ou desabilitar a função de detecção de temperatura da palma da mão. Quando habilitada, o dispositivo exibirá a temperatura da palma da mão do usuário durante o processo de verificação. Observação: Esta função não está habilitada por padrão e pode ser atualizada para oferecer suporte.
Calibração de temperatura★	Calibre a temperatura comparando o valor atual da temperatura com o valor da temperatura da superfície do dispositivo.
Habilitar a detecção de máscara	Para habilitar ou desabilitar a função de detecção de máscara. Quando habilitada, o dispositivo irá identificar se o usuário está usando uma máscara durante a verificação.
Exibir temperatura corporal	Para habilitar ou desabilitar a função de exibição da temperatura corporal. Quando habilitada, o dispositivo exibirá o valor específico da temperatura do usuário durante o processo de verificação.
Habilitar Detecção de Máscara	Para habilitar ou desabilitar a função de detecção de máscara. Quando está habilitada, o dispositivo identificará se o usuário está usando uma máscara ou não durante a verificação.
Negar acesso sem máscara	Para habilitar ou desabilitar 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	Para habilitar ou desabilitar a função de permitir acesso a pessoas não registradas. Quando habilitada, desde que a pessoa passe pela detecção, o dispositivo permite que a pessoa entre sem registro.
Habilitar a captura de pessoas não registradas	Para habilitar ou desabilitar a função de captura de pessoas não registradas. Quando habilitado, o dispositivo irá capturar automaticamente a foto da pessoa não registrada. Para habilitar essa função, é necessário ativar a opção **Permitir Acesso a Pessoas Não Registradas**.
Disparar Alarme Externo ★	When enabled, if the user's temperature is higher than the set threshold value or the mask detection is enabled, but the mask is not worn by the person, it will trigger an alarm.
Limpar Alarme Externo ★	It clears the triggered alarm records of the device.
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.

Update de Firmware ★	Escolha se deseja atualizar a versão do software do módulo de detecção de temperatura por imagem térmica.

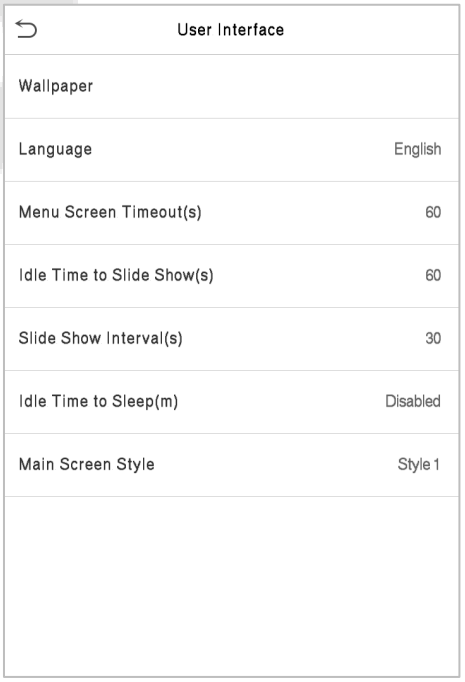
8 Personalização

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



8.1 Configurações da Interface

Toque em **Interface do Usuário** na interface de **Personalizar** para personalizar o estilo de exibição da interface principal.



Function Name	Description
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.
Apresentação de Slides por Inatividade (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.

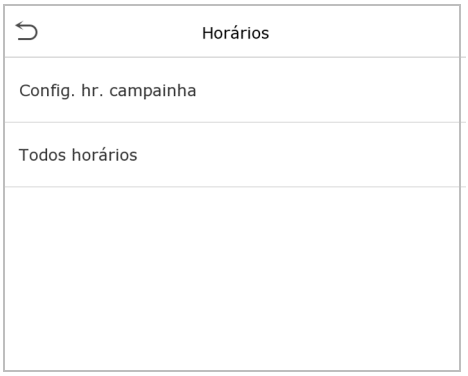
8.2 Configurações de voz

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

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

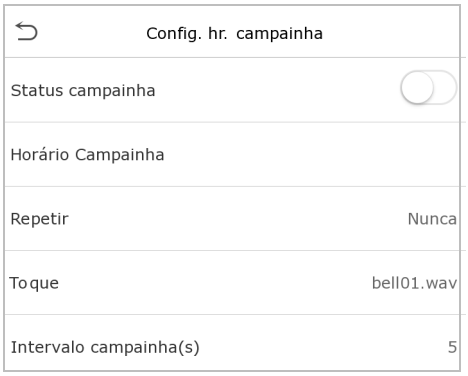
8.3 Horários

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



Novo Alarme

1. Toque em **Novo Alarme** na interface **Horário** 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 tempo necessário, o dispositivo acionará automaticamente para tocar a campainha durante esse tempo.
Repetir	Defina o número necessário de contagens para repetir a campainha programada.
Toque	Selecione um som de campainha.
Intervalo campainha (s)	Defina o tempo de reprodução da campainha. Os valores válidos variam de 1 a 999 segundos.

- **Todos os Horários**

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

- **Edite a campainha agendada**

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

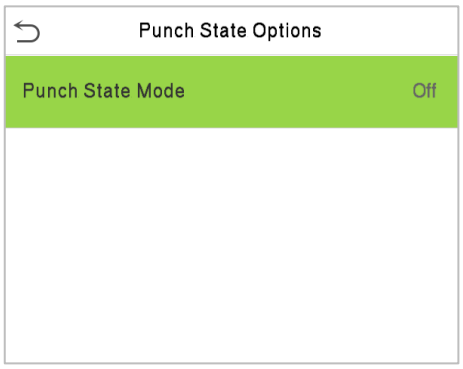
- **Deletar um horário**

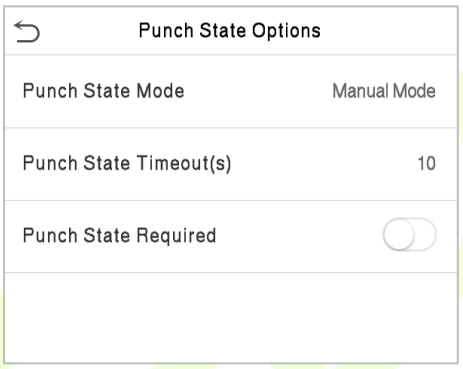
Na interface **Todos os Horários de campainha**, toque no alarme a ser deletado.

Em seguida, toque em **Excluir** e selecione **Sim** para excluir a campainha selecionada.

8.4 Configurações de Status de Registro de Presença

Selecione a opção **Status de Registro de Presença** na interface de **Personalização** para configurar as configurações do estado de batida.



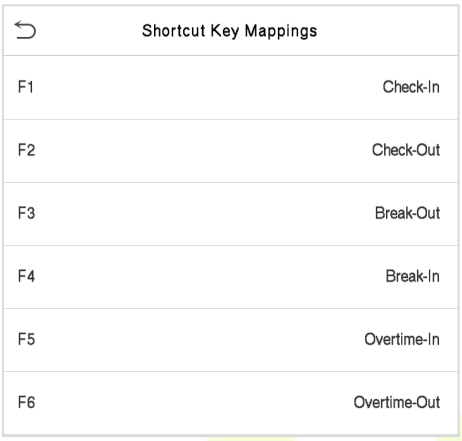


Function Name	Description
Modo de Status de Registro de Presença	Selecione um Modo de Status de Registro de Presença: **Off:** Isso desabilita a função de registro de presença. E a tecla de registro de presença definida no menu de **Mapeamento de Teclas de Atalho** se torna inválida. **Modo Manual:**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

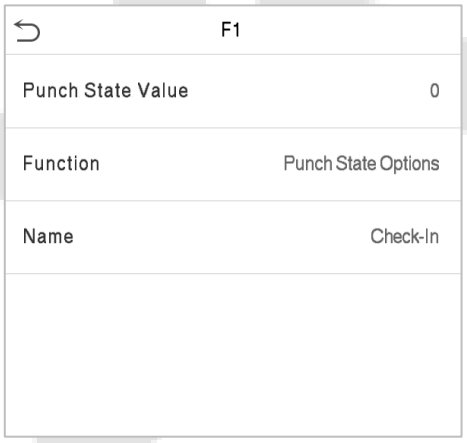
8.5 Mapeamento de Teclas de Atalho

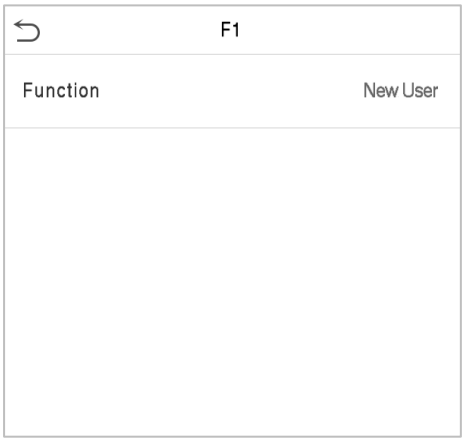
Os usuários podem definir teclas de atalho para os status de registro de presença e teclas funcionais na interface principal. Portanto, na interface principal, quando as teclas de atalho são pressionadas, o status de registro de presença correspondente ou a interface funcional são exibidos diretamente.

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



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

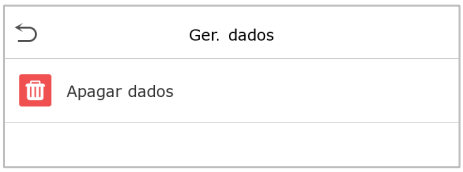




- Se a tecla de atalho for definida como uma tecla de estado de presença (como entrada, saída, etc.), então é necessário configurar o valor do estado de presença (valor válido de 0 a 250), o nome e o horário de alternância.

9 Gerenciamento de Dados

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



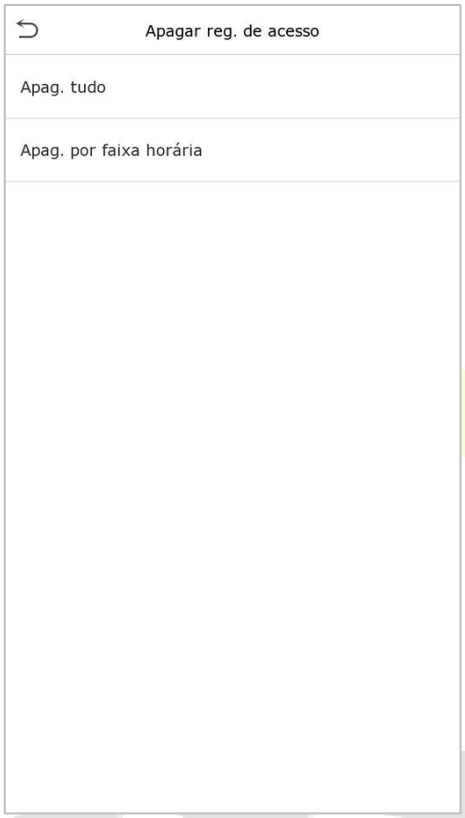
9.1 Excluir dados

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

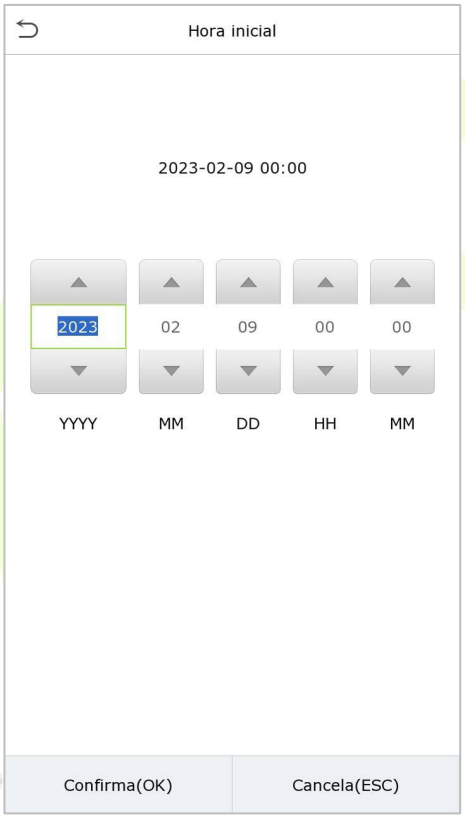
Função	Descrição
Apagar reg. de acesso	Para apagar dados de frequência/registros de acesso
Apagar foto ponto	Para apagar fotos de ponto registradas.
Apagar foto lista bloqueio	Para apagar as fotos tiradas durante verificações com falha.
Apagar todos os dados	Para apagar informações e registros de presença/registros de acesso de todos os usuários registrados.
Apagar privilégios de administrador	Para remover todos os privilégios de administrador (não apagar usuários).
Apagar dados de acesso	Para apagar todos os dados de acesso.
Excluir Templates de Fotos de Usuário	Para excluir templates de fotos do usuário no dispositivo. Ao excluir templates, há um lembrete de risco: "Um novo cadastro facial será necessário após atualização do algoritmo".

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

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



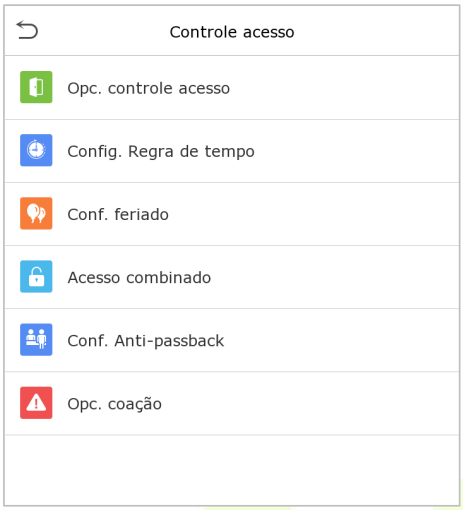
Selecione Apagar por intervalo de tempo.



Defina o intervalo de tempo e clique em OK.

10 Controle de acesso

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

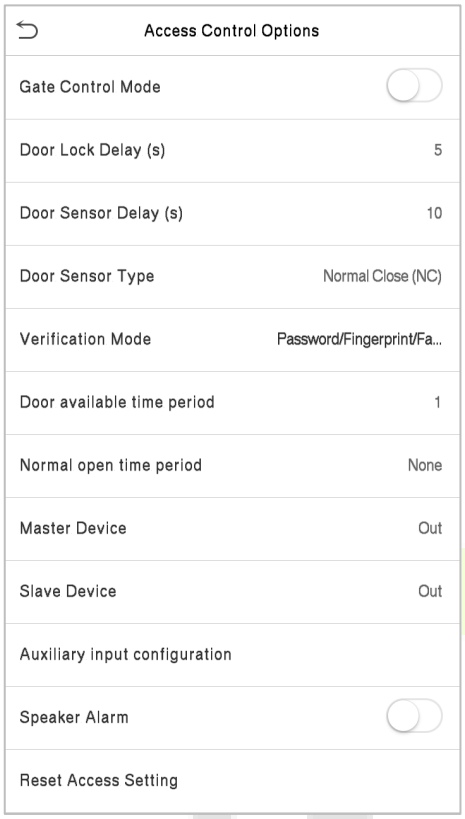


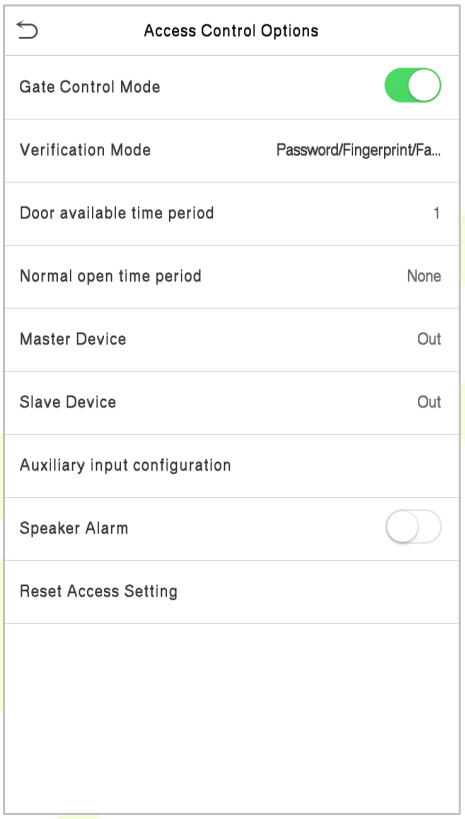
Para ter uma autenticação válida, o usuário cadastrado deve atender às seguintes condições:

- O tempo atual de desbloqueio da porta deve estar dentro de qualquer fuso horário válido do período de tempo do usuário.
- O grupo do usuário já deve estar definido na combinação de desbloqueio da porta (e se houver outros grupos, sendo configurados no mesmo 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 a no estado de desbloqueio por padrão.

10.1 Opções de controle de acesso

Toque em **Opções de Controle de Acesso** na interface de **Controle de Acesso** para definir os parâmetros disponíveis.





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

Modo de verificação	O modo de verificação suportado inclui Senha/Impressão Digital/Rosto, Apenas Impressão Digital, Apenas ID de Usuário, Senha, ID de Usuário + Impressão Digital, Impressão Digital + Senha, ID de Usuário + Impressão Digital + Senha, Apenas Rosto, Rosto + Impressão Digital, Rosto + Senha, Rosto + 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.
Período de tempo normalmente aberto	Período de tempo programado para o modo "Normal Aberto", para que a porta fique sempre aberta durante este período.
Equipamento mestre	Ao configurar o equipamento mestre, o status pode ser definido para sair ou entrar. **Saída:** O registro verificado no software é o registro de saída. **Entrada:** O registro verificado no software é o registro de entrada.
Dispositivo auxiliar	Ao configurar o dispositivo auxiliar, o status pode ser definido para sair ou entrar. **Saída:** O registro verificado no software é o registro de saída. **Entrada:** O registro verificado no software é o registro de entrada
Configuração de entrada auxiliar	Define o período de tempo de destravamento da porta e o tipo de saída auxiliar do dispositivo terminal auxiliar. Os tipos de saída auxiliar incluem "Nenhum", "Acionamento da porta", "Acionamento de alarme" e "Acionamento de porta e alarme".
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 incluem tempo de trava da porta, tempo de atraso do sensor, tipo de sensor, modo de verificação, período de tempo disponível da porta, período de tempo normal de abertura, dispositivo mestre e alarme. No entanto, dados de controle de acesso apagados em Ger. Dados é excluído.

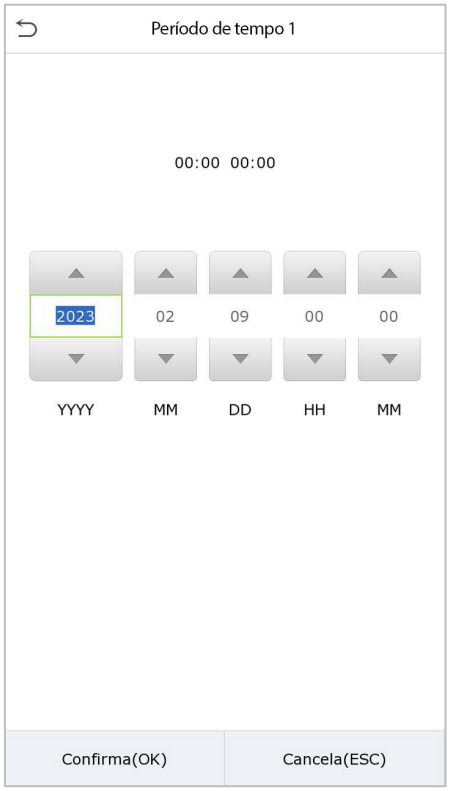
10.2 Configuração de regra de tempo

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

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

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

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



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

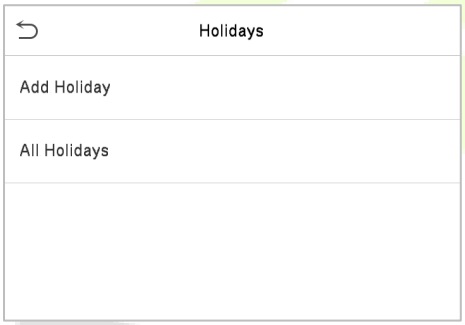
Observação:

- Quando o horário de término é anterior ao horário de início (como 23:57~23:56), indica que o acesso está proibido o dia todo.
- Quando a hora de término for posterior à 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) .
- A faixa horária padrão 1 indica que a porta está aberta o dia todo.

10.3 Feriados

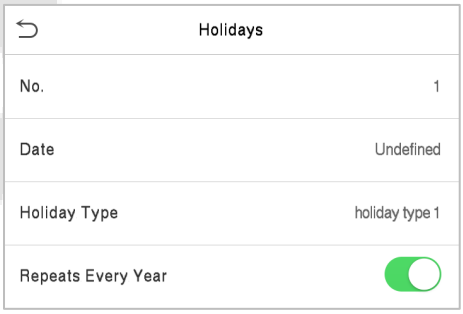
Sempre que houver feriado, poderá necessitar de um horário de acesso especial; mas alterar o horário de acesso de todos um por um é extremamente complicado, então você pode definir um horário de acesso de feriado que seja aplicável a todos os funcionários, e o usuário poderá abrir a porta durante os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

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



- **Adicionar um novo feriado**

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



- **Editar um feriado**

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

- **Excluir um feriado**

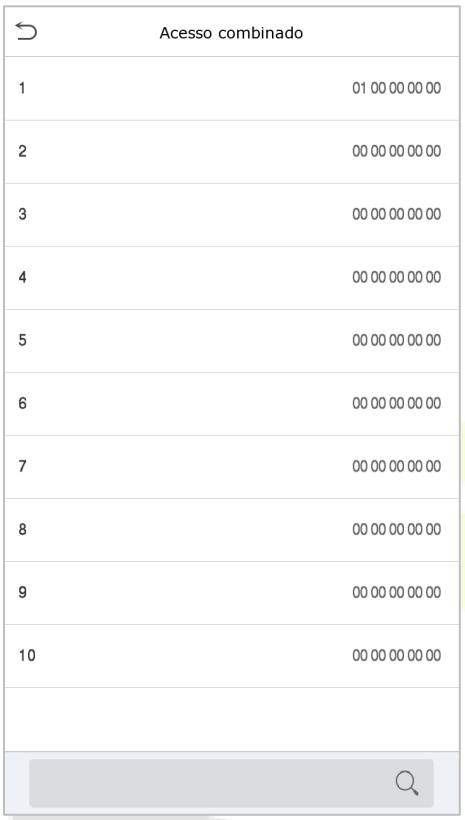
Na interface de **Feriados**, selecione um item de feriado a ser excluído e toque em **Apagar**. Pressione **OK** para confirmar a exclusão. Após a exclusão, este feriado não é mais exibido na interface **Todos os feriados**.

10.4 Acesso combinado

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

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

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



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

Por Exemplo:

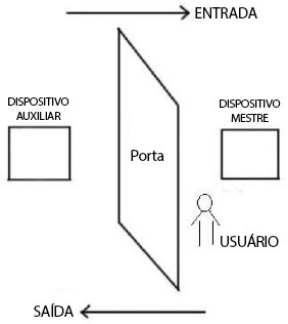
- Se a **combinação de desbloqueio da porta 1** for configurada como (01 03 05 06 08), isso indica que a combinação de desbloqueio 1 é composta por 5 pessoas e todas as 5 pessoas são de 5 grupos diferentes, a saber, Grupo AC 1, Grupo AC 3, Grupo AC 5, Grupo AC 6 e Grupo AC 8, respectivamente.
- Se a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

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

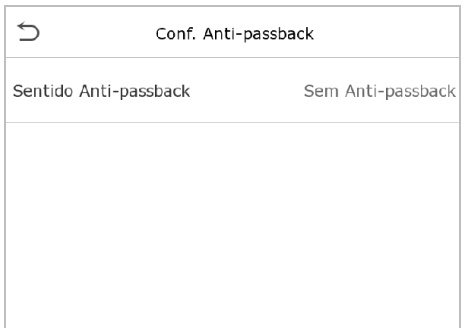
10.5 Configuração Anti-Passback

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

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



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

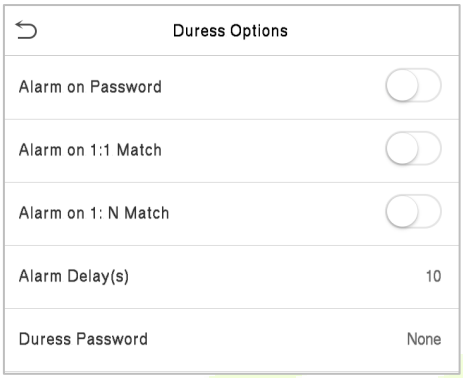


Function Name	Description
Direção Anti-Passback	**Sem Anti-passback:** A função anti-passback está desativada, o que significa que a verificação bem-sucedida através do dispositivo mestre ou do dispositivo auxiliar pode desbloquear a porta. O status de entrada ou saída não é salvo nesta opção para o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

10.6 Opções de Coação

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

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



Função	Descrição
Senha de alarme	Quando um usuário usa o método de verificação de senha, um sinal de alarme será gerado somente quando a verificação de senha for bem-sucedida, caso contrário não haverá sinal de alarme.
Alarme em Caso de Autenticação 1:1	Quando um usuário utiliza o método de verificação 1:1, um sinal de alarme será gerado; caso contrário, não haverá sinal de alarme.
Alarme em Caso de Autenticação 1:N	Quando um usuário utiliza o método de verificação 1:N, um sinal de alarme será gerado; caso contrário, não haverá sinal de alarme.
Atraso do Alarme (s)	O sinal de alarme não será transmitido até que o tempo de atraso do alarme 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 verificação, um sinal de alarme é gerado.

11 Procurar registros

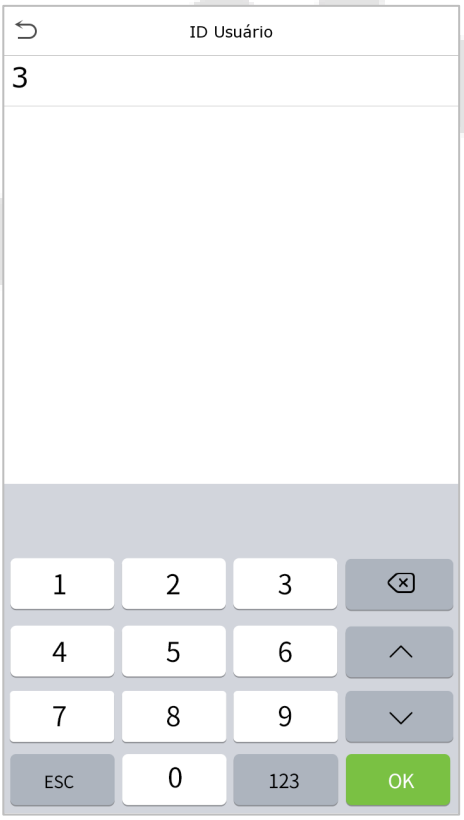
Assim que a autenticação de um usuário for validada, os logs de eventos serão salvos no dispositivo. Esta função permite que os usuários verifiquem seus registros de acesso.

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

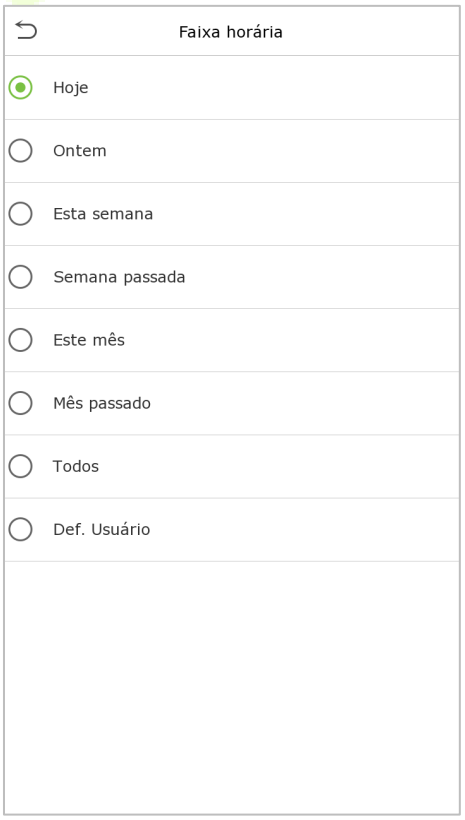
O processo de pesquisa de fotos de presença e lista de bloqueio é semelhante ao da pesquisa de logs de eventos. Veja a seguir um exemplo de pesquisa de logs de eventos.

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

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

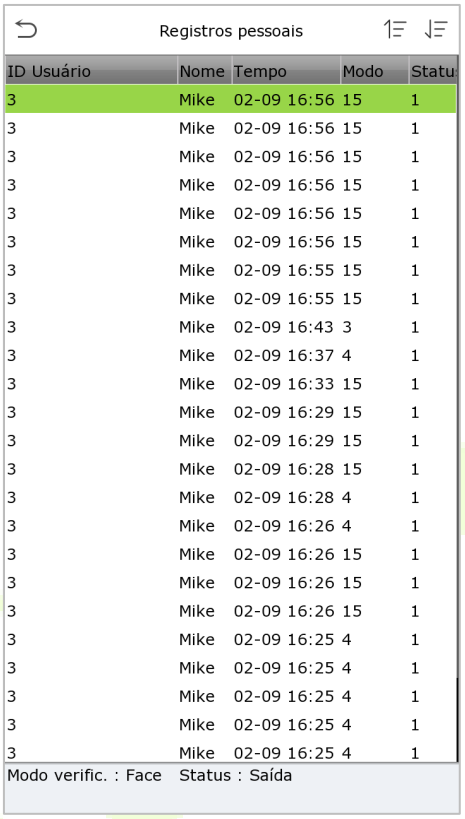


2. Selecione o intervalo de tempo em que os logs precisam ser pesquisados.



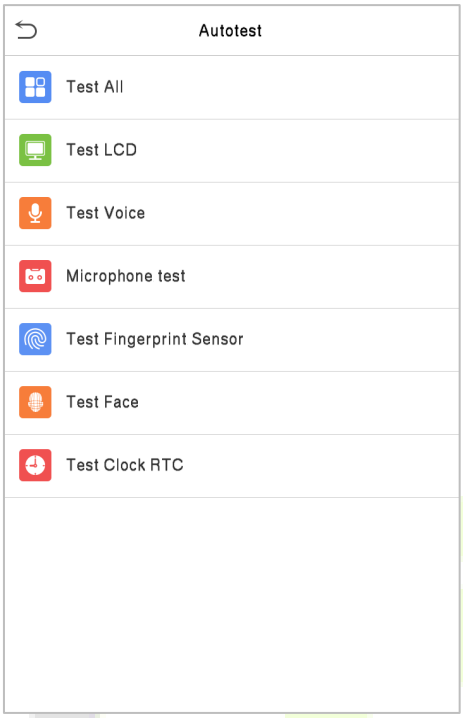
3. Depois que a pesquisa de log for bem-sucedida, toque no registro destacado em verde para visualizar seus detalhes.

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



12 Auto teste

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

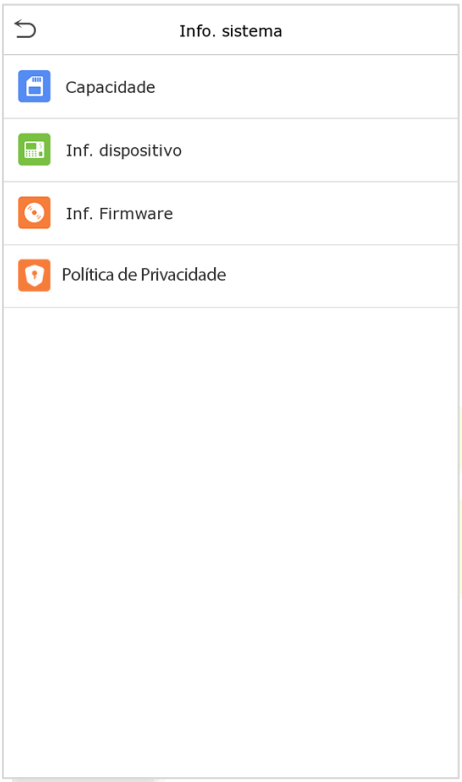


Function Description

Função	Descrição
Testar tudo	Para testar automaticamente se o LCD, áudio, câmera e relógio em tempo real (RTC) estão normais.
Teste LCD	Para testar automaticamente a tela LCD 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	Testar o sensor de impressão digital pressionando um dedo no scanner para verificar se a imagem da impressão digital adquirida está clara. Quando você pressionar um dedo no scanner, a imagem da impressão digital será exibida na tela.
Teste face	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.

13 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.



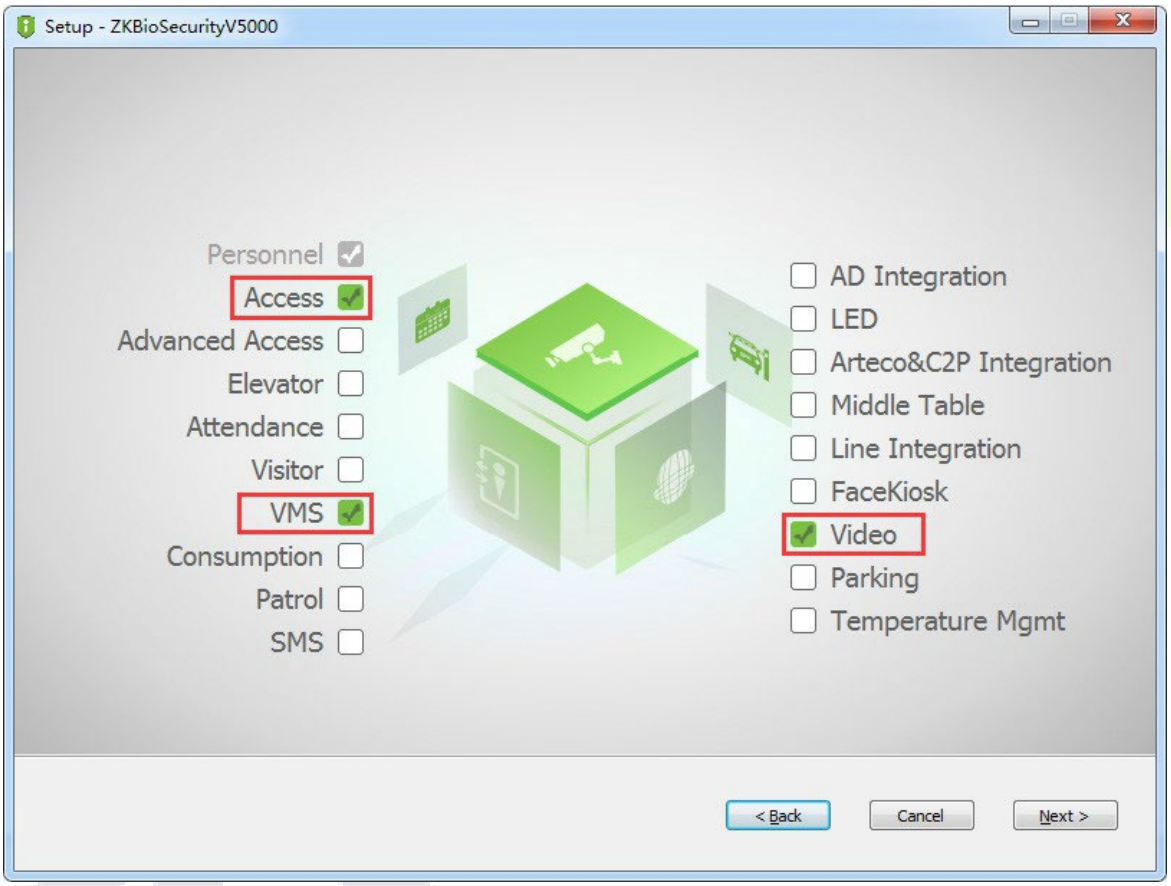
Menu	Descrição
Capacidade do dispositivo	Exibe o armazenamento do usuário do dispositivo atual, palma, senha, face, cartão, administradores, registros de acesso, fotos de presença e lista de bloqueio e fotos do usuário.
Informação do dispositivo	Exibe o nome do dispositivo, número de série, endereço 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.

14 Configurações da Função de Videoport eiro LAN★

14.1 Instalando o Plugin ZKBio VMS no Software ZKBioSecurity

- **Instale o Software ZKBioSecurity**

Durante a instalação, selecione o módulo "VMS" do software ZKBioSecurity para instalar, conforme mostrado na interface de instalação a seguir.



Observação: O módulo de Vídeo e o módulo VMS não podem ser selecionados ao mesmo tempo.

- **Instalando o Plugin ZKBio VMS**

Dê um duplo clique no arquivo fornecido **ZKBioVMSPlugin_sqlite.exe** para instalar o Plugin ZKBio VMS.

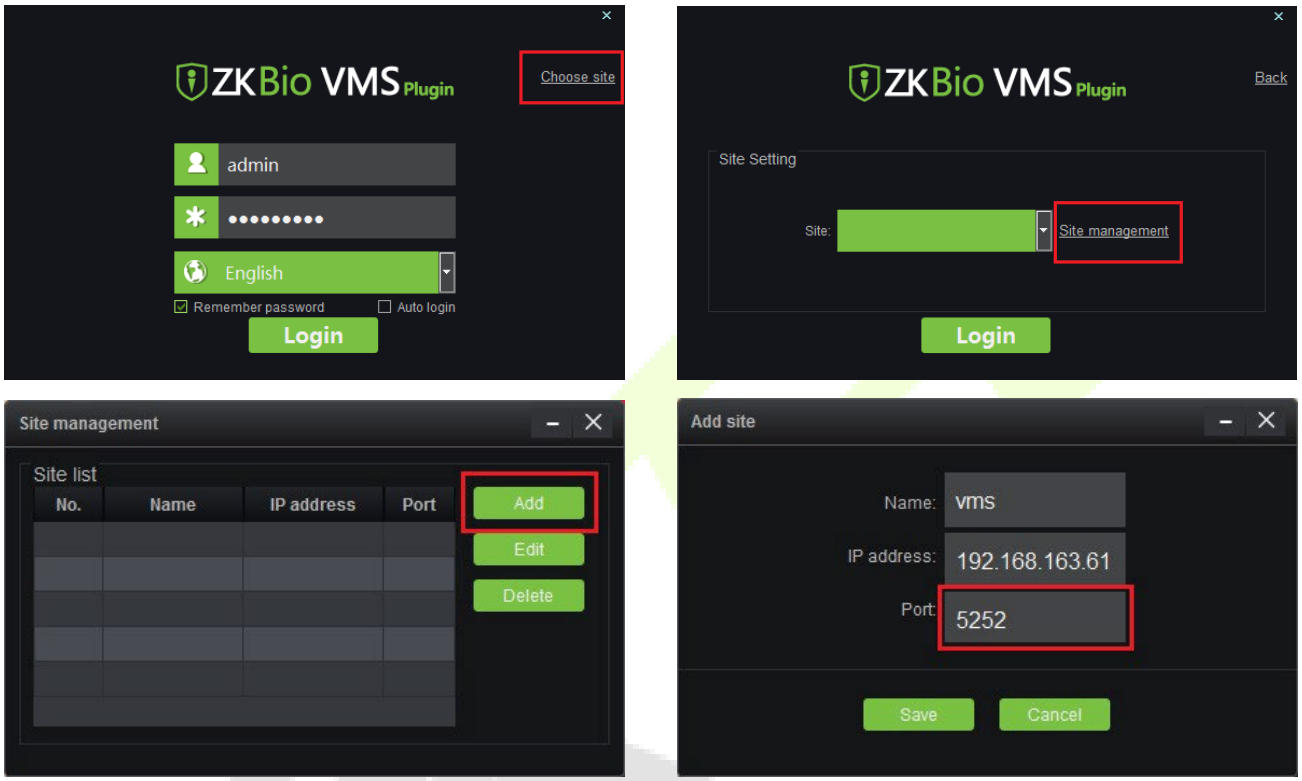
Observação: O software ZKBioSecurity e o Plugin ZKBio VMS precisam ser abertos simultaneamente para reconhecer a função de intercomunicação.

14.2 Parâmetros de Configuração

Configure os parâmetros necessários corretamente para garantir uma conexão entre o dispositivo e o software.

1. Adicionar local no plugin Video-VMS

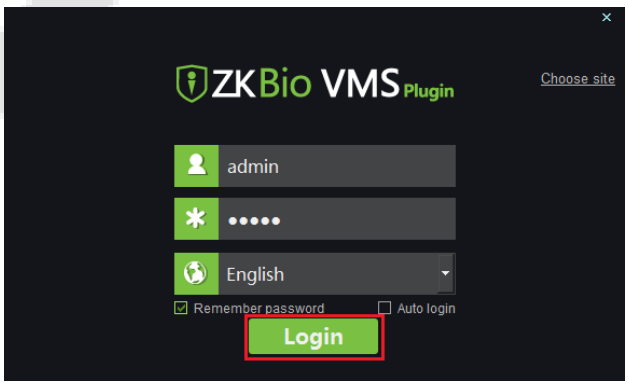
a. Dê um duplo clique no ícone para abrir o Plugin Video-VMS. Clique em **Escolher local** > **Gerenciamento de local** > **Adicionar** na interface de login. Em seguida, insira o Nome, Endereço IP e Porta para adicionar um local, conforme mostrado na figura a seguir.



Endereço IP: Insira o endereço IP local

Porta: A porta padrão é 5252

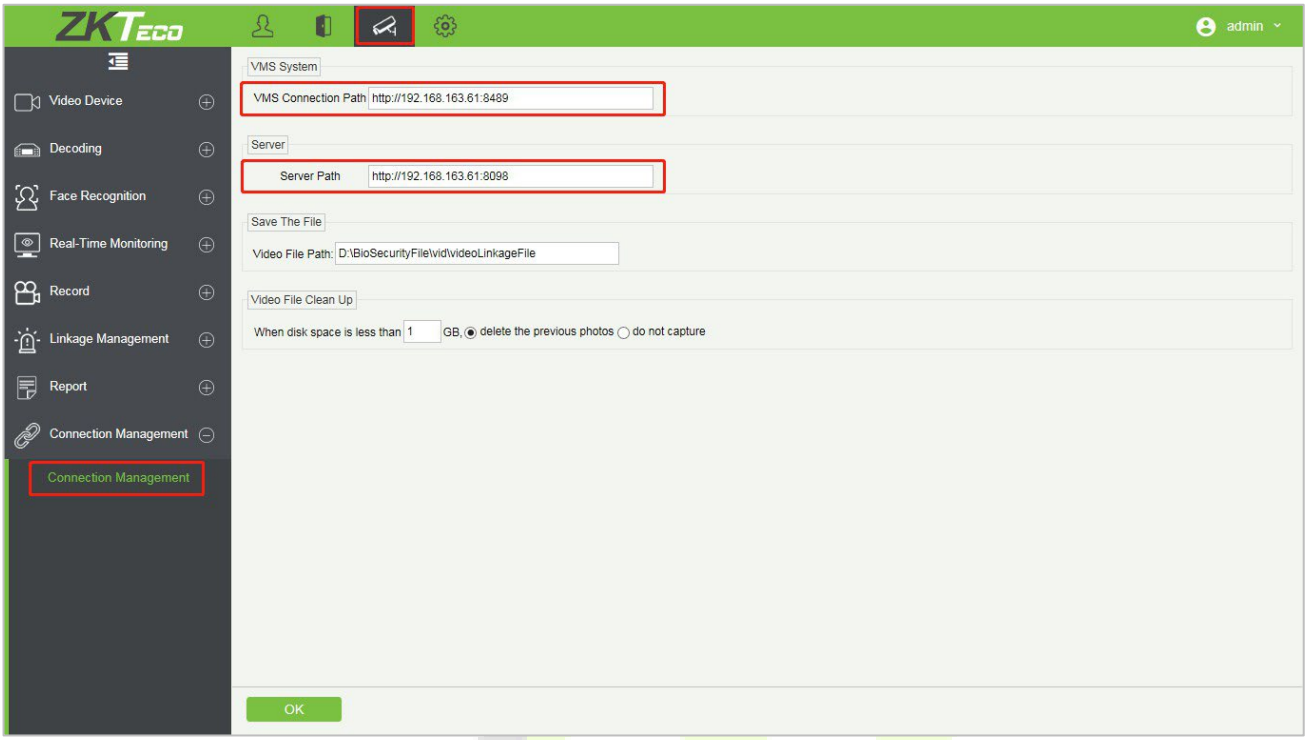
b. Após adicionar o local, insira o nome de usuário e a senha e clique em **Login** para acessar o plugin Video-VMS. O nome de usuário e a senha inicial são ambos "admin".



Observação: Quando o plugin Video-VMS se conecta com sucesso ao ZKBioSecurity, a senha é alterada sincronicamente para a senha do usuário admin do ZKBioSecurity.

2. Configure o caminho de conexão entre o ZKBioSecurity e o plugin VMS

Clique em **Vídeo > Conexão > Gerenciamento de Conexão** no software ZKBioSecurity para alterar o caminho, como mostrado na imagem a seguir:



Caminho da Conexão VMS

- **URL:** "http://local IP address: port"
- **Porta:** Por padrão, é 8489 (por exemplo, http://192.168.163.61:8489).

Caminho do Servidor

- **URL:** "http://server IP address: port"
- **Porta:** A porta é a porta de serviço definida durante a instalação (por exemplo, http://192.168.163.61:8098) (não é a porta ADMS).

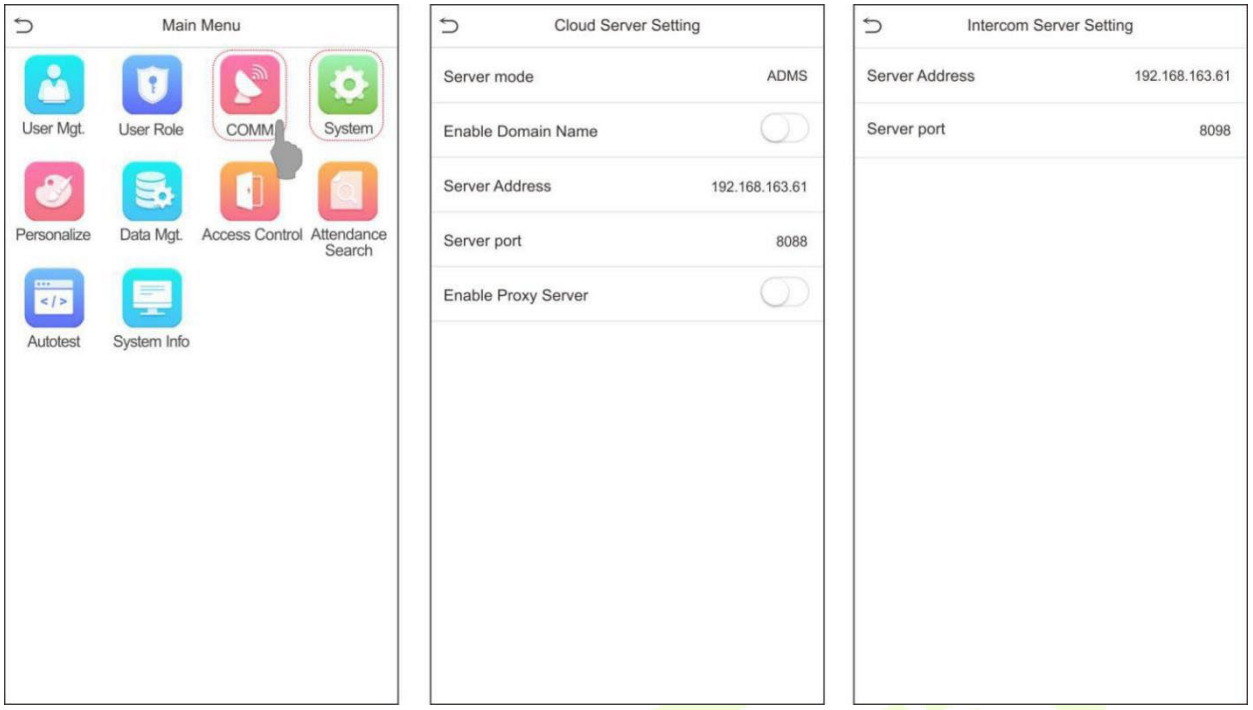
3. Configure os parâmetros no dispositivo

a. Clique em ☰ **> COMM. > Configuração do Servidor em Nuvem no dispositivo para definir o endereço** do servidor e a porta do servidor, ou seja, o endereço IP e o número da porta do servidor após a instalação do software. Se o dispositivo se comunicar com o servidor com sucesso, o ícone será exibido no canto superior direito da interface de espera.

b. Clique em ☰ **> Sistema>Parâmetros de Videoporteiro>Configuração do Servidor de Intercomunicação** para definir o endereço e a porta do servidor

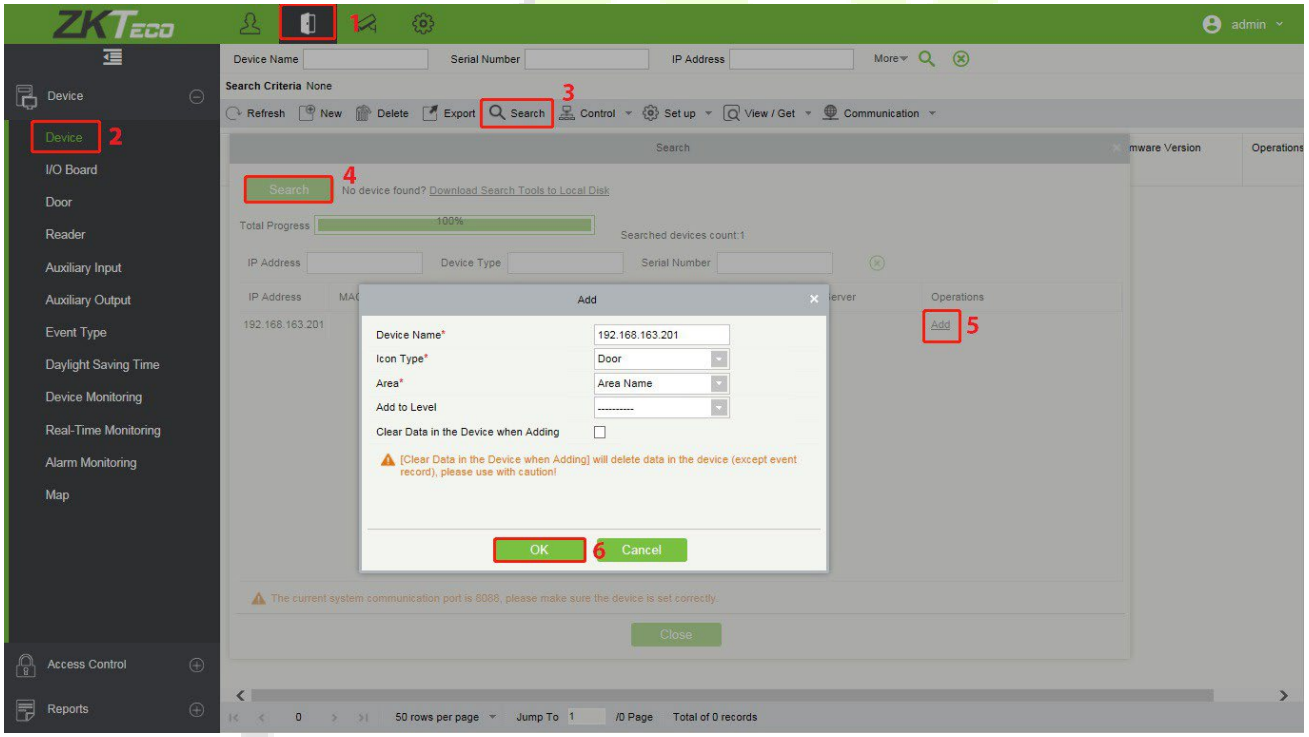
Endereço do Servidor: Insira o endereço IP da instalação do ZKBioSecurity.

Porta do Servidor: A porta é a porta de serviço definida durante a instalação (não é a porta ADMS).

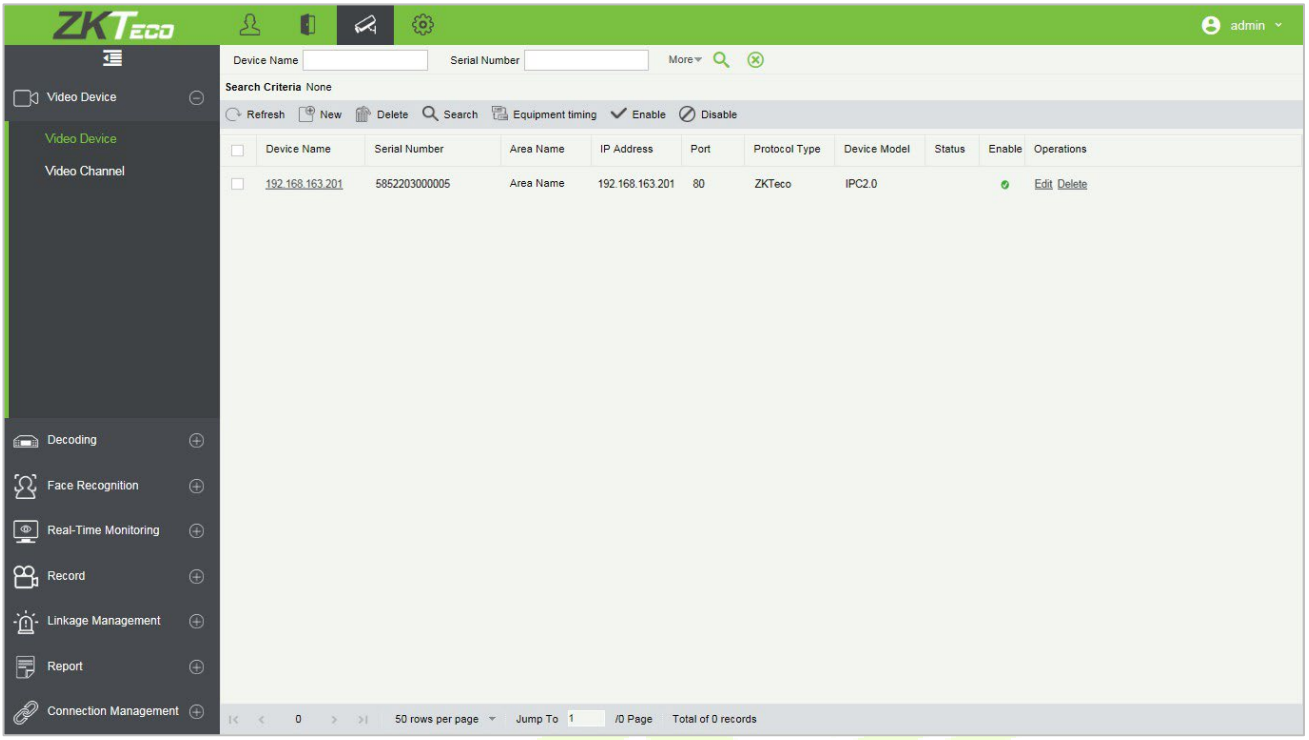


4. Adicionando dispositivo no software ZKBioSecurity.

a. Clique em **Acesso > Dispositivo > Pesquisar > Pesquisar** para adicionar o dispositivo no software ZKBioSecurity.



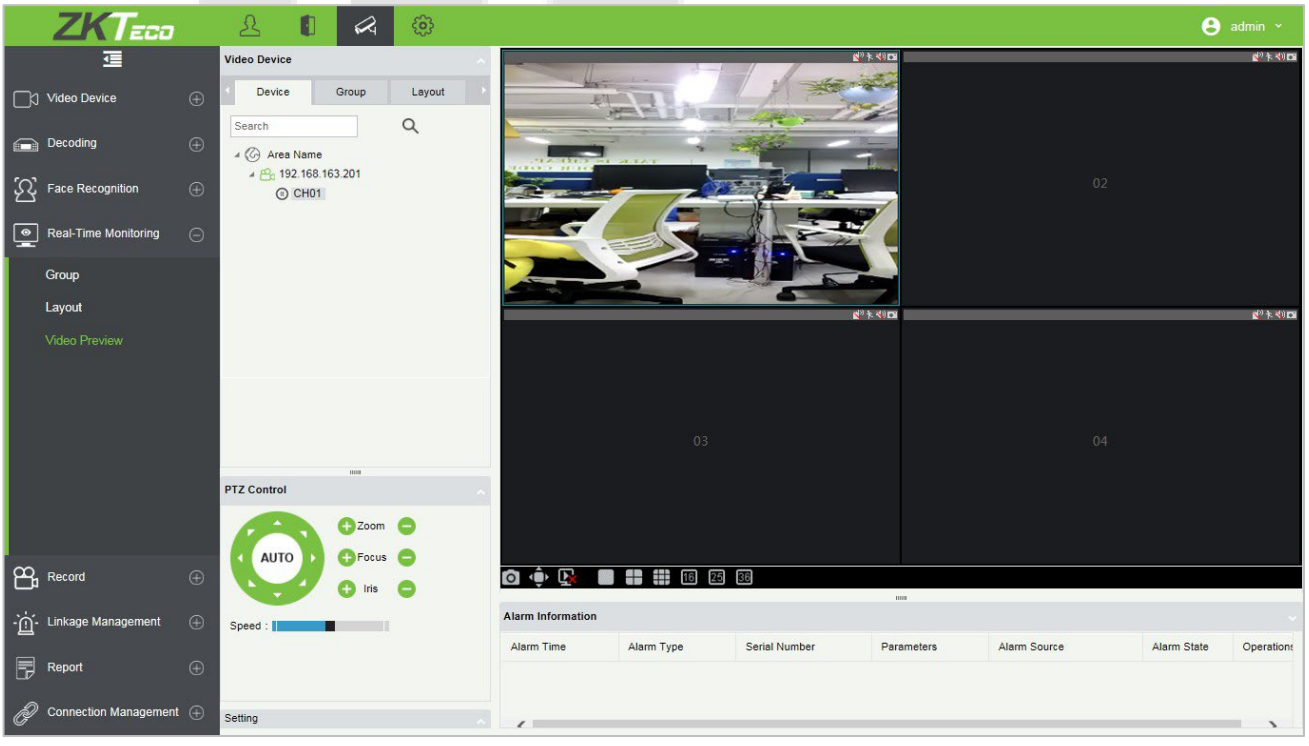
b. Após o dispositivo ser adicionado com sucesso ao módulo de acesso, ele é automaticamente adicionado ao módulo de vídeo. O usuário pode clicar em Vídeo > Dispositivo de Vídeo > Pesquisar para visualizar.



Observação: Se o dispositivo não for adicionado ao módulo de vídeo, verifique se as configurações de parâmetros estão corretas.

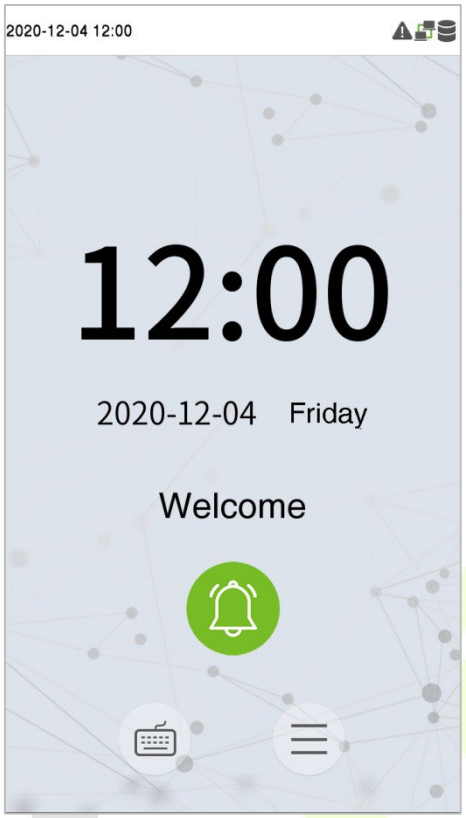
14.3 Visualização de Vídeo no Software ZKBioSecurity

Clique em **Vídeo > Monitoramento em Tempo Real > Visualização de Vídeo** para entrar na interface de pré-visualização do dispositivo.

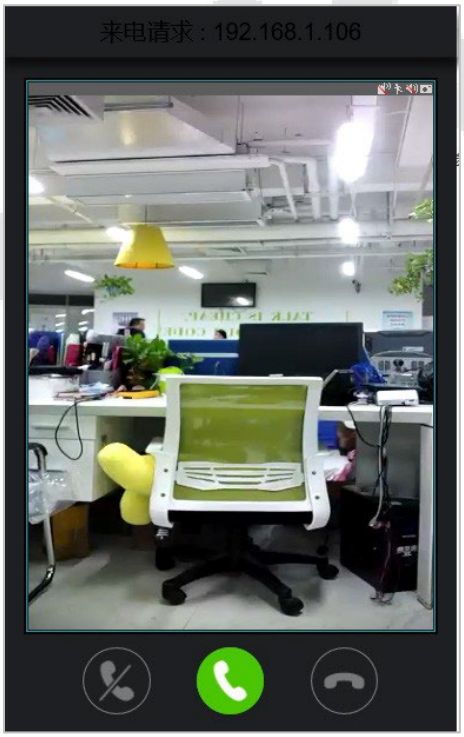


14.4 Realizar uma Chamada no Dispositivo

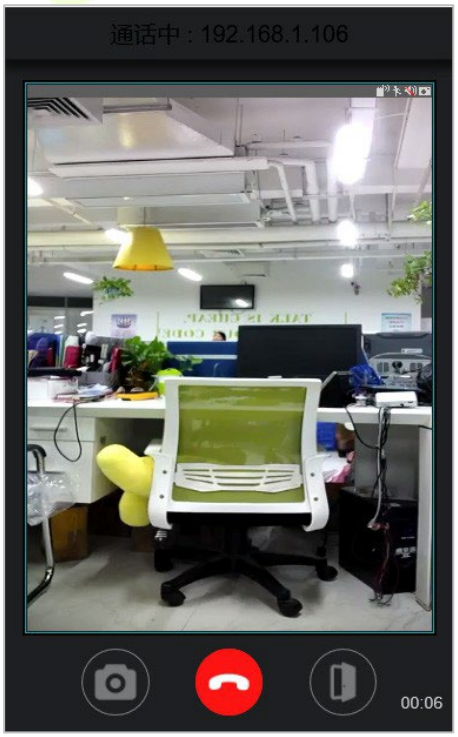
1. Clique no ícone na tela do dispositivo para fazer uma chamada.



2. A página do servidor exibe automaticamente a janela de chamada, como mostrado na figura a seguir.

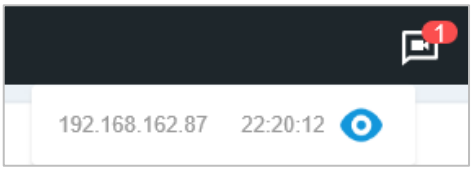


Interface de Chamada



Interface durante a Chamada

Funções

	É o botão **Atender**, o usuário pode clicar para atender a chamada atual. Após atender, a janela da chamada é aberta, e áudio e vídeo são ativados por padrão.
	É o botão **Desligar**. Após desligar, a chamada atual é encerrada imediatamente.
	É o botão **Ignorar**, usado para ignorar a chamada atual. Clique nele para fechar a janela da chamada  e o ícone no canto superior direito exibirá o número de chamadas pendentes  O usuário pode clicar no ícone  no menu suspenso para abrir novamente a janela de chamada do dispositivo atual e escolher atender, como mostrado na figura a seguir. 
	É o botão **Desligar**, usado para encerrar a chamada atual.
	É o botão **Captura de Tela**, usado para tirar uma captura de tela.
	É o botão **Abrir Remotamente**, usado para abrir a porta remotamente. O tempo padrão de acionamento da fechadura é de 5 segundos.

Observação: Se a interface de pré-visualização do dispositivo estiver aberta no software ZKBioSecurity, a interface de chamada não será mais exibida nesta janela de chamada.

15 Conectar ao Software ZKBioAccess MTD★

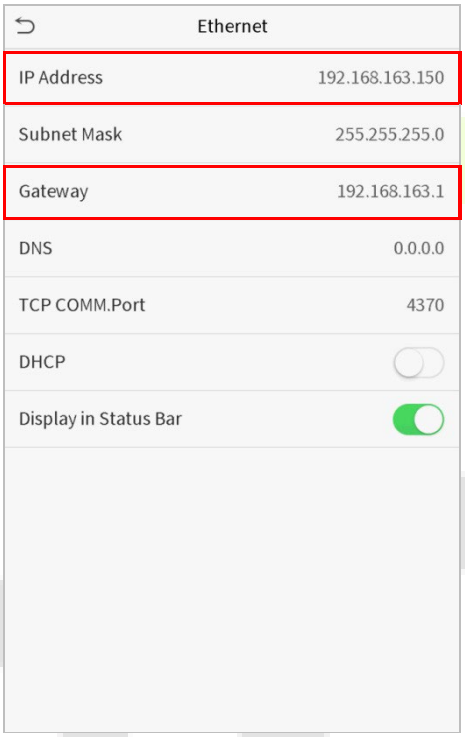
15.1 Configurar o Endereço de Comunicação

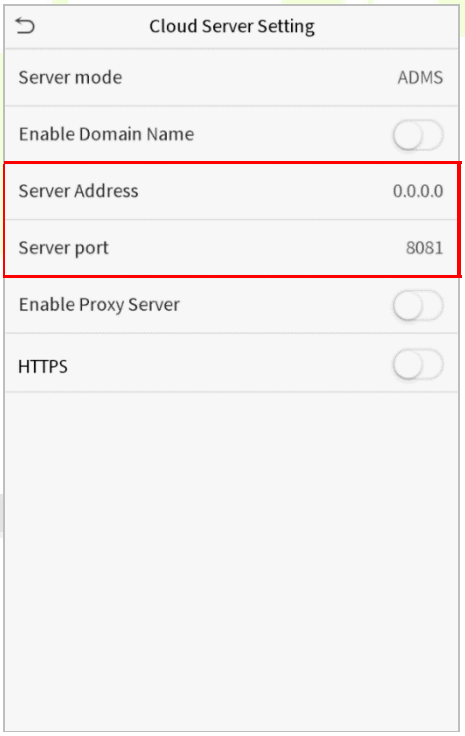
- **Lado do Dispositivo**

1. Toque em **COMM. > Ethernet** no menu principal para definir o endereço IP e o gateway do dispositivo. (Observação: O endereço IP deve ser capaz de se comunicar com o servidor ZKBioAccess MTD, de preferência no mesmo segmento de rede que o endereço do servidor)
2. No **menu principal**, clique em **COMM. > Configuração do Servidor em Nuvem** para definir o endereço e a porta do servidor.

   Endereço do servidor: Defina o endereço IP do servidor ZKBioAccess MTD.

   Porta do servidor: Defina a porta do servidor como a do ZKBioAccess MTD (O padrão é 8088).





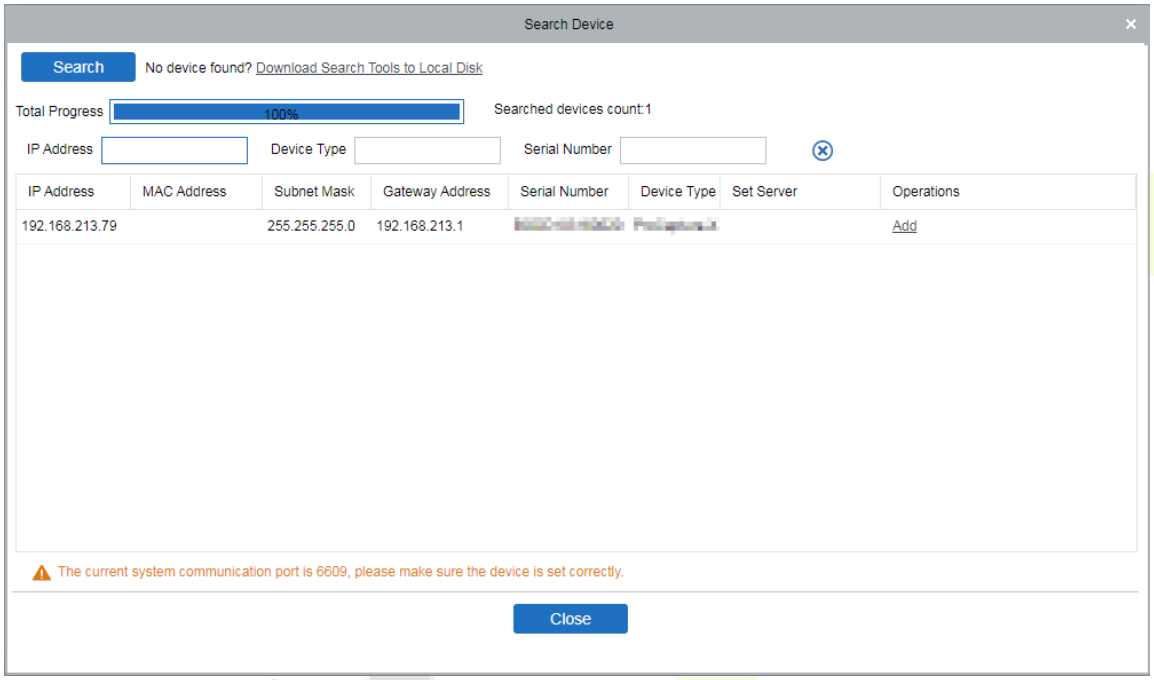
- **Software Side**

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

15.2 Adicionar Dispositivo no Software

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

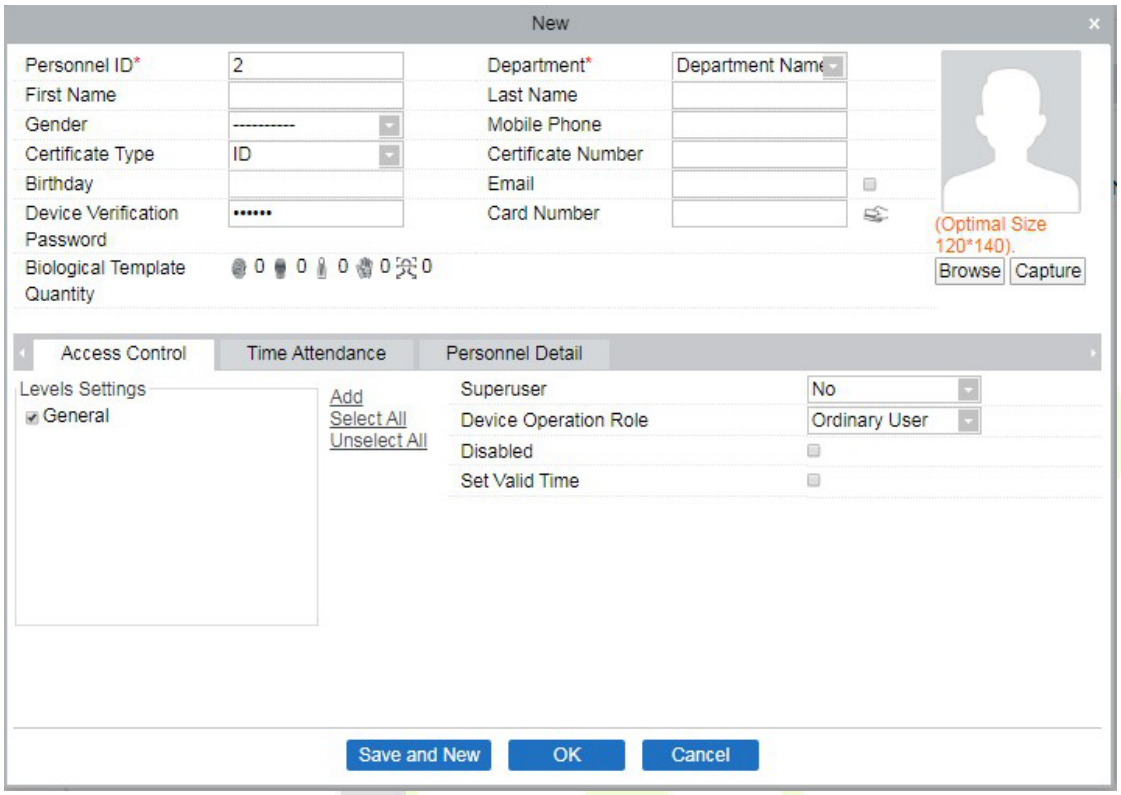
1. Clique em **Controle de Acesso > Dispositivo > Buscar Dispositivo** para abrir a interface de busca no software.
2. Clique em **Buscar** e ele mostrará "**Buscando...**"
3. Após a busca, a lista e o número total de controladores de acesso serão exibidos.



4. Clique em **Adicionar** na coluna de operação, uma nova janela será exibida. Selecione o tipo de ícone, Área e Adicionar ao Nível em cada menu suspenso e clique em "OK" para adicionar o dispositivo.

15.3 Adicionar Pessoal no Software

1. Clique em **Pessoal > Pessoa > Novo**

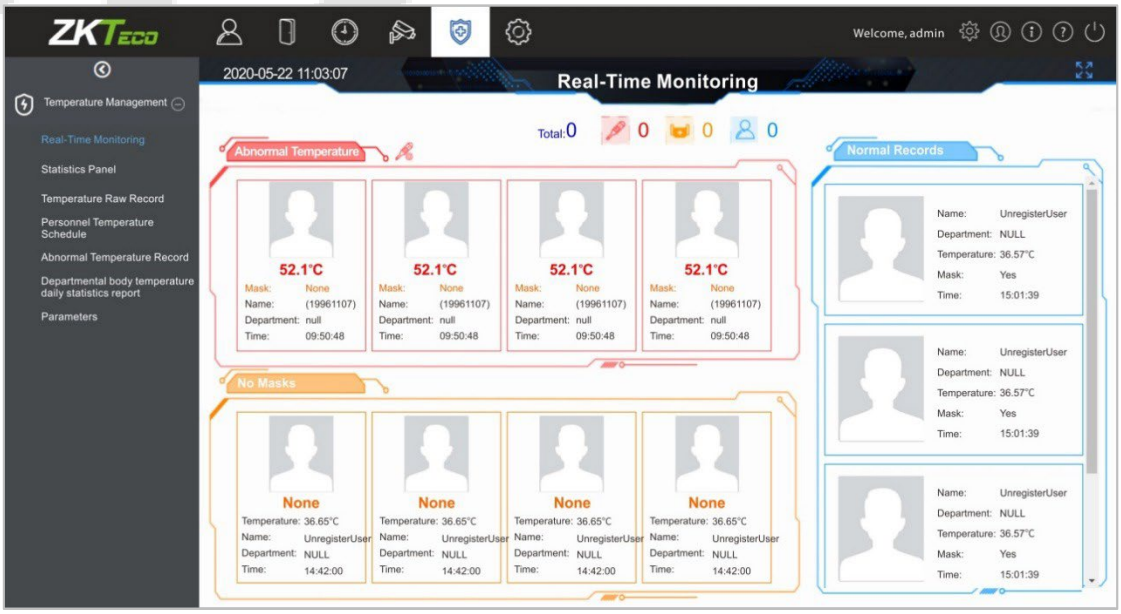


2. Preencha todos os campos obrigatórios e clique em **OK** para registrar um novo usuário.

3. Clique em **Acesso > Dispositivo > Controle de Dispositivo > Sincronizar Todos os Dados com os Dispositivos** para sincronizar todos os dados no dispositivo, incluindo os novos usuários

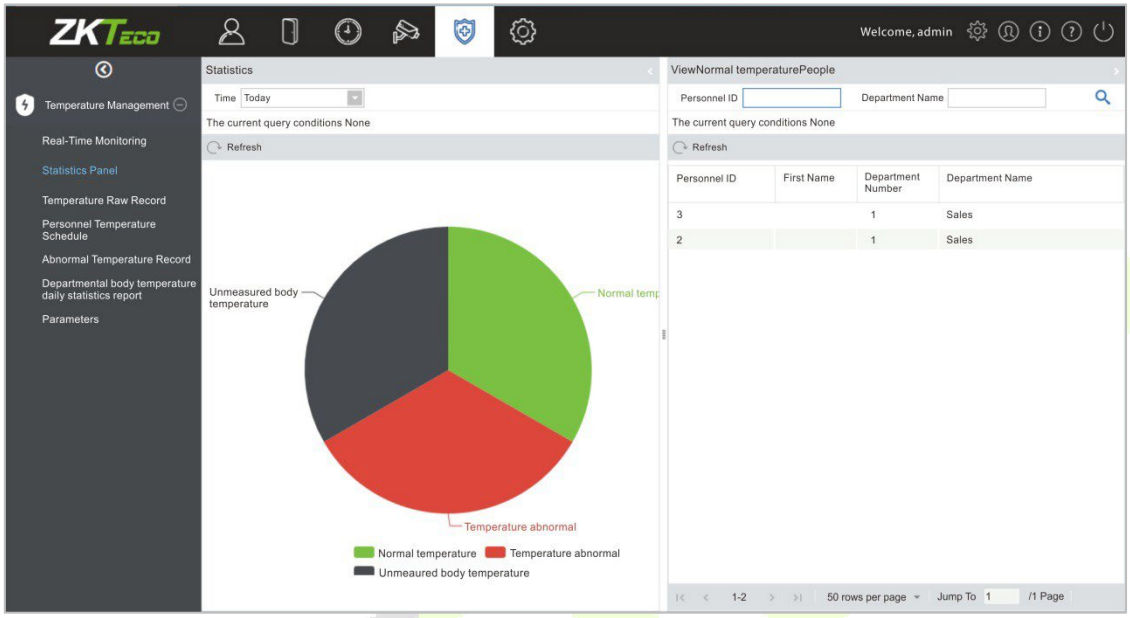
15.4 Monitoramento em Tempo Real no Software ZKBioAccess MTD

1. Clique em **Prevenção > Epidemia > Detecção de Temperatura > Monitoramento em Tempo Real** para visualizar todos os eventos das pessoas presentes em Anormalidade de Temperatura, Sem Máscara e Registros Normais.



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

2. Clique em **Epidemia > Gerenciamento de Temperatura > Painel de Estatísticas** para visualizar a análise de dados estatísticos na forma de um gráfico de pizza e ver as pessoas com temperatura normal, temperatura anormal e temperatura não medida. Além disso, informações detalhadas das pessoas podem ser vistas à direita ao clicar na categoria específica no gráfico de pizza.



Nota: Para outras operações específicas, consulte o Manual do Usuário do ZKBioAccess MTD.

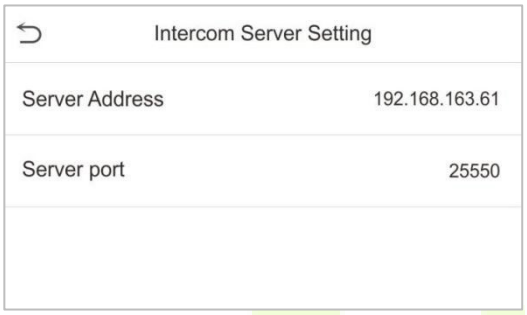
16 Conectando ao Software ZKBio Talk.★

Baixe e instale o software ZKBio Talk. Em seguida, mantenha as configurações de parâmetros do software ZKBioSecurity inalteradas para as configurações relevantes. (Consulte as Configurações da Função de Videoporteiro LAN).

Aqui estão os passos para conectar o ZKBio Talk ao software ZKBioSecurity:

1. Primeiramente, altere os parâmetros no dispositivo.

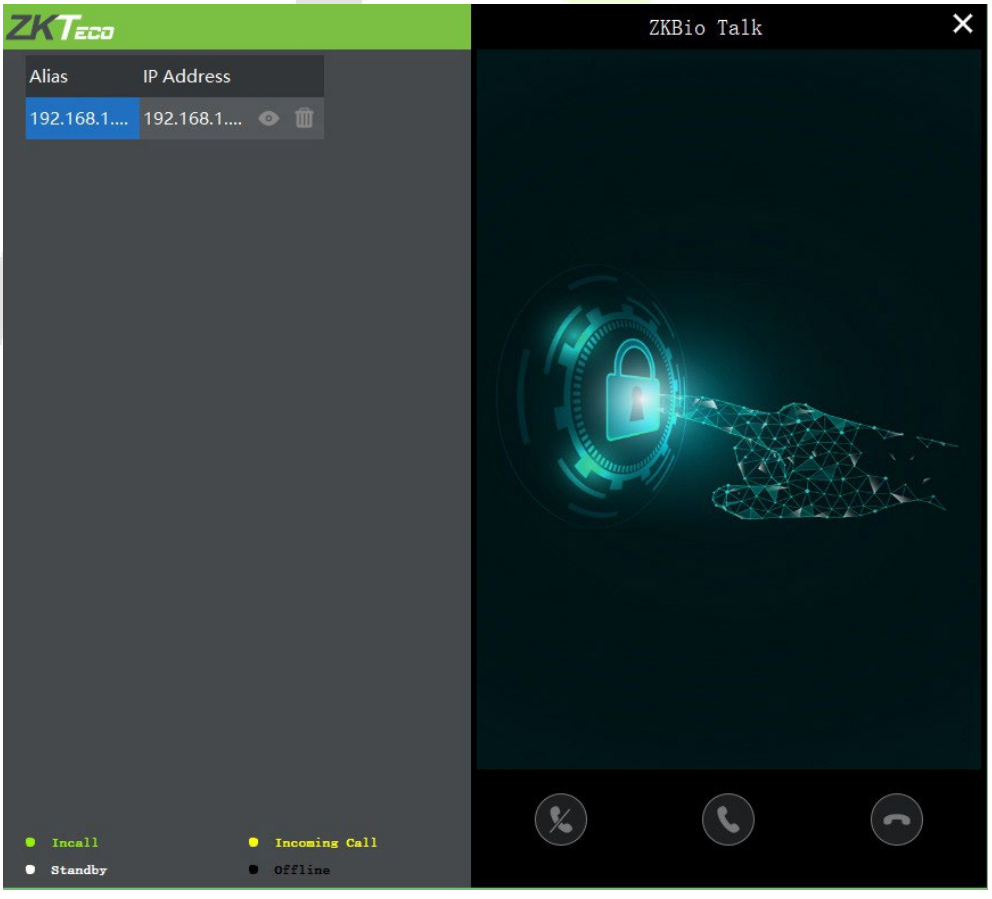
   Toque em ☰ **> Sistema > Parâmetros de intercomunicação por vídeo > Configuração do servidor de intercomunicação** no dispositivo para alterar o endereço do servidor e a porta do servidor, conforme mostrado na figura a seguir.



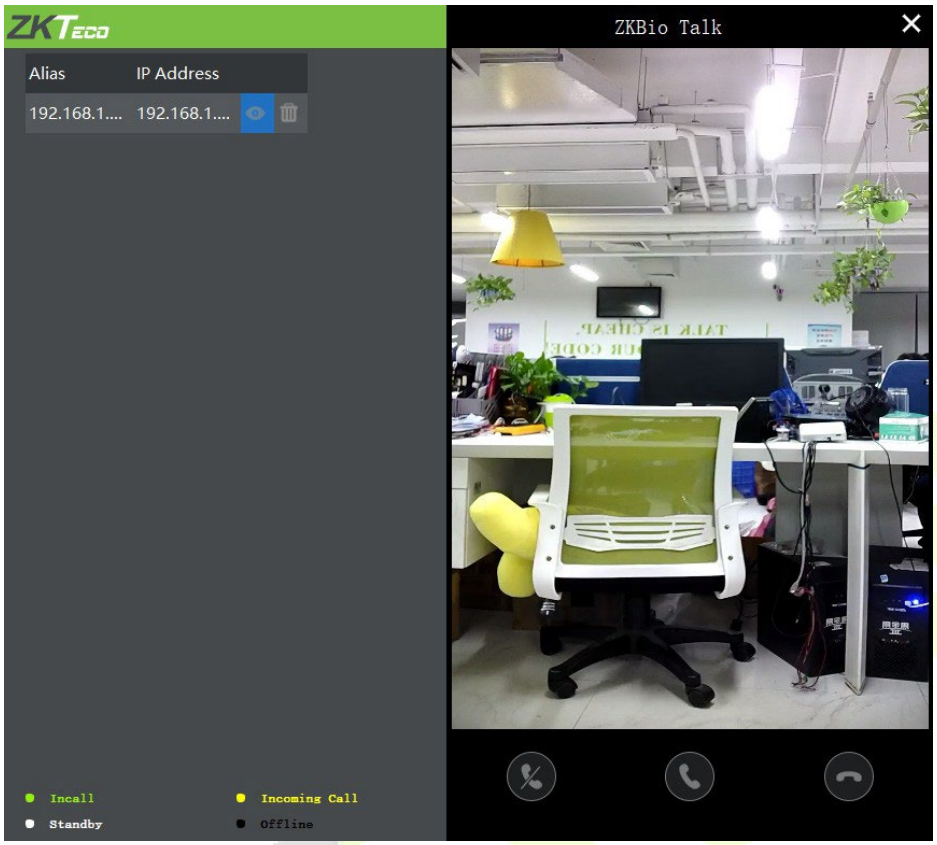
   Endereço do Servidor: Insira o endereço IP atual da instalação do servidor.

   Porta do Servidor: A porta padrão do servidor é 25550.

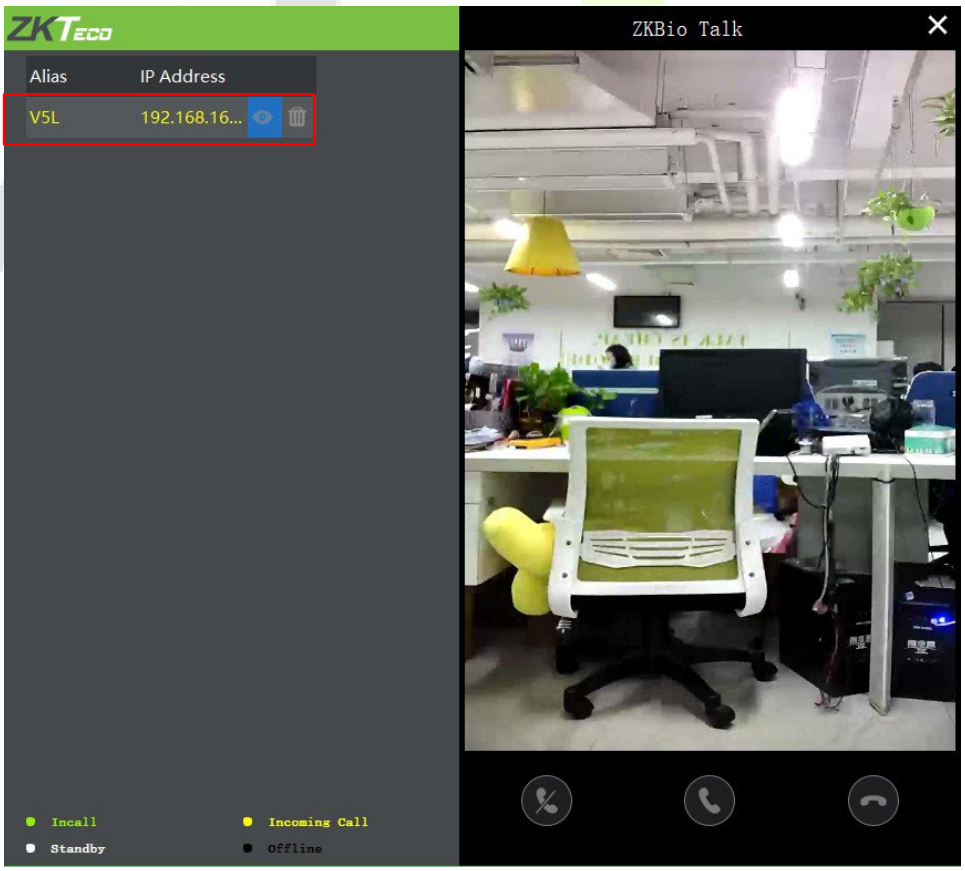
2. Clique duas vezes no ícone para abrir o software ZKBio Talk. Quando os parâmetros de intercomunicação por vídeo do lado do dispositivo estiverem configurados corretamente, o dispositivo automaticamente exibirá a lista de dispositivos à esquerda, conforme mostrado na figura a seguir.



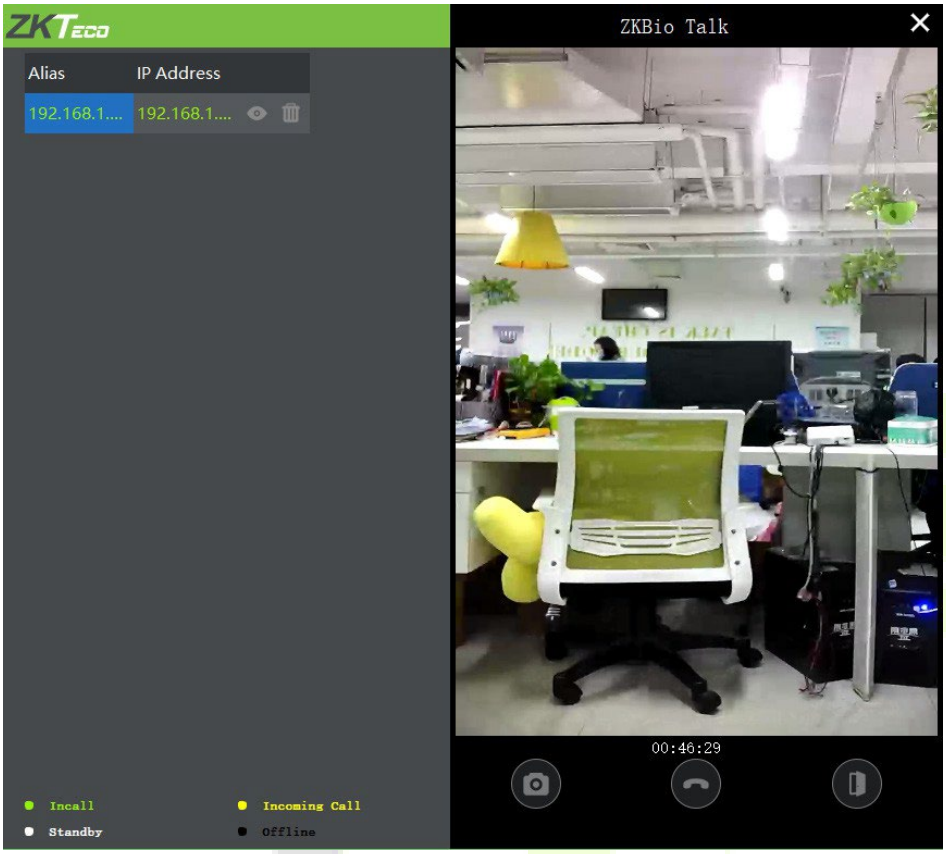
3. Um usuário pode clicar em para visualizar o vídeo à direita. Ao clicar no ícone ou , o usuário pode fechar a tela de visualização. Nenhuma ação é executada ao clicar em .



4. Quando um usuário clica no ícone na interface principal do dispositivo para fazer uma ligação, a interface do software exibe o endereço IP do dispositivo que está fazendo a chamada em amarelo.



5. Quando o usuário clica no ícone para atender a chamada, o endereço IP é exibido em verde durante a chamada. A duração da chamada também é exibida logo acima do ícone.



Descrição da Função:

	Esta é a tecla de Snapshot, usada para tirar uma captura de tela
	Esta é a tecla de Abertura Remota, usada para abrir a porta remotamente. O tempo de acionamento de travamento padrão é de 5 segundos.

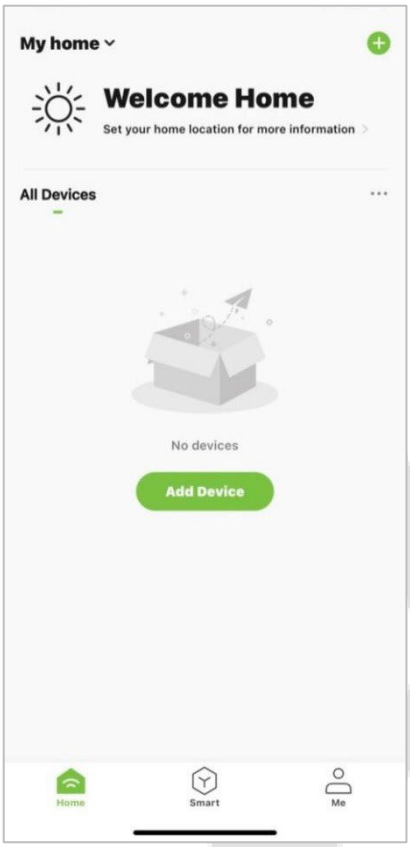
Observação: Somente os dispositivos offline podem ser removidos.

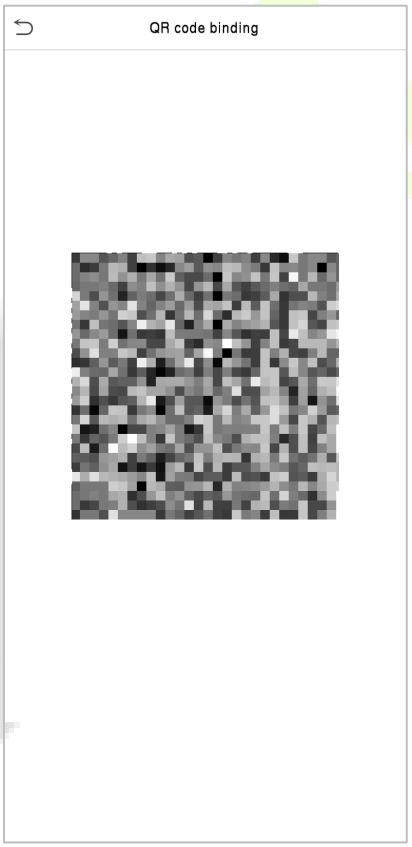
17 Conectando ao aplicativo ZSmart★

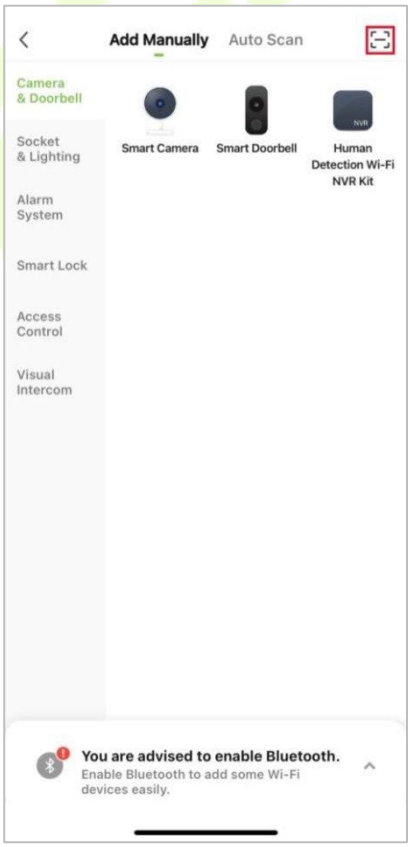
17.1 Adicionando dispositivo no aplicativo ZSmart

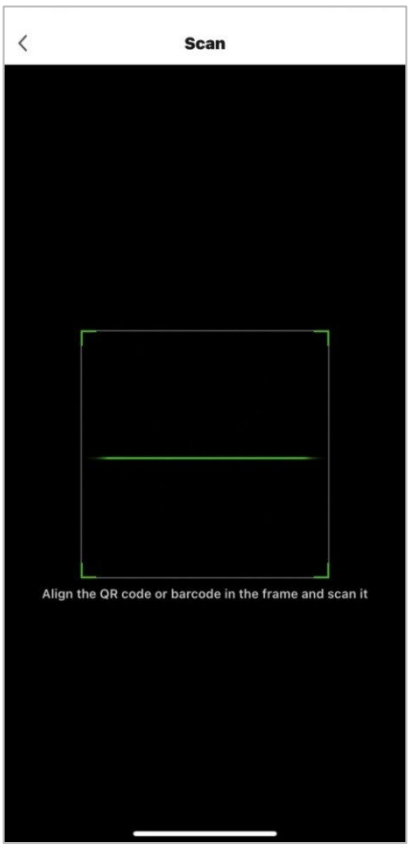
Após baixar e instalar o aplicativo ZSmart em seu celular, crie uma conta de usuário inicialmente com seu endereço de e-mail. Após criar a conta de usuário, faça o login no aplicativo e clique no ícone Add Device ou ⊕ no canto superior direito da tela para adicionar um dispositivo. O processo é o seguinte:

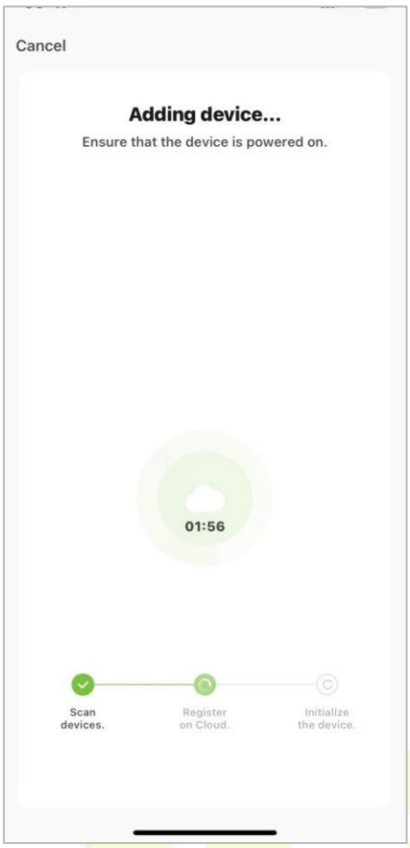
1. Clique em **Adicionar Dispositivo** na página inicial.
2. Toque em **Sistema > Parâmetros de Intercomunicação por Vídeo > Associação por Código QR** para mostrar o código QR do dispositivo.
3. Clique no ícone ⊡ no canto superior direito

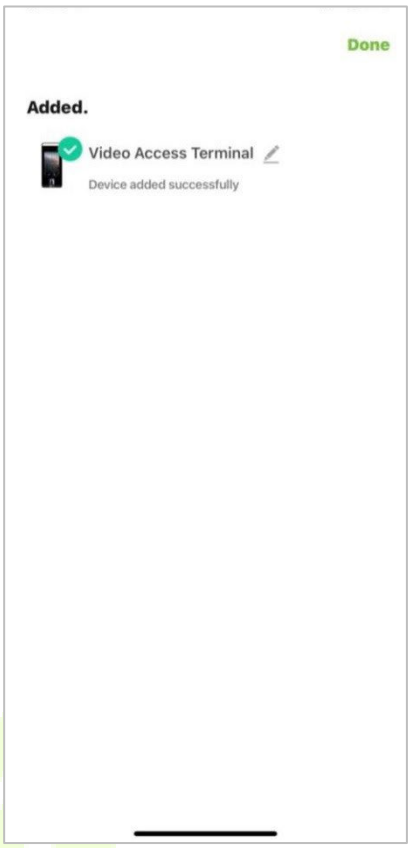






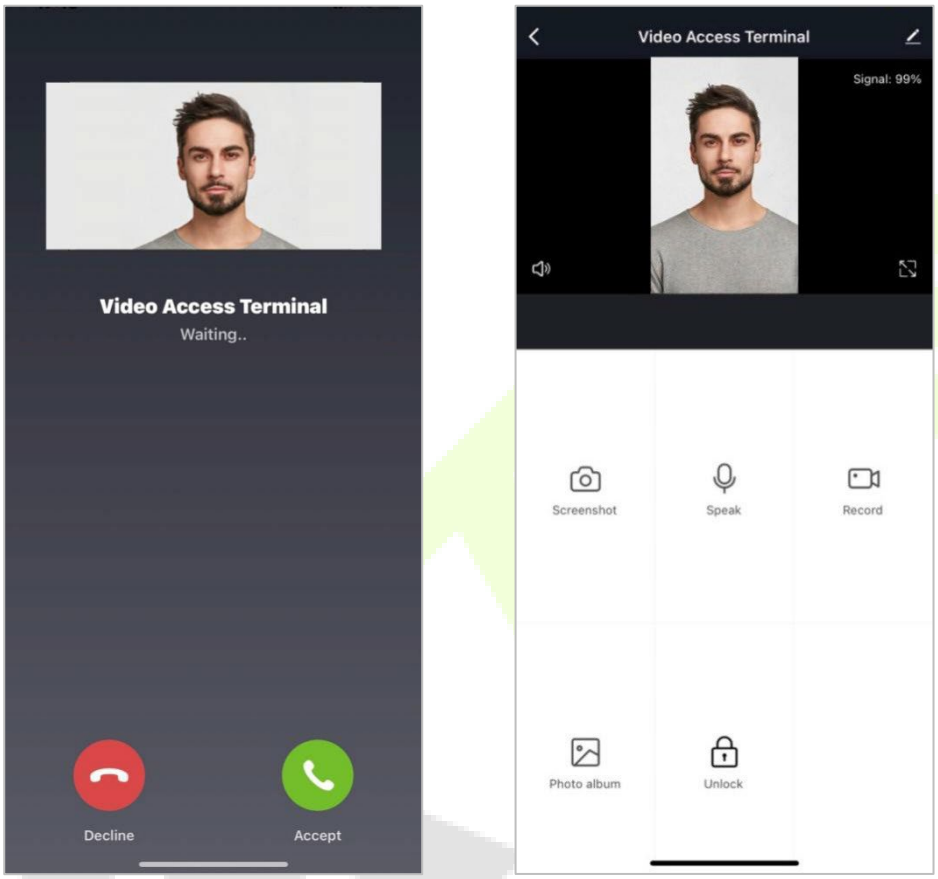






17.2 Conexão de Interfone com Vídeo

Os visitantes pressionam o botão no dispositivo para fazer uma chamada e o telefone irá tocar. O usuário pode aceitar ou recusar a chamada. Depois que o usuário aceita a chamada, abrirá a interface de vídeo do interfone. Digite a senha para destrancar a porta.



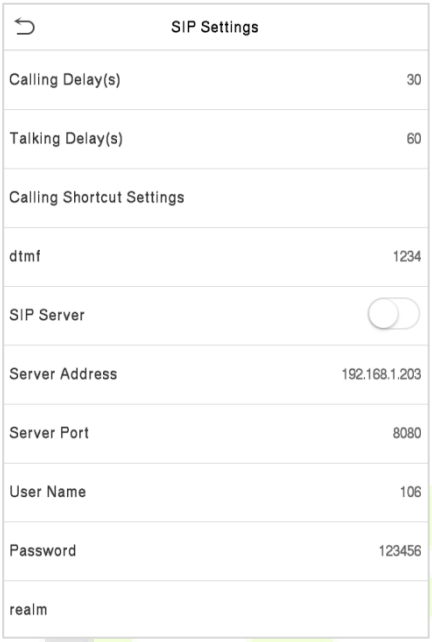
Parâmetro	Descrição
Captura de Tela	Clique para tirar uma captura de tela.
Falar	The icon becomes blue when click it, and you can talk to the device at this time.
Gravar	Clique para gravar um vídeo.
Galeria de Fotos	Visualizar e deletar capturas de tela e vídeos gravados.
Destrancar	Clique para abrir a porta remotamente. O registro de abertura é salvo em **Eu** > **Centro de Mensagens**.

Observações: Para outras operações específicas, consulte o Manual do Usuário do ZSmartAPP.

18 Conectando ao SIP ★

Toque em Parâmetros de Intercomunicação por Vídeo na interface do Sistema para acessar as configurações de parâmetros de monitoramento.

Observação: Essa função precisa ser usada com a estação interna Vpad A2.

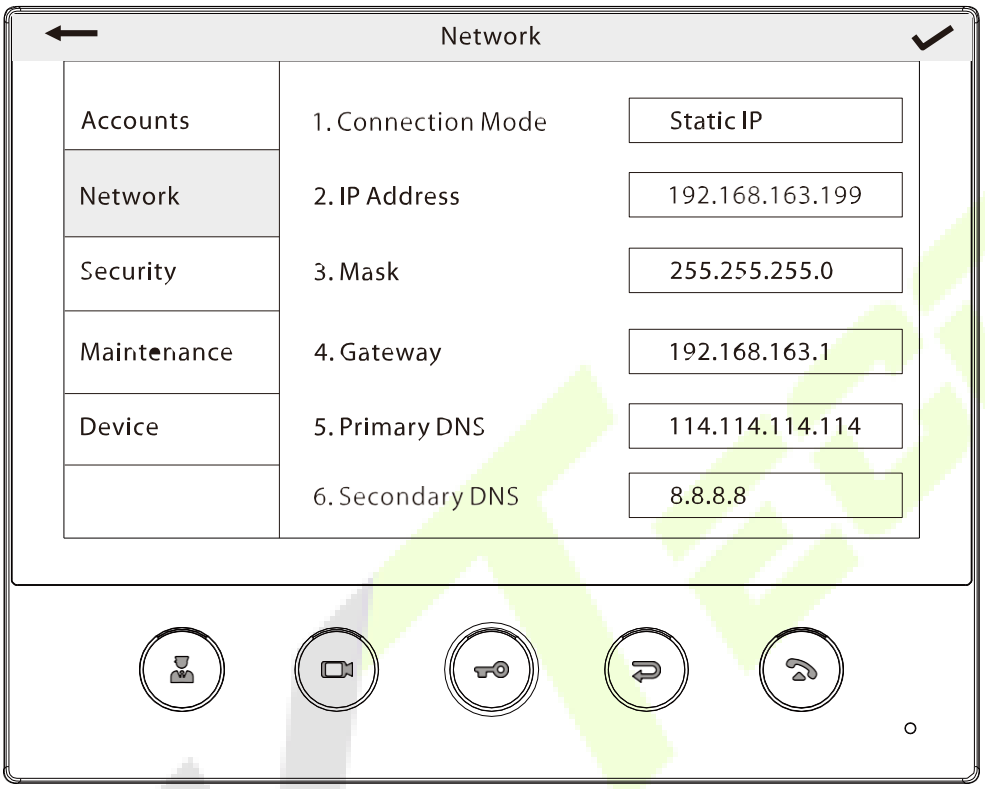


Função	Descrição
Atraso na Chamada (s)	Defina o tempo de chamada, valor válido de 30 a 60 segundos.
Limite da Conversa (s)	Defina o tempo de intercomunicação, valor válido de 60 a 120 segundos.
Configurações de Atalho de Chamada	Você pode definir uma tecla de atalho para chamar a estação interna rapidamente, sem precisar inserir o endereço IP da unidade interna toda vez.
dtmf	O valor do WebServer é o mesmo que o valor do DMTF no dispositivo para destravá-lo.
Servidor SIP	Selecione se deseja habilitar o endereço do servidor. Depois de conectado ao servidor, você pode chamá-lo ao inserir o nome de usuário da estação interna.
Endereço do Servidor	Digite o endereço do servidor.
Porta do Servidor	Digite a porta do servidor.
Nome de Usuário	Digite o Nome de Usuário do servidor.
Senha	Digite a senha do servidor.
Domínio	Digite o domínio do servidor.

O SpeedFace-V5L e a estação interna para realizar a intercomunicação de vídeo possuem dois modos, respectivamente, LAN e servidor SIP.

18.1 Uso da Rede Local

Configure o endereço IP na estação interna. **Toque em Menu** > **Avançado** > **Rede** > **1. Rede** > **1. IPv4.**



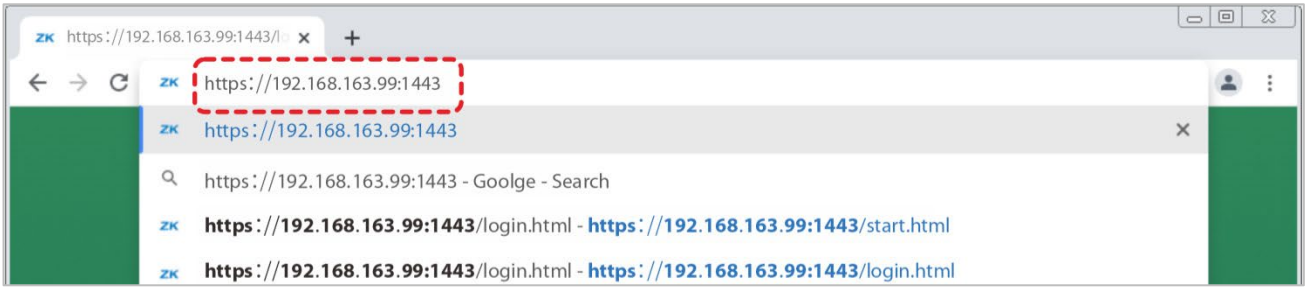
Observação: Na rede local (LAN), os endereços IP da estação interna e do SpeedFace-V5L devem estar no mesmo segmento de rede.

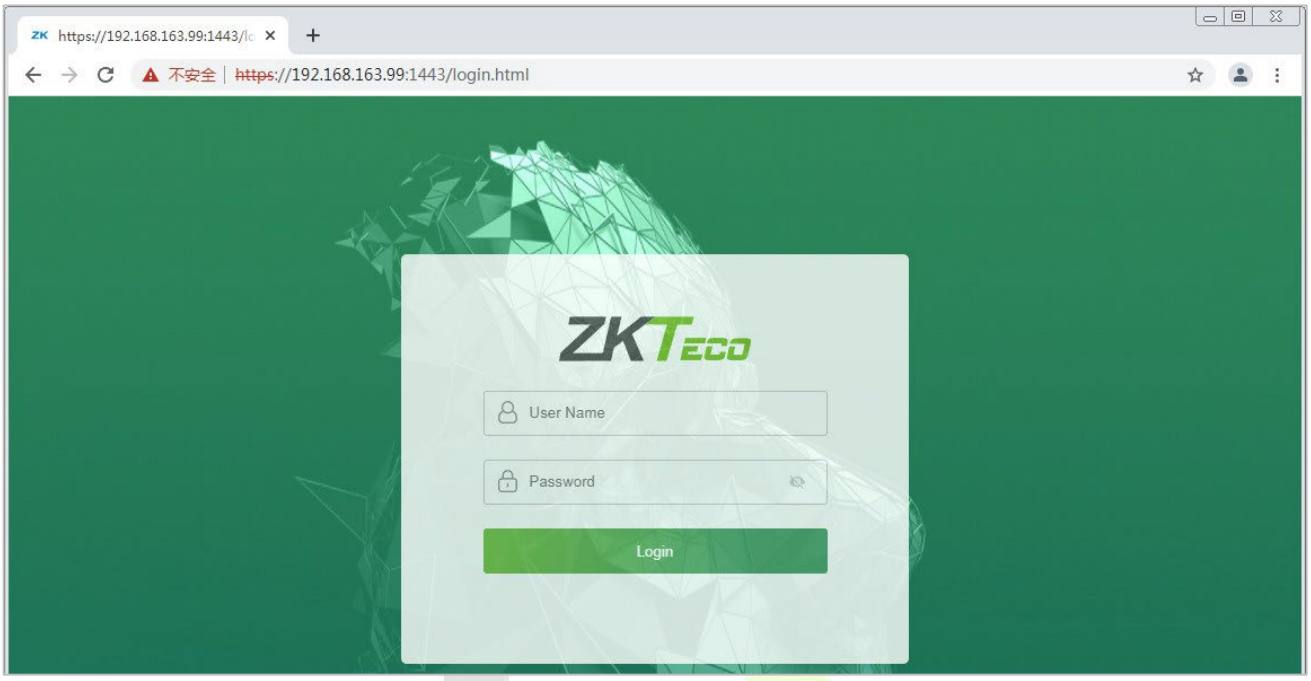
- **Digite diretamente o endereço IP da estação interna.**

Uma vez que a estação interna esteja configurada na rede, a função de intercomunicação por vídeo pode ser realizada tocando no ícone na tela do SpeedFace-V5L e inserindo o endereço IP da estação interna na interface de salto.

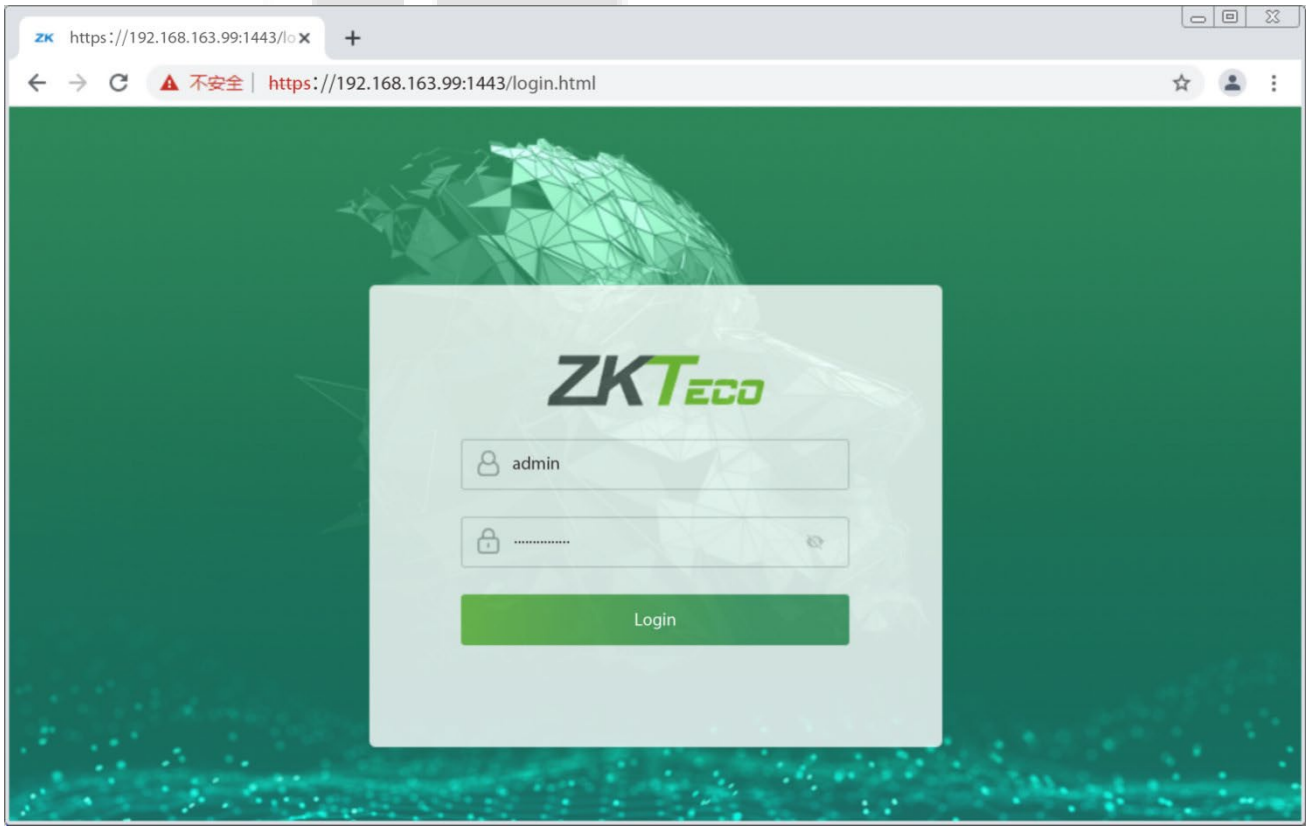
- **Personalizar as Opções de Status de Presença**

1. Use o seu navegador para inserir o endereço para fazer login no WebSever, o endereço é o Endereço IP Serial:1443, por exemplo: https://192.168.163.99:1443.

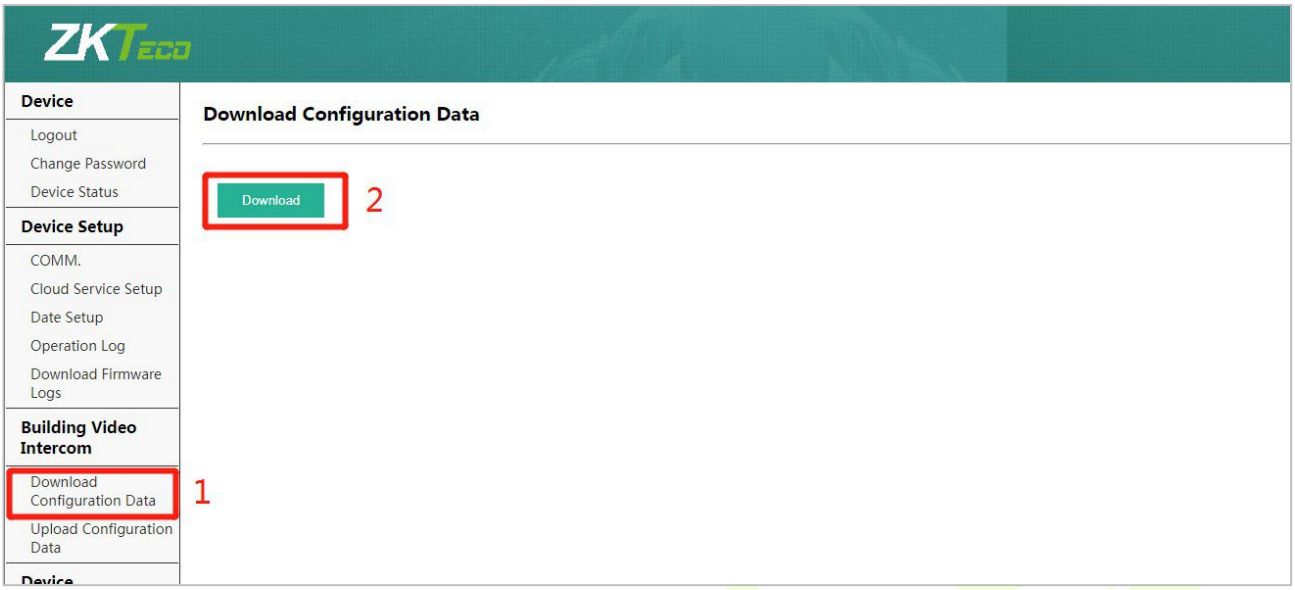




2. Digite a conta e a senha do WebSever, a conta inicial é: admin, senha: admin@123.



3. Baixe os dados de configuração.



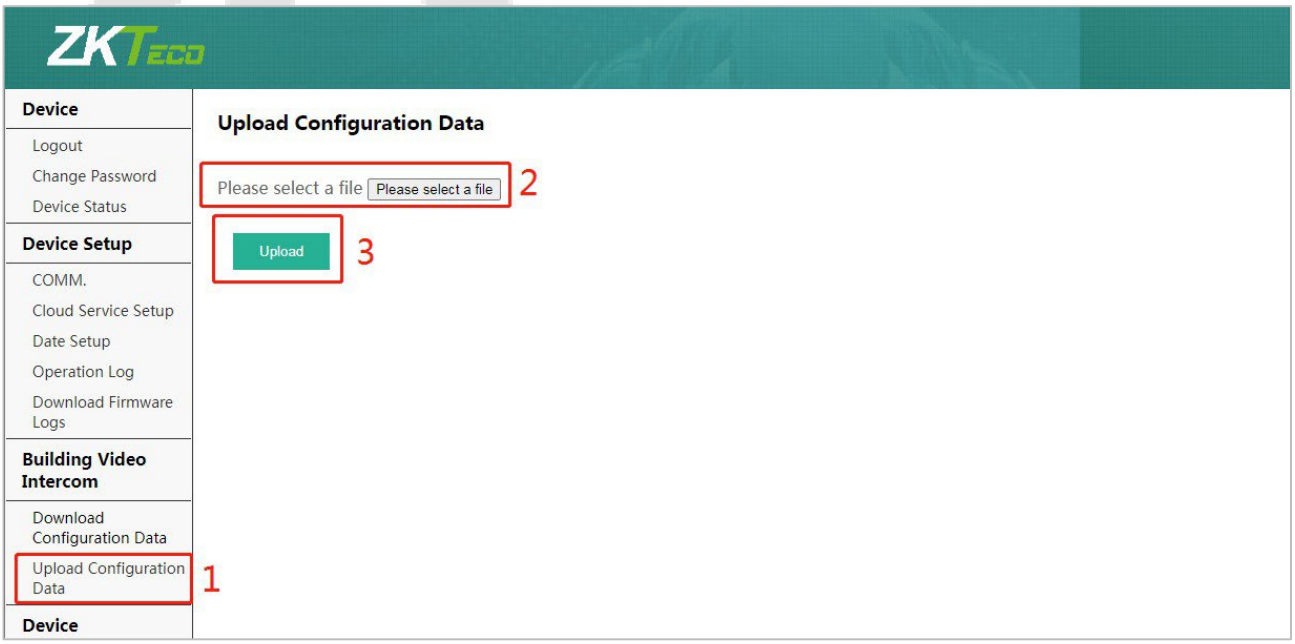
4. Digite o endereço de comunicação da estação interna e o número do dispositivo no formulário para download.

	A	B	C	D	E
1	IP Address	Subnet Mask	Gateway	Dialing Number	
2	192.168.163.199	255.255.255.0	192.168.163.1	9	
3	192.168.163.205	255.255.255.0	192.168.163.1	3	
4	192.168.163.103	255.255.255.0	192.168.163.1	4	
5	192.168.163.104	255.255.255.0	192.168.163.1	5	
6	192.168.163.105	255.255.255.0	192.168.163.1	6	
7					

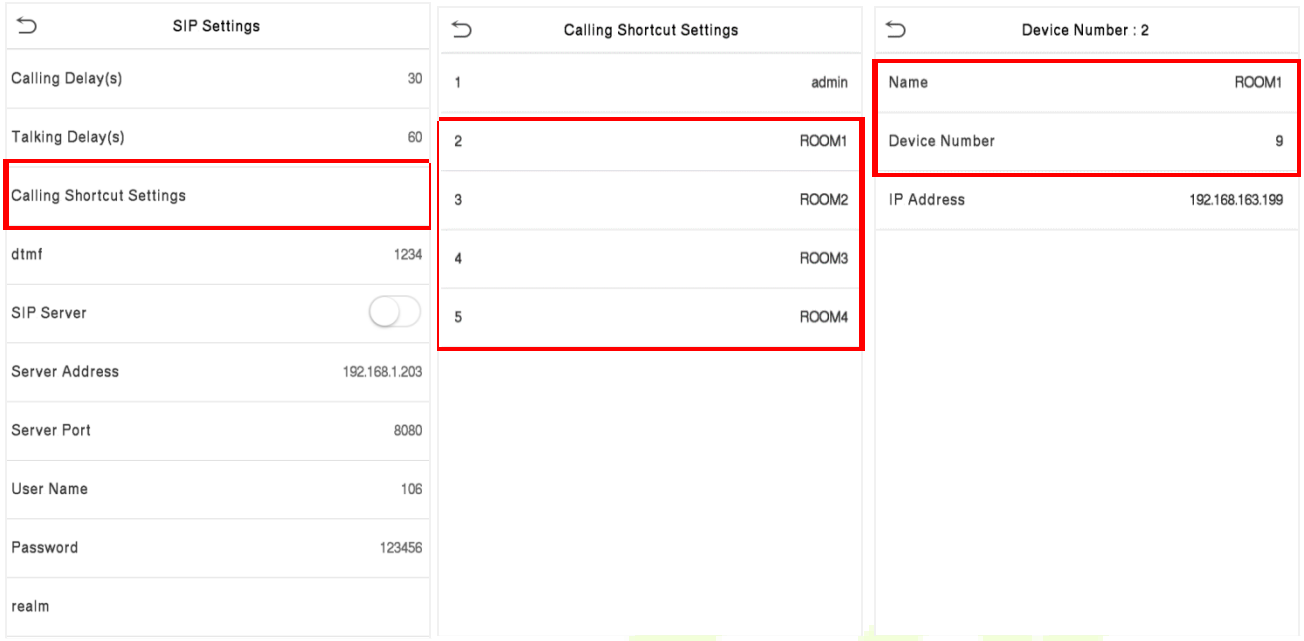
Endereço IP / Máscara de Sub-rede / Gateway: Deve ser o mesmo que a estação interna a ser conectada.

Número de Discagem: Personalize o número da estação interna, você pode inserir o valor no SpeedFace-V5L para chamar a estação interna rapidamente para a intercomunicação por vídeo.

5. Assim que o formulário estiver configurado e salvo, faça o upload do formulário de configuração no WebServer.



6. No SpeedFace-V5L, toque em **Configurações de Atalho de Chamad**a, selecione qualquer item exceto admin e insira as informações do formulário que você acabou de fazer o upload.



Função	Descrição
Nome	Você pode personalizar qualquer caractere (suporta chinês, inglês, números, símbolos, etc.) que será exibido na página de chamada.
Número do Dispositivo	É o número de discagem nos dados de configuração, você pode inserir o valor no SpeedFace-V5L para chamar a estação interna rapidamente para a intercomunicação por vídeo.
Endereço IP	Após inserir o número de discagem, o endereço IP correspondente nos dados de configuração será emparelhado automaticamente.

- **Nome**

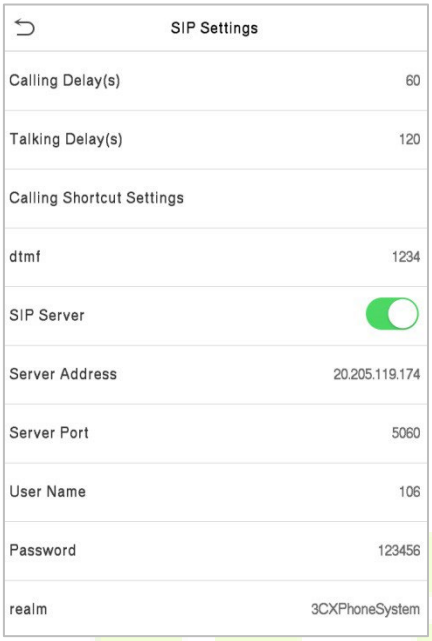
Você pode então tocar em 199 nas opções de status de ponto para implementar diretamente a intercomunicação por vídeo.

- **Número do Dispositivo**

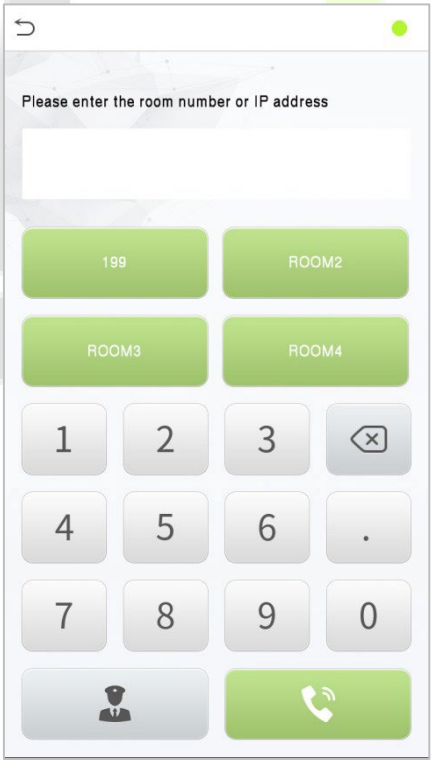
Digite o número do dispositivo na tela de chamada.

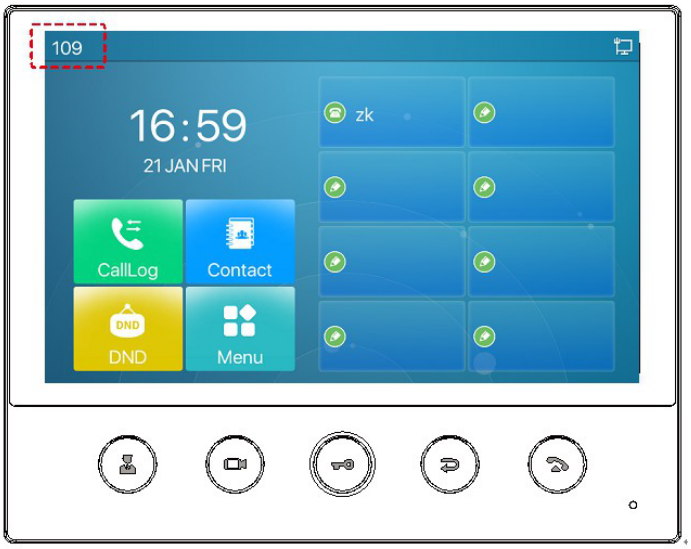
18.2 Servidor SIP

No SpeedFace-V5L, toque em **Servidor SIP**, após o dispositivo ser reiniciado, insira os parâmetros relacionados ao servidor, como mostrado abaixo:



Uma vez que o SIP estiver configurado corretamente, um ponto verde aparecerá no canto superior direito da página de chamada para indicar que o SpeedFace-V5L está conectado ao servidor. Você pode chamar o nome da conta da estação interna.





Para obter detalhes sobre a operação e o uso da estação interna, consulte o manual do usuário da estação interna.

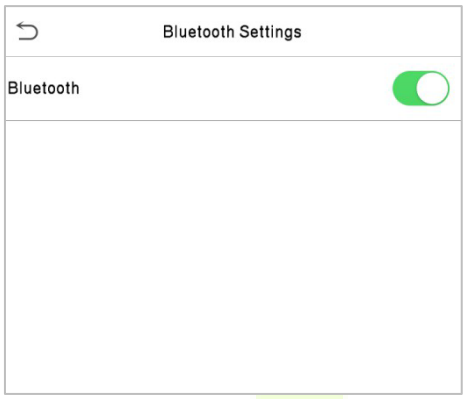
18.3 Recursos SIP

Versão do Firmware	3.5.34
Conexão SIP em ambiente LAN	Sim
Conexão SIP em ambiente NAT	Sim
Opções para configuração Stun	Sim
Opção para configuração de servidor SIP secundário	Sim
Opção para configurar servidor por domínio ou IP	Sim
Streaming de vídeo por ONVIF	Sim
Streaming de vídeo por RTSP	Sim
Botão de chamada SIP intuitivo na tela principal	Sim
Botão de chamada SIP flutuante na tela	Sim
Conexão de botão externo para chamada SIP	Sim
Configurações do botão SIP para chamar diretamente central ou digitando ramal	Sim
Configuração personalizada DTMF	Sim
Ajuste de codecs de áudio	Não
Ajuste de FPS e taxa de compressão de vídeo	Não
Configuração WEB do equipamento, incluindo SIP	Sim
Configuração de ajuste de volume	Sim
Autenticação facial durante chamada SIP	Sim
Ajuste do timeout da autenticação facial para voltar para a chamada SIP	Sim
Ajuste do tempo de espera quando "chamando"	Sim
Ajuste do tempo de chamada máximo	Sim
Equipamento receber chamada SIP	Sim
Chamadas de áudio e vídeo	Sim
Função para desabilitar chamadas de vídeo	Sim
Autenticar no servidor Voip UDP	Sim
Autenticar no servidor Voip TCP	Sim
Autenticar no servidor Voip TLS	Não
Conexão com Indoor Station (ZKTeco)	Não
Permite troca de número do ramal	Sim
Permite troca de IP servidor	Sim
SIP com rede Wi-Fi	Sim

19 Conectando ao Fechadura Bluetooth★

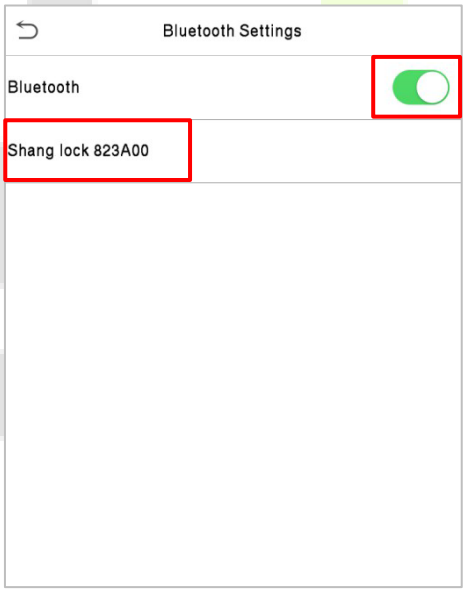
Através desta função Bluetooth, a fechadura Bluetooth pode ser vinculada ao dispositivo, e quando o usuário passa pela verificação no dispositivo ou insere o código correto da fechadura Bluetooth, a fechadura pode ser destrancada remotamente.

Toque em **Configurações Bluetooth** na interface de **Configurações de Comunicação** para configurar o Bluetooth.



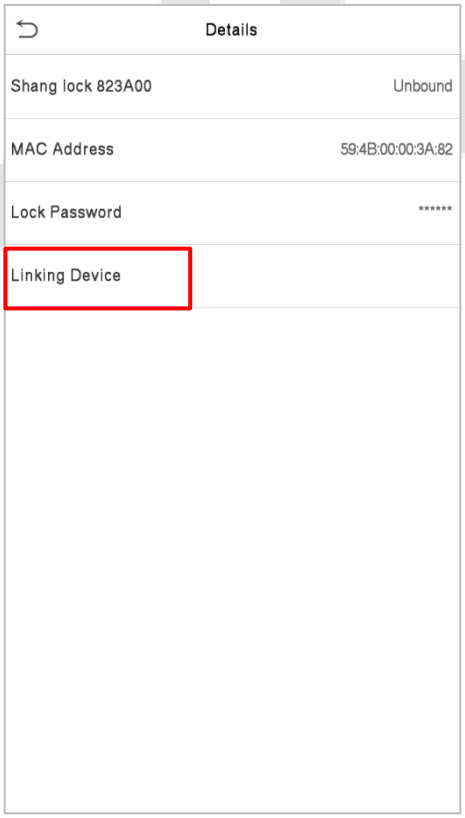
19.1 Vincular Dispositivo

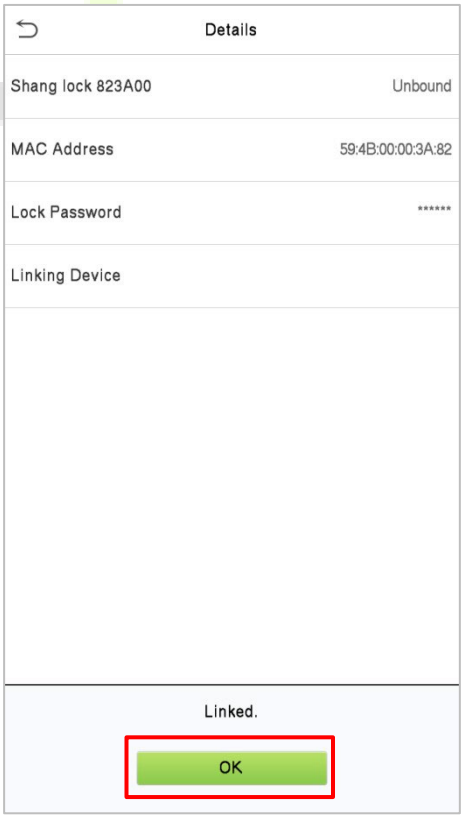
- Clique em **Bluetooth** para habilitar a função Bluetooth.
- Você precisa tocar no teclado da fechadura Bluetooth para acordar a fechadura, o dispositivo buscará através do Bluetooth e exibirá a fechadura Bluetooth a ser vinculada na interface de Configurações Bluetooth.



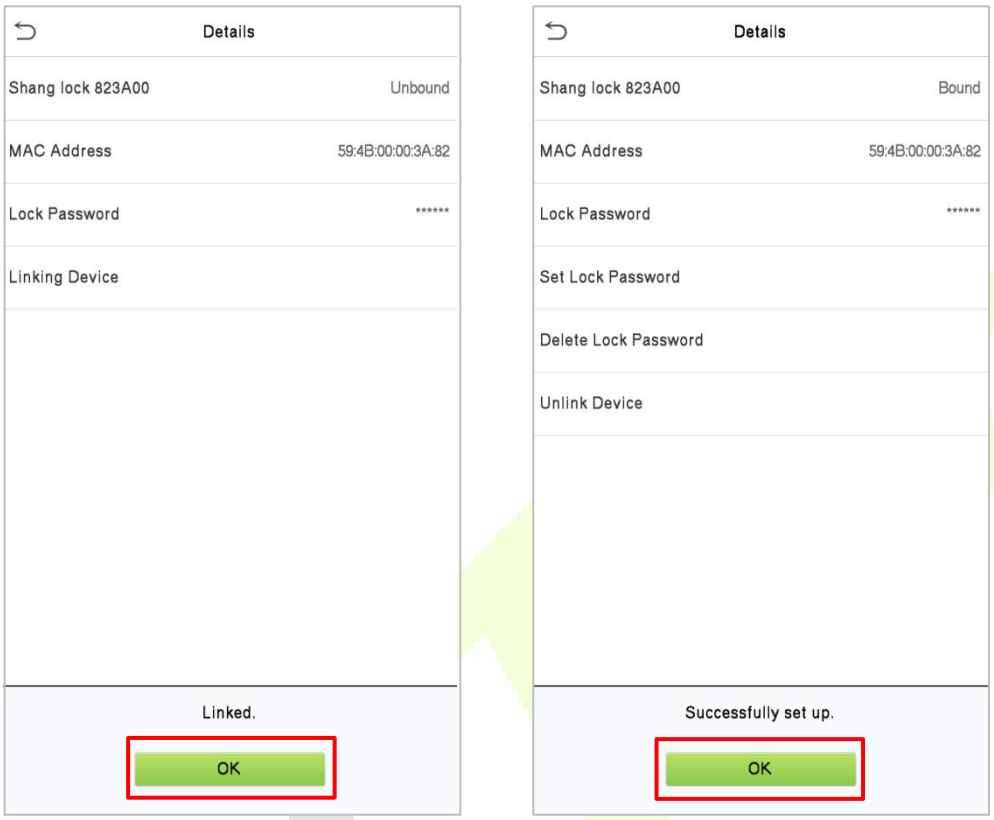
- Selecione a fechadura Bluetooth a ser vinculada, entre na interface de configuração de senha da fechadura.
- Por favor, digite uma nova senha de 6 a 9 dígitos, clique em **Confirmar** para salvar a senha e, em seguida, a interface exibirá **Desvinculada** após a conclusão.

- Selecione novamente a fechadura Bluetooth desvinculada para acessar a interface de Detalhes.
- Por favor, toque no teclado da fechadura Bluetooth para acordar o dispositivo primeiro e, em seguida, clique em **Vincular Dispositivo**. A fechadura Bluetooth emitirá um som de bip, e a interface exibirá um aviso de **Vinculado**, indicando que o dispositivo foi vinculado com sucesso.



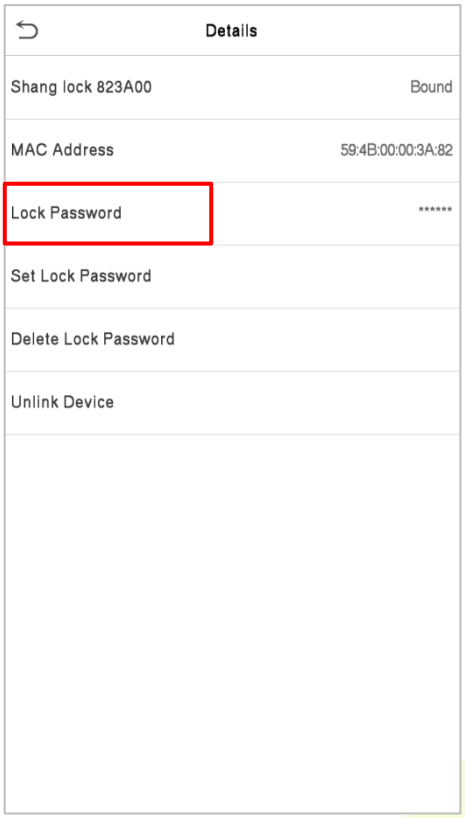


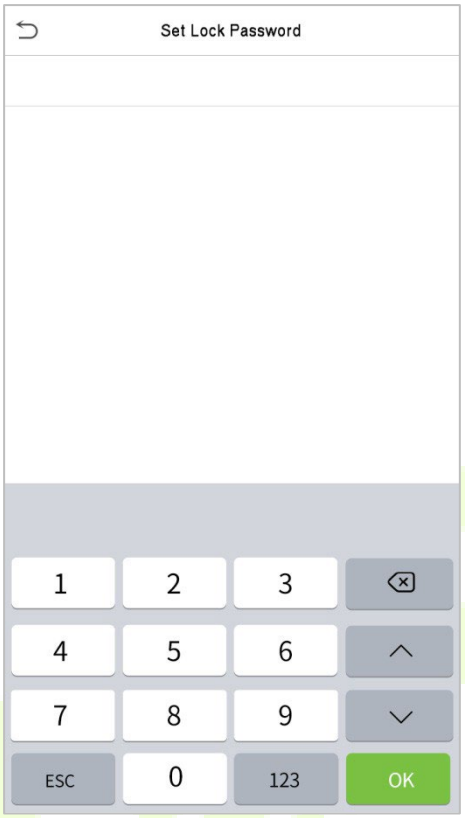
- Após clicar em **OK** na interface de vinculação bem-sucedida, o dispositivo sincronizará automaticamente a configuração da senha da fechadura para a fechadura Bluetooth. A fechadura Bluetooth emitirá um som de bip, e a interface do dispositivo exibirá um aviso de **Configuração realizada com** sucesso, indicando que o dispositivo foi configurado com sucesso.



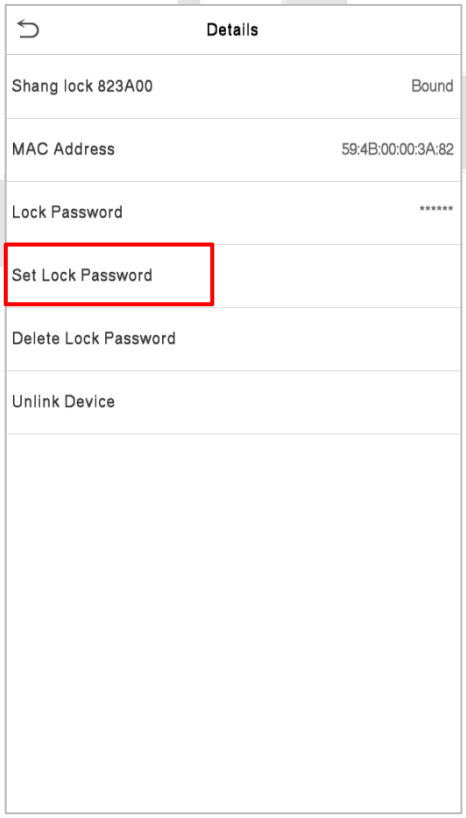
19.2 Alterar Senha

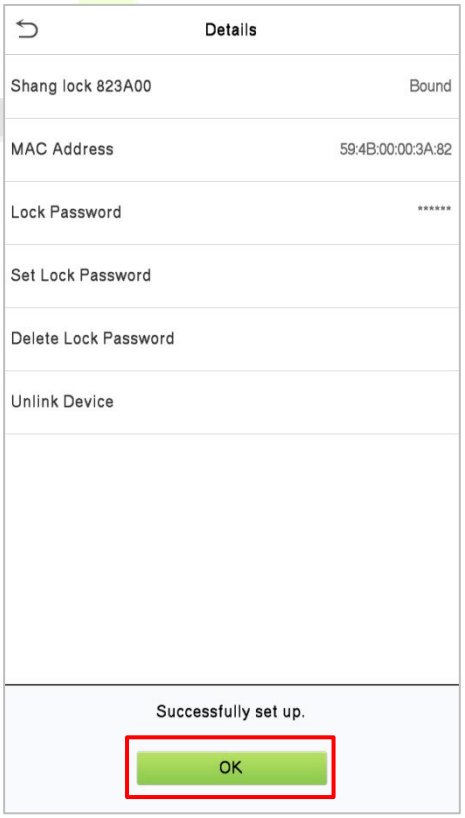
- Toque em **Comunicação > Configurações Bluetooth**, selecione a fechadura Bluetooth vinculada e entre na interface de **Detalhes**.
- Clique em **Senha da Fechadura** para abrir a interface de configuração de senha, digite a nova senha duas vezes e clique em **OK** para salvar.





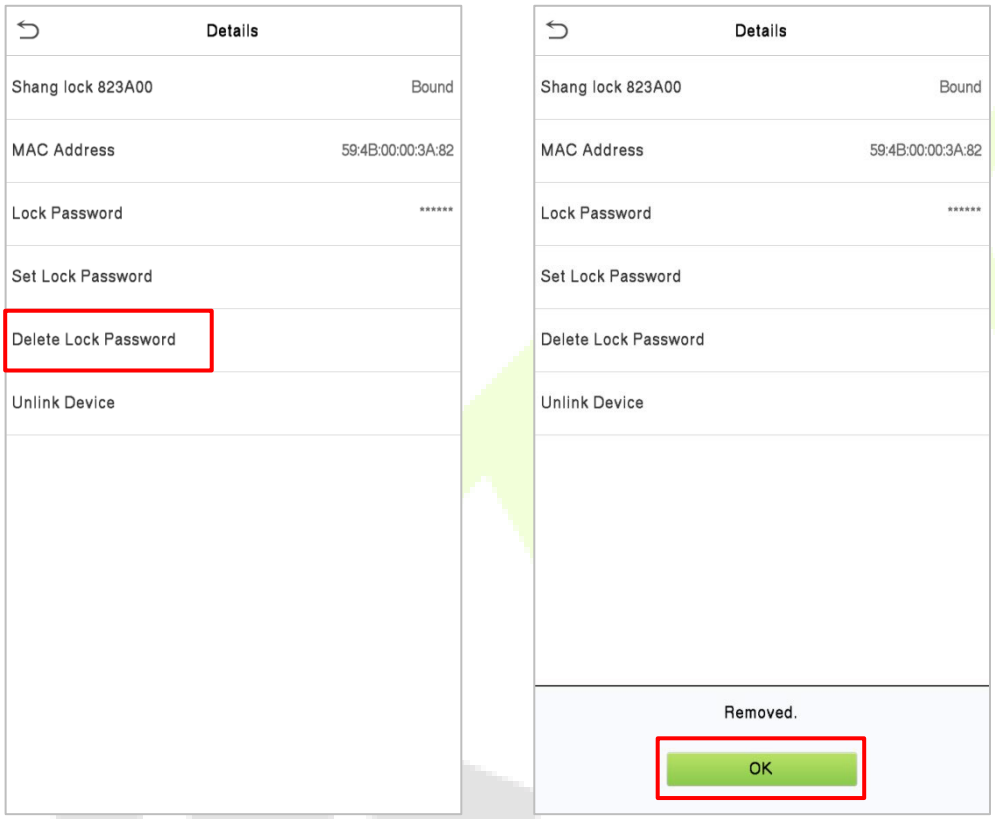
- Por favor, toque no teclado da fechadura Bluetooth para acordar o dispositivo primeiro e, em seguida, clique em **Definir Senha da Fechadura** para sincronizar a nova senha com a fechadura Bluetooth. A fechadura Bluetooth emitirá um som de bip, e a interface do dispositivo exibirá um aviso de **Configuração realizada com sucesso**, indicando que o dispositivo foi configurado com sucesso.





19.3 Excluir Senha

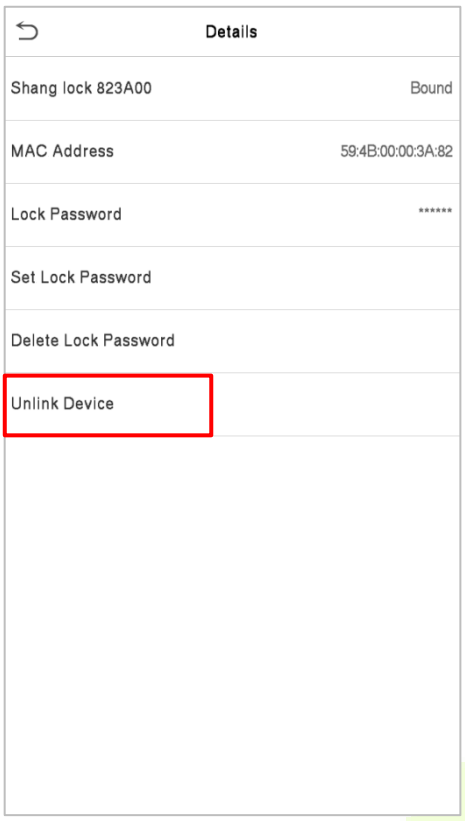
- Toque em **Com. > Configurações Bluetooth**, selecione a fechadura Bluetooth vinculada e entre na interface de Detalhes.
- Por favor, toque no teclado da fechadura Bluetooth para acordar o dispositivo primeiro e, em seguida, clique em **Excluir Senha da Fechadura**. A fechadura Bluetooth emitirá um som de bip, e a interface exibirá um aviso de **Removida**, indicando que a senha foi excluída com sucesso.

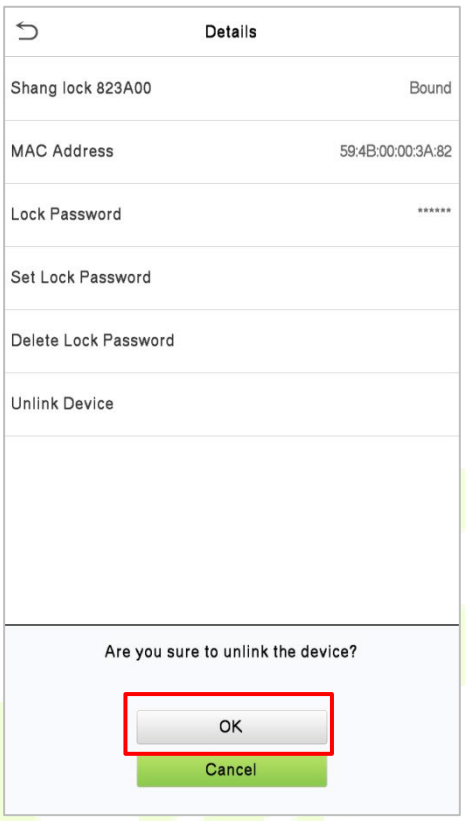


Note: After deleting the password, the Bluetooth lock will be restored to the original password: 123456.

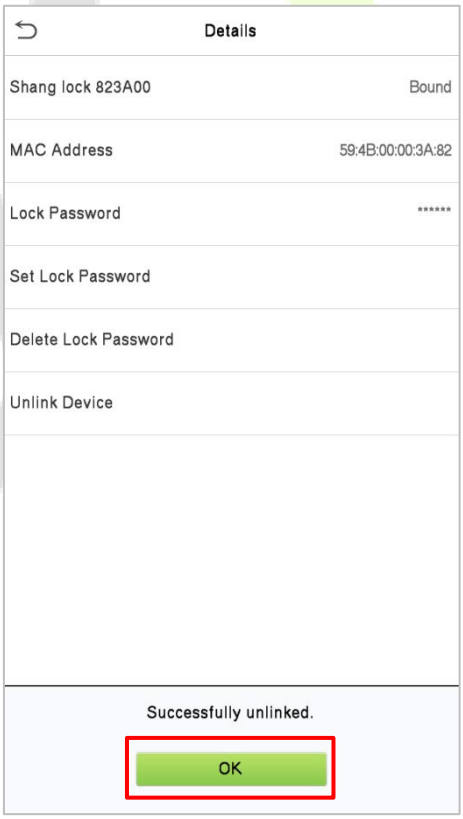
19.4 Desvincular Dispositivo

- Toque em **Comm. > Configurações Bluetooth**, selecione a fechadura Bluetooth vinculada e entre na interface de **Detalhes**.
- Por favor, toque no teclado da fechadura Bluetooth para acordar o dispositivo primeiro e, em seguida, clique em **Desvincular Dispositivo** na interface de **Detalhes**. A interface exibirá um aviso **Tem certeza de que deseja desvincular o dispositivo?**, então clique em **OK**.





- Após a fechadura Bluetooth emitir um som de bip, a interface exibirá um aviso de **Desvinculado com sucesso**, indicando que a desvinculação do dispositivo foi concluída.



Observação: Após o dispositivo ser desvinculado, a fechadura Bluetooth será restaurada para a senha original: 123456.

19.5 Desbloquear

Depois que o usuário vincula o cadeado Bluetooth ao dispositivo, o cadeado pode ser desbloqueado por meio de uma senha ou remotamente através do dispositivo.

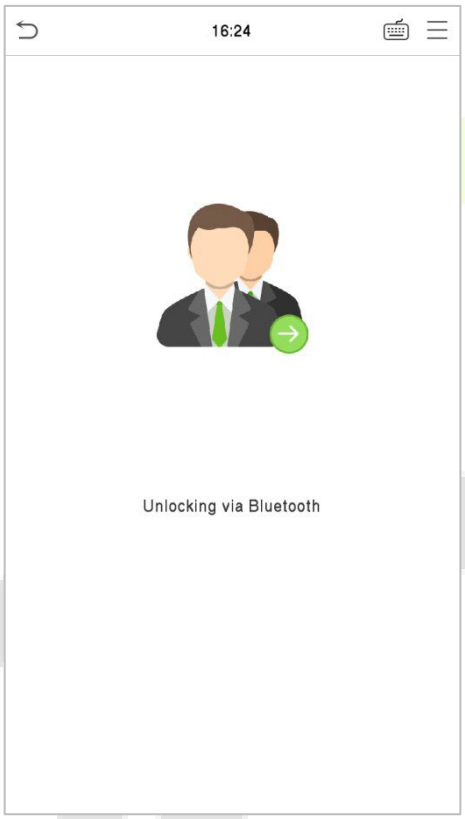
- **Desbloquear através de senha**

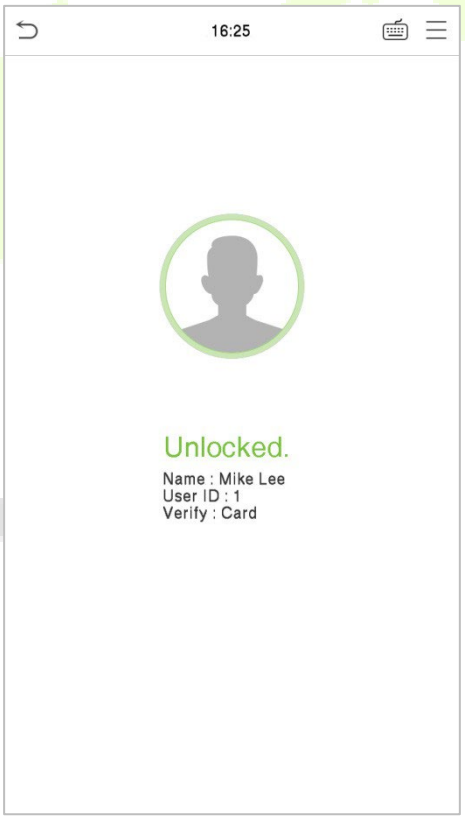
Após alterar a senha no dispositivo, você pode digitar essa senha no teclado do cadeado Bluetooth para desbloqueá-lo.

- **Desbloquear através do SpeedFace-V5L**

Após vincular o cadeado Bluetooth ao dispositivo, o cadeado Bluetooth pode ser aberto remotamente quando o usuário verifica o rosto, cartão, impressão digital ou senha no dispositivo.

Após a verificação, a interface exibe uma mensagem **Desbloqueando via Bluetooth** e o cadeado é aberto após 5 segundos.





Apêndice 1

Requisitos para a Coleta e Registro de Imagens de Rosto em Luz Visível em Tempo Real

1) É recomendado realizar o registro 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 registro.
4) Exponha adequadamente seu rosto e testa e não cubra o rosto e as sobrancelhas com o cabelo.
5) É recomendado mostrar uma expressão facial normal. (Um sorriso é aceitável, mas não feche os olhos ou incline a cabeça para qualquer direção).
6) São necessárias duas imagens para pessoas que usam óculos, uma com óculos e outra sem eles.
7) Não use acessórios como lenço ou máscara que possam cobrir a boca ou o queixo.
8) Por favor, posicione-se diretamente em direção ao dispositivo de captura e localize seu rosto na área de captura de imagem, conforme mostrado na imagem abaixo.
9) Não inclua mais de um rosto na área de captura.
10) É recomendada uma distância de 50cm a 80cm para capturar a imagem. (A distância é ajustável, dependendo da altura do corpo).

Requisitos para Dados de Imagens Digitais de Rosto em Luz Visível

A foto digital deve ter bordas retas, ser colorida, meio retratada, com apenas uma pessoa, e essa pessoa deve estar desimpedida 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

Rosto neutro ou sorriso simples e olhos naturalmente abertos são recomendados

Gesto e ângulo

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

Acessórios

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

Face

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

Formato de imagem

Deve estar em BMP, JPG ou JPEG.

Requisito de dados

Deve seguir os requisitos:

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

Apêndice 2

Política de Privacidade

Aviso:

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

I. Informações coletadas

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

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

II. Segurança e gerenciamento 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 você entra na interface do menu principal. Se ainda não definir o privilégio de administrador após receber o prompt do sistema, você deve estar ciente do possível risco de segurança (por exemplo, os dados podem ser modificados manualmente).
2. Todas as funções de exibição de informações biométricas estão desativadas em nossos produtos por padrão. Você pode escolher Menu > Configurações do sistema para definir se deseja exibir as informações biométricas. Se você habilitar essas funções, assumimos que você está ciente dos riscos de segurança especificados na política de privacidade.
3. Apenas seu ID de usuário é exibido por padrão. Você pode definir se deseja exibir outras informações de verificação do usuário (como Nome, Departamento, Foto, etc.) sob o privilégio de Administrador.

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

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

III. Como 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 verificáveis, excluiremos essas informações o mais rápido possível.

IV. Outros

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

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

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