Manual do usuário

SpeedFace M4

Data: Fevereiro de 2023

Versão: 1.1 Português

Acerca do Manual

Este manual apresenta as operações do SpeedFace M4.

Todas as figuras apresentadas são meramente ilustrativas. As figuras neste manual podem não ser exatamente consistentes com os produtos reais.

Índice

DECLARAÇÃO DE SEGURANÇA DE DADOS

Como fornecedor de produtos inteligentes, talvez precisemos conhecer e coletar algumas de suas informações pessoais para melhor auxiliá-lo no uso de nossos produtos e serviço. Assim sendo, trataremos sua privacidade com cuidado de acordo com nossa Política de Privacidade.
Por favor, leia e entenda completamente todos os regulamentos da política de proteção de privacidade e pontos-chave que aparecem no dispositivo antes de usar nossos produtos.
Como usuário do produto, você deve cumprir as leis e regulamentos aplicáveis relacionados à proteção de dados pessoais ao coletar, armazenar e usar dados pessoais, incluindo, entre outros, tomar medidas de proteção para dados pessoais, tais como realizar gerenciamento de direitos para dispositivos, fortalecer a segurança física de cenários de aplicação de dispositivos e assim por diante.

MEDIDAS DE SEGURANÇA

As instruções abaixo visam garantir que o usuário possa usar o produto corretamente para evitar perigos ou perdas materiais. As seguintes precauções são para manter os usuários seguros e evitar qualquer dano. Por favor, leia atentamente antes da instalação.
⚠ O descumprimento das instruções pode causar danos ao produto ou lesões físicas (pode até causar a morte).

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

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

Apenas altere os controles definidos nas instruções de operação. O ajuste inadequado dos controles pode causar danos e envolver um técnico qualificado para retornar o dispositivo à operação normal. Não conecte vários dispositivos a um único adaptador de energia, pois a sobrecarga do adaptador pode causar superaquecimento e risco de incêndio.

7. **Peças de reposição** - Quando forem necessárias peças de reposição, os técnicos de manutenção devem usar apenas peças de reposição fornecidas pelo fornecedor. Substitutos não autorizados podem resultar em queimaduras, choques ou outros perigos.
8. **Verificação de segurança** - Após a conclusão do serviço ou reparo na unidade, peça ao técnico para realizar verificações de segurança para garantir a operação adequada do dispositivo.
9. **Fonte de alimentação** - Opere o sistema apenas com a fonte de alimentação indicada. Se o tipo de fonte de alimentação a ser usado não estiver explicito, entre em contato com seu revendedor.
10. **Raios** -Para-raios externos podem ser instalados para proteção contra tempestades elétricas. Os dispositivos devem ser instalados em áreas com acesso limitado.

Segurança elétrica

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

Segurança da Operação

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

Nota:

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

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

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

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

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

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

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

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

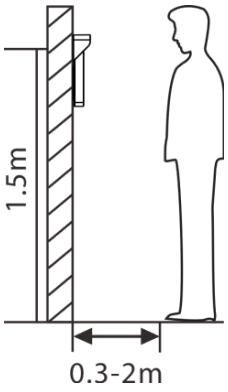
Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

1 Instruções de Uso

Antes de entrar nos recursos do dispositivo e suas funções, é recomendável estar familiarizado com os fundamentos abaixo.

1.1 Posição em Pé, Postura e Expressão Facial

Distância recomendada



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

Postura em pé e expressão facial recomendadas

Nota: Mantenha sua expressão facial e postura de pé natural durante o cadastro ou autenticação.

1.2 Cadastro de Palma

Posicione a palma da mão na área de coleta de forma que a palma fique paralela ao dispositivo.

Certifique-se de manter espaço entre os dedos.

Nota:

1) Posicione a palma da mão a 30-50 cm do dispositivo.

2) Posicione a palma da mão na área de coleta de forma que a palma fique paralela ao dispositivo.

3) Certifique-se de manter espaço entre os dedos.

4) Por favor, evite luz solar direta quando utilizando o reconhecimento de palma em ambientes externos. De acordo com testes em laboratório, o reconhecimento de palma é mais eficaz quando a intensidade da luz não ultrapassa 10.000 lux.

1.3 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

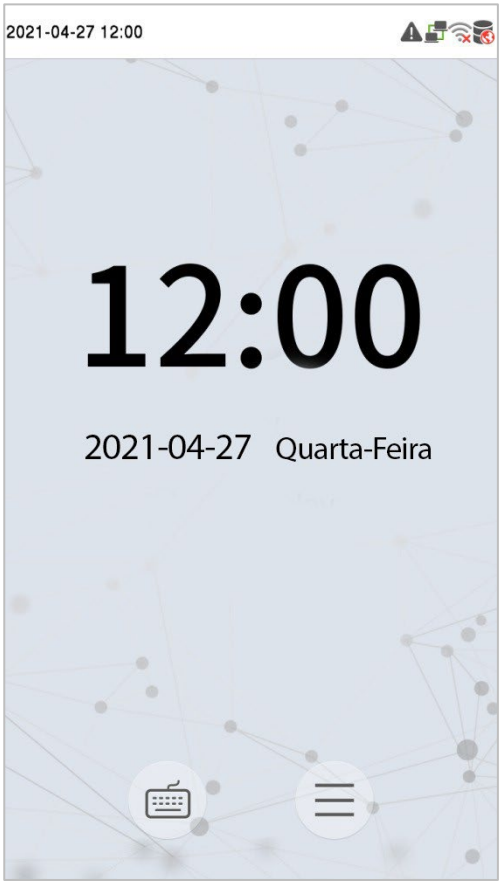
- Ao cadastrar uma face, mantenha uma distância de 40 cm a 80 cm entre o dispositivo e a face.
- Tenha cuidado para não mudar sua expressão facial. (Ex.: sorriso, etc.)
- Se você não seguir as instruções na tela, o cadastro de face pode demorar mais ou pode falhar.
- Tenha cuidado para não cobrir os 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:



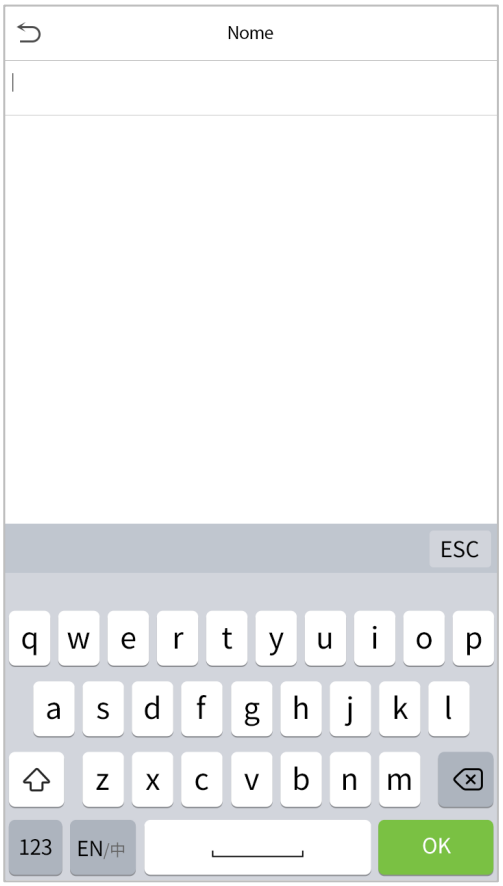
Nota:

1) Clique em para autenticar com ID do usuário.

2) Quando não houver um super administrador cadastrado no dispositivo, clique em para acessar o menu.

3) Depois de configurar o super administrador no dispositivo, será necessário autenticar com o Super Administrador para entrar nas funções do menu.

1.5 Teclado Virtual



Nota: 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.

1.6 Modo de autenticação

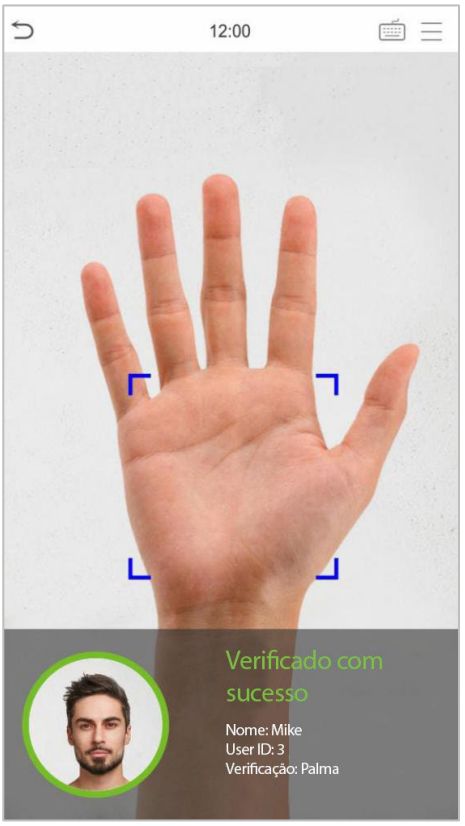
1.6.1 Autenticação de Palma

Modo de autenticação de Palma 1:N

Nesse modo de autenticação, o dispositivo compara a imagem da palma coletada com todos os dados da palma cadastrados no equipamento.

O dispositivo distingue automaticamente entre a palma da mão e o modo de verificação por face à medida que o usuário coloca a palma da mão na área de coleta.

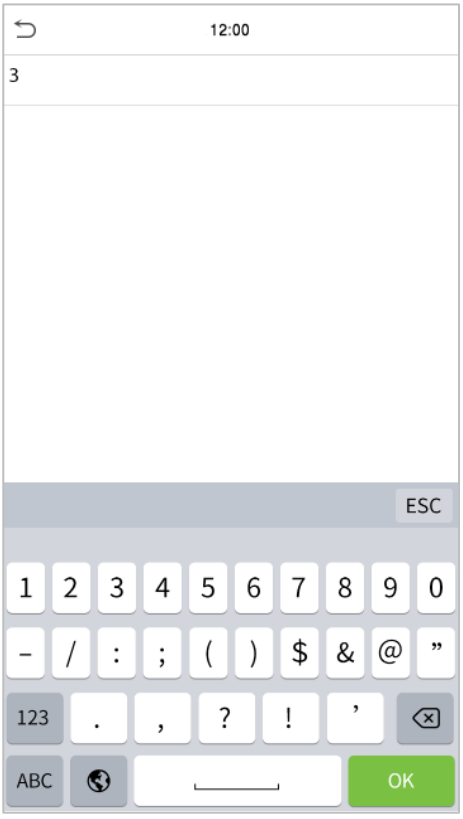
Em seguida, a imagem da palma é coletada e o dispositivo procura a imagem da palma com todas as palmas cadastradas e retorna uma se foi validada ou não.



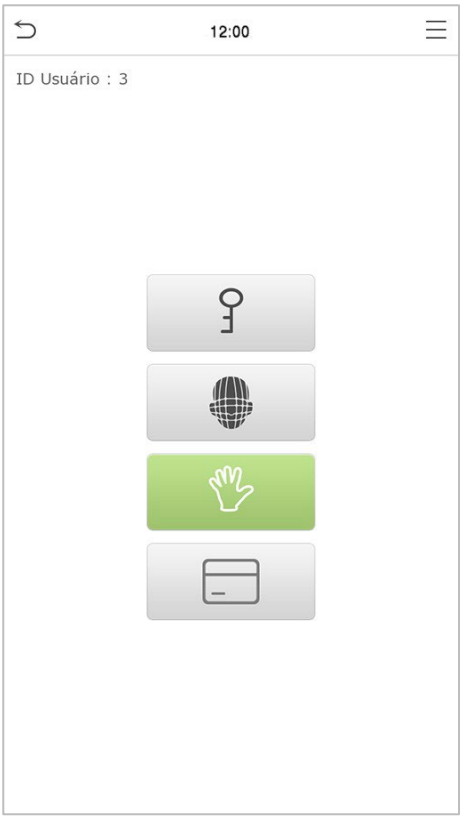
1:1 Modo de autenticação de Palma 1:1

Clique no botão na tela principal para entrar no modo de autenticação de palma 1:1,

1. Insira o ID do usuário e pressione [OK], conforme mostrado na imagem abaixo



Caso o usuário possua face, cartão e senha cadastrados além de sua palma e o método de autenticação estiver configurado para autenticação palma/ face/ cartão/ senha, a tela a seguir será exibida. Selecione o ícone para entrar no modo de autenticação da palma da mão. Em seguida, posicione a palma para autenticação.



1.6.2 Autenticação facial

1. Modo de autenticação Facial 1:N

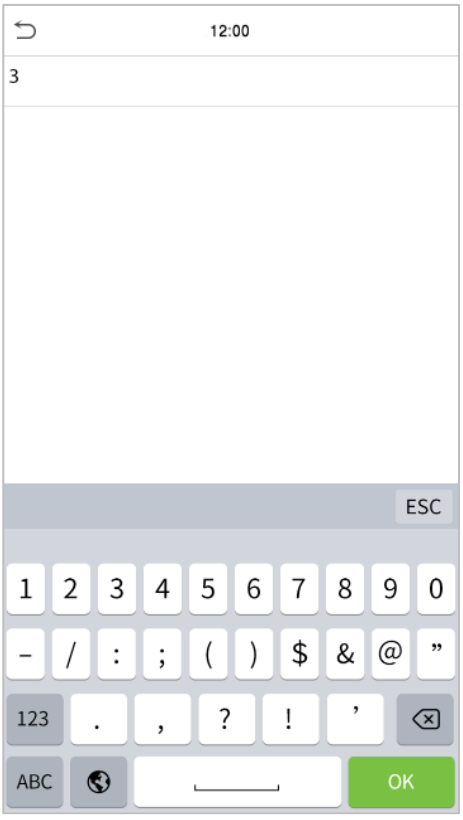
Neste modo de autenticação, o dispositivo compara as imagens faciais coletadas com todos os dados faciais cadastrados no dispositivo. Nas imagens abaixo é possível ver uma demonstração de um resultado de comparação bem-sucedida.

2. Ativar detecção de máscara

Quando o usuário ativa a função "Ativar detecção de máscara", o dispositivo identifica se o usuário está ou não usando uma máscara durante a verificação. Nas imagens abaixo é possível ver a comparação dos possíveis resultados da detecção:

Modo de autenticação facial 1:1

Nesse modo de autenticação, o dispositivo compara a face capturada pela câmera com o cadastro facial relacionado ao ID do usuário cadastrado. Pressione na tela principal e entre no modo de autenticação facial 1:1, digite o ID do usuário e clique em [OK].



Se o usuário tiver registrado palma, cartão e senha além do seu rosto, e o método de verificação estiver configurado para palma/face/cartão/senha de verificação, a tela a seguir será exibic elecione para entrar no modo de verificação facial.

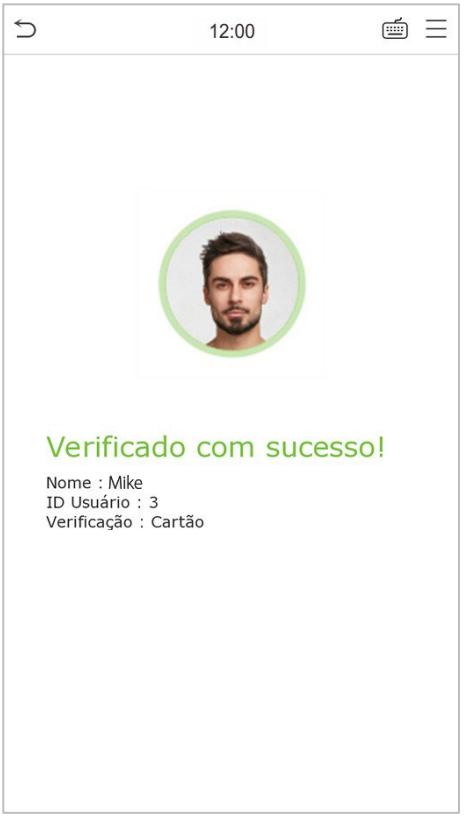
Após a verificação bem-sucedida, será exibida a mensagem "Verificado com sucesso", conforme mostrado abaixo:

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

1.6.3 Autenticação de cartão

Modo de autenticação de cartão 1: N

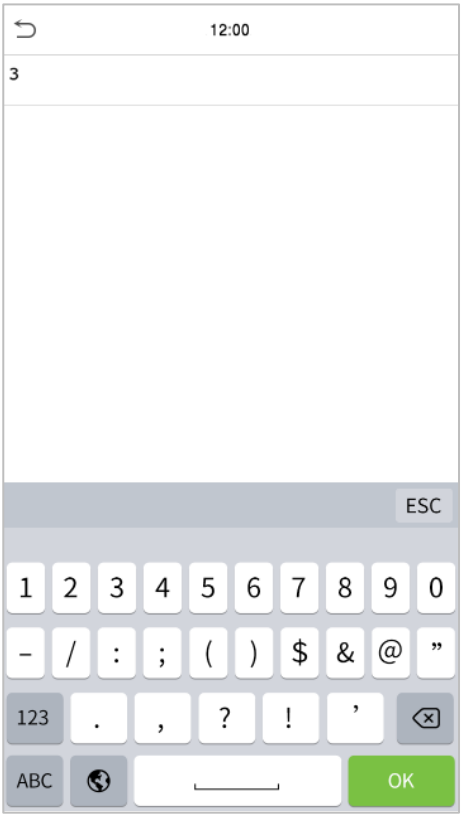
O modo de autenticação de cartão 1:N compara o número do cartão lido com todos os números de cartão cadastrados no dispositivo; A seguir está a tela de autenticação de cartão.



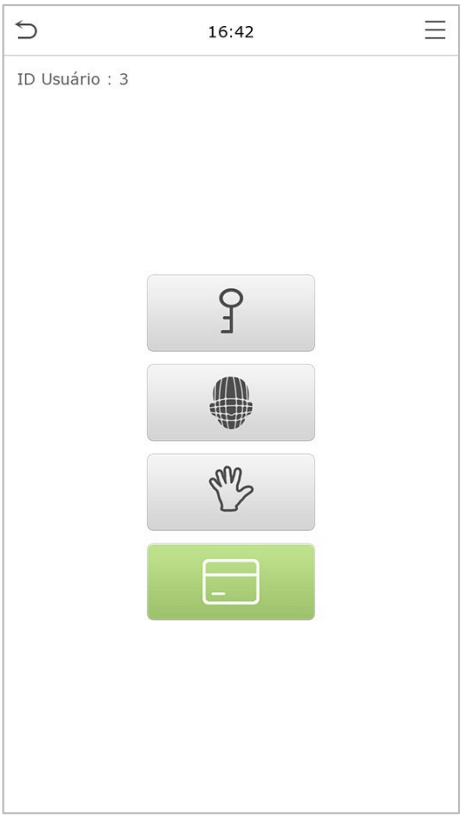
1:1 Modo de autenticação de cartão 1:1

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.

1. Selecione na tela principal para abrir o modo de autentificação de cartão 1:1.
2. Digite o ID do usuário e clique em [OK].

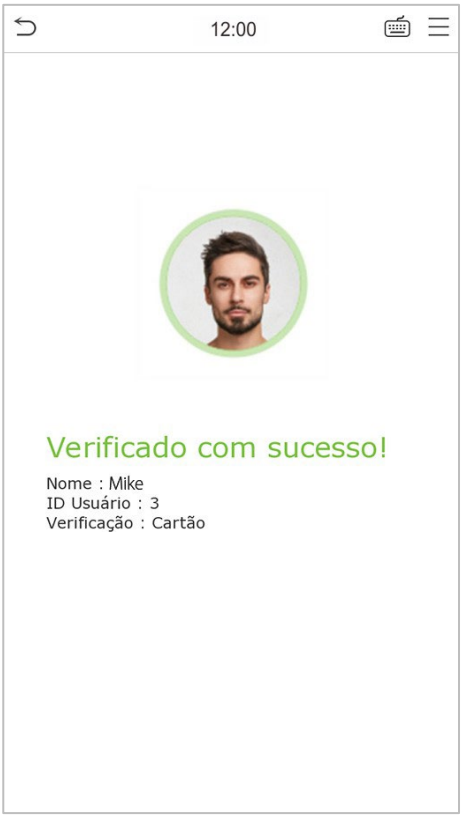


Se o usuário tiver cadastrado palma, face e senha, além do cartão e o método autenticação estiver configurado para palma/face/cartão/senha, a tela a seguir será exibida. Selecione o ícone para entrar no modo de autenticação do cartão.



2. Passe o cartão (o cartão precisa estar registrado).

A autenticação foi bem-sucedida:



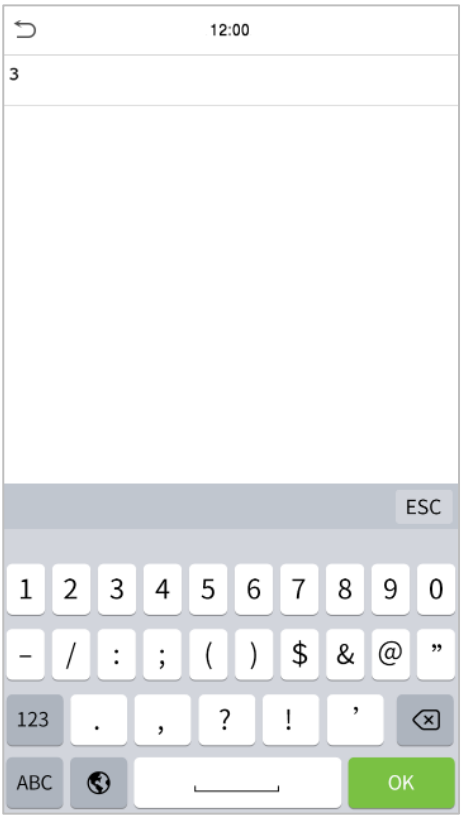
A autenticação falhou:

1.6.4 Autenticação de senha

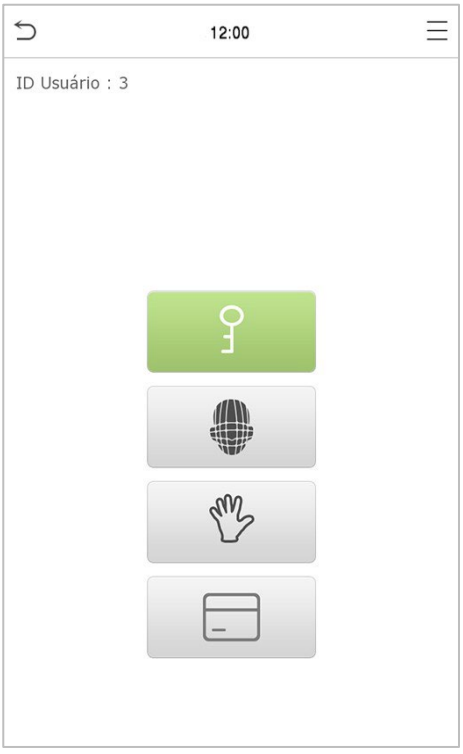
O dispositivo compara a senha inserida com a senha cadastrada no ID de usuário informado.

Clique no botão na tela principal para entrar no modo de autenticação de senha 1:1.

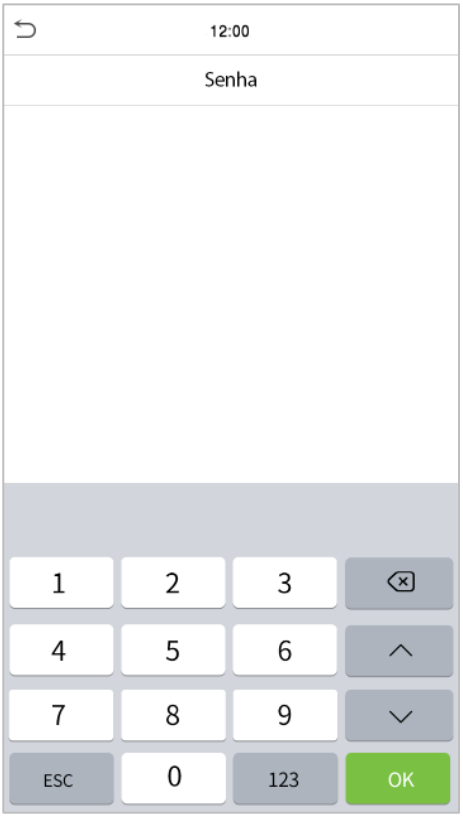
1. insira o ID do usuário e pressione [OK].



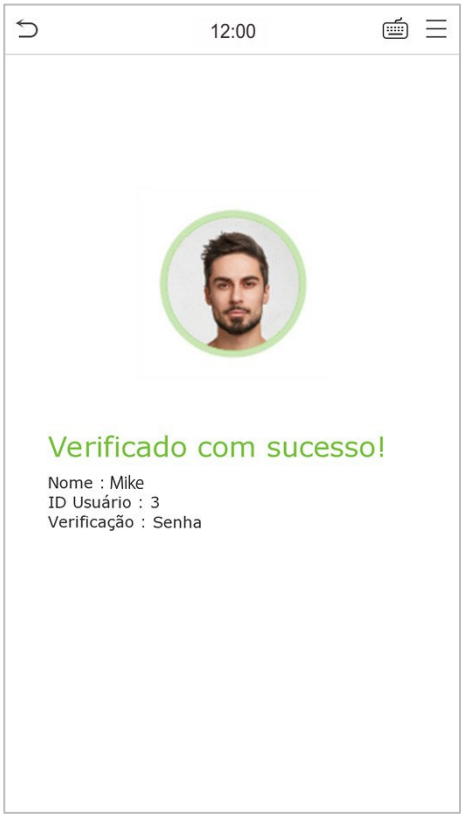
Se o usuário tiver cadastrado palma, face e cartão, além da senha e o método de autenticação estiver configurado para palma/face/cartão/senha, a tela a seguir será exibida. Selecione para acessar o modo de autenticação por senha



2. Insira a senha e pressione [OK].



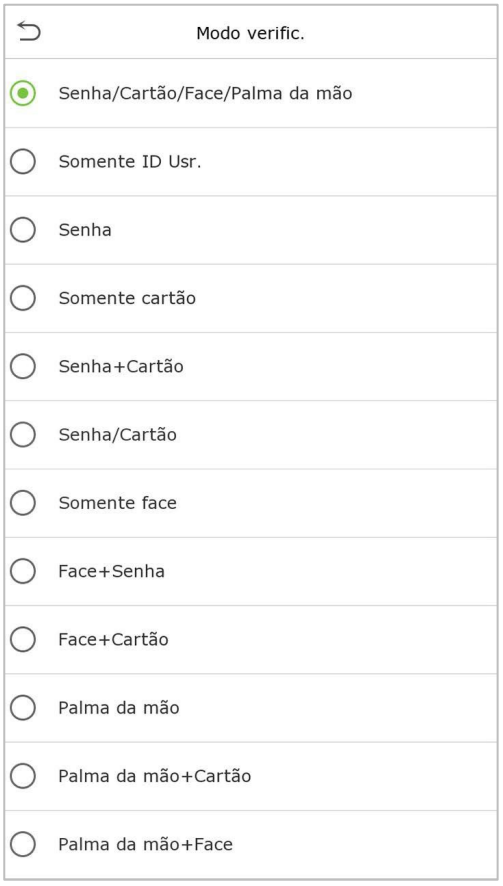
A autenticação foi bem-sucedida:



A autenticação falhou:

1.6.5 Autenticação Combinada

Para aumentar a segurança, este dispositivo oferece a opção de usar vários métodos de autenticação. Um total de 12 combinações de autenticações diferentes podem ser usadas, conforme mostrado abaixo:



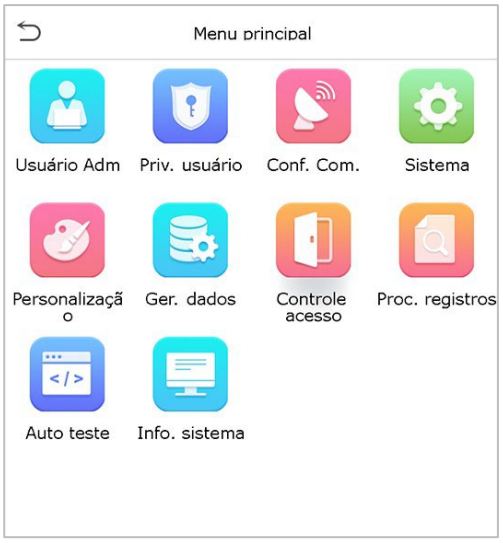
Nota:

1) "/" significa "ou"
"+" significa "e".

2) Você precisa registrar a informação necessária para autenticação antes de usar a autenticação combinada, caso contrário, a verificação pode falhar. Por exemplo, se um usuário tem registro facial, mas o modo de verificação é Face + Senha, esse usuário nunca vai passar a autenticação.

2 Menu Principal

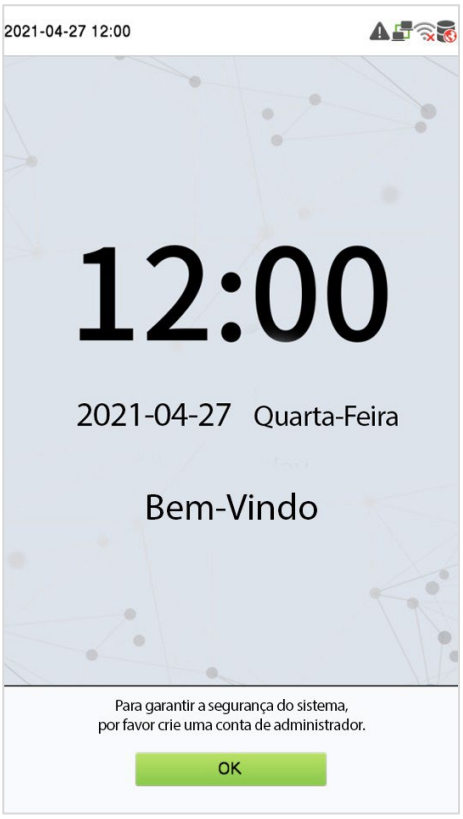
Selecione na tela de espera para entrar no Menu Principal, a seguinte tela será exibida:



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, Palma, Parâmetros de face, redefinir padrões de fábrica, atualização USB e Configuração de tipo de dispositivo e Configuração de detecção.
Personalização	Isso inclui configurações de Interface do Usuário, Voz e Alarme.
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 rejeitados.
Autoteste	Para testar automaticamente se cada módulo funciona corretamente, incluindo a tela LCD, áudio, microfone, 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.



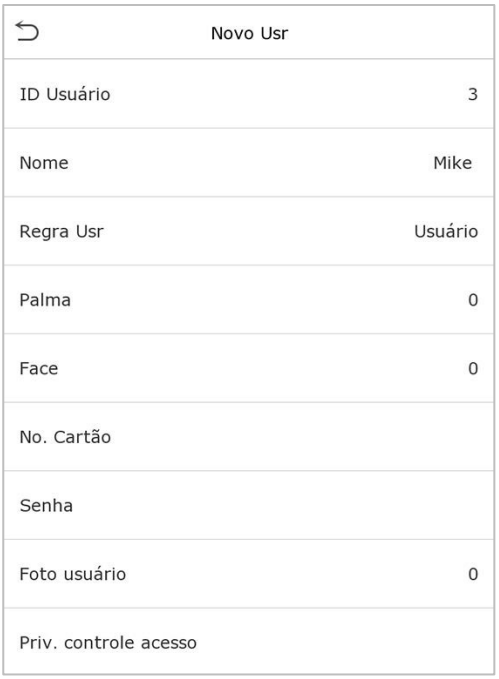
3 Gestão de Usuários

3.1 Cadastro de Usuários

Clique em Usuário Adm. no menu principal.

3.1.1 ID de usuário e nome

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



Nota:

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.

Nota: 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.

3.1.3 Registrar palma

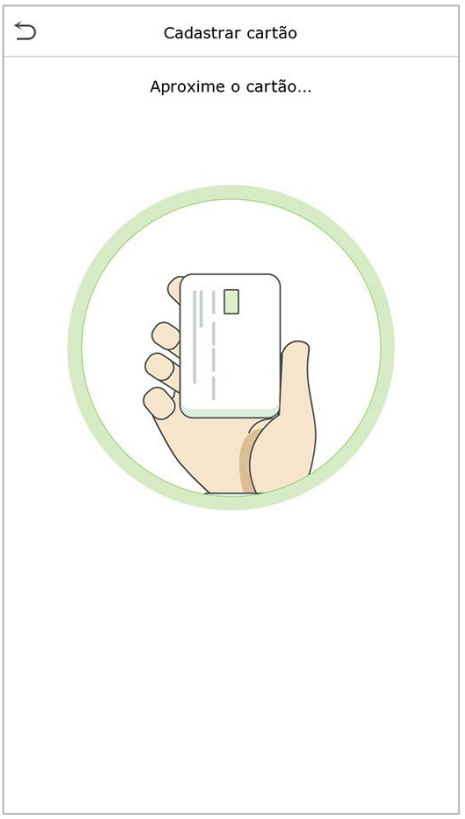
Toque em "Palma" na interface do Novo Usuário para entrar na página de cadastro da palma.
Selecione a palma a ser cadastrada.

3.1.4 Registrar Face

Toque em Face na interface do Novo Usuário para entrar na página de cadastro de face.
Por favor, olhe para a câmera, posicione a face dentro da caixa de guia e fique parado durante o cadastro.
A interface de registro é a seguinte:

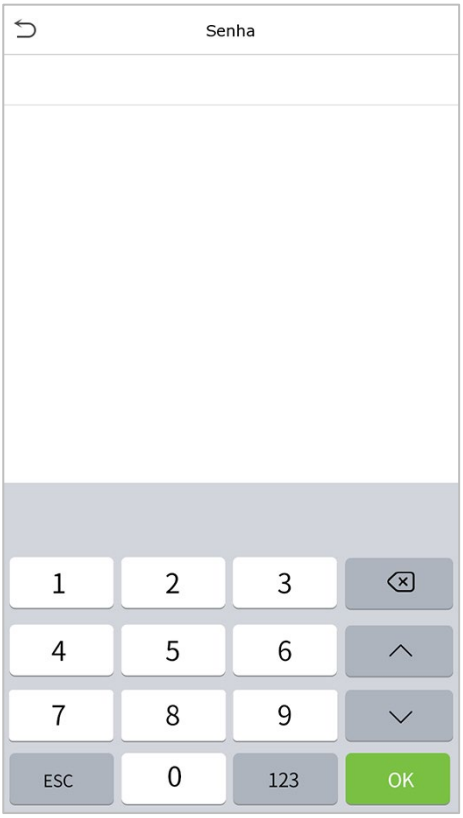
3.1.5 Registrar Cartão

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.



3.1.6 Registrar Senha

Toque em Senha na interface Novo usuário para entrar na página de cadastro de senha.
Digite a senha escolhida, clique em OK. Digite novamente a mesma senha para confirmar e clique em OK.
Se a senha reinserida for diferente da senha inserida inicialmente, o dispositivo irá mostrar a mensagem "Senha não coincide!" e o usuário precisará reconfirmar a senha novamente.



Nota: A senha pode conter de 1 a 8 dígitos.

3.1.7 Foto do Usuário

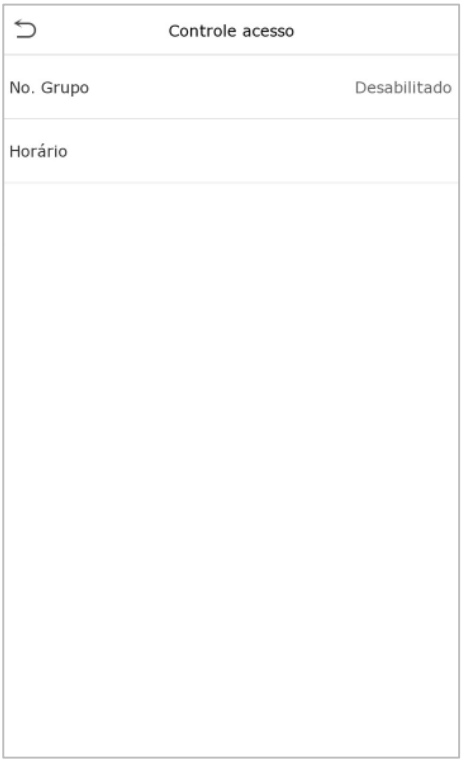
Quando um usuário cadastrado com uma foto fizer a autenticação, a foto cadastrada será exibida.

Toque em Foto do Usuário, a câmera do dispositivo será aberta, toque no ícone da câmera para tirar uma foto. O sistema retornará à interface do novo usuário após tirar uma foto.

Nota: Ao cadastrar uma face, o sistema captura automaticamente uma foto como a foto do usuário. Se você não cadastrar uma foto de usuário, o sistema definirá automaticamente a foto capturada durante o cadastro como a foto padrão.

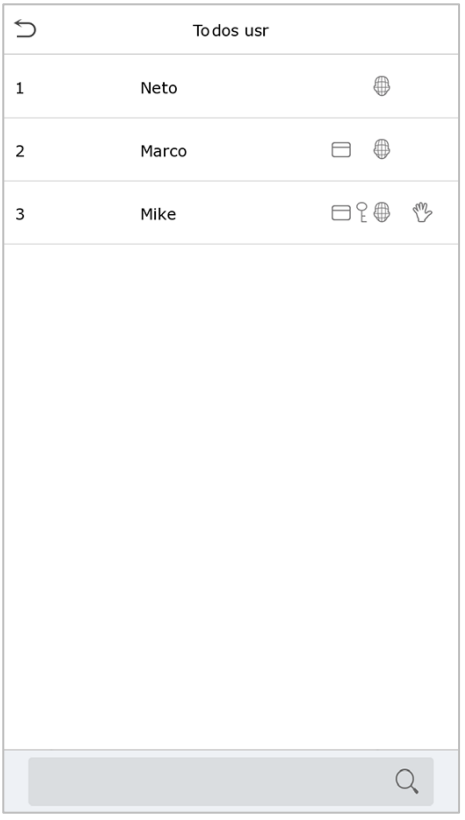
3.1.6 Função de controle de Acesso

A Função de Controle de Acesso define o privilégio de acesso à porta para cada usuário. Isso inclui o grupo de acesso, o modo de verificação e, também, facilita a definição do período de acesso do grupo.
Toque em Função de controle de acesso > Grupo de acesso, para atribuir os usuários cadastrado a diferentes grupos para um melhor gerenciamento. Novos usuários pertencem ao Grupo 1 por padrão e podem ser reatribuídos a outros grupos. O dispositivo suporta até 99 grupos de controle de acesso.
Clique em **Modo de Autentificação**, selecione o Modo de verificação a ser usado.



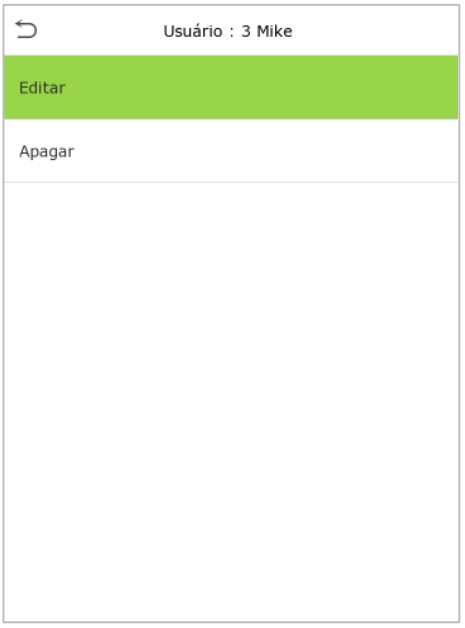
3.2 Procura de Usuários

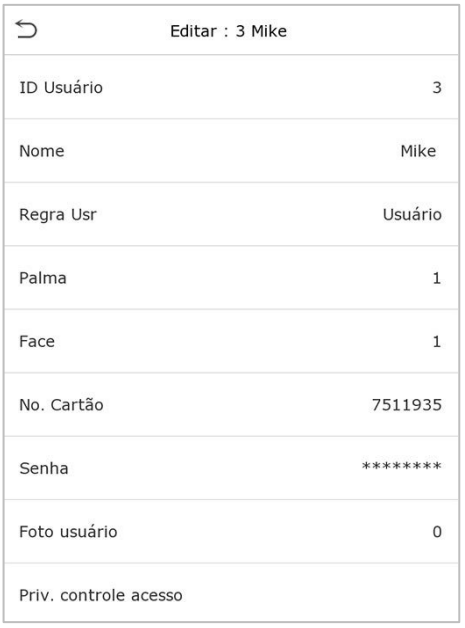
Na interface Todos os Usuários, toque na barra de pesquisa na lista de usuários para inserir a palavra-chave (onde a palavra-chave pode ser o ID do usuário, sobrenome ou nome completo) e o sistema procurará as informações do usuário.



3.3 Editar Usuários

Na interface Todos os Usuários, toque no usuário desejado na lista e toque em Editar para editar as informações do usuário



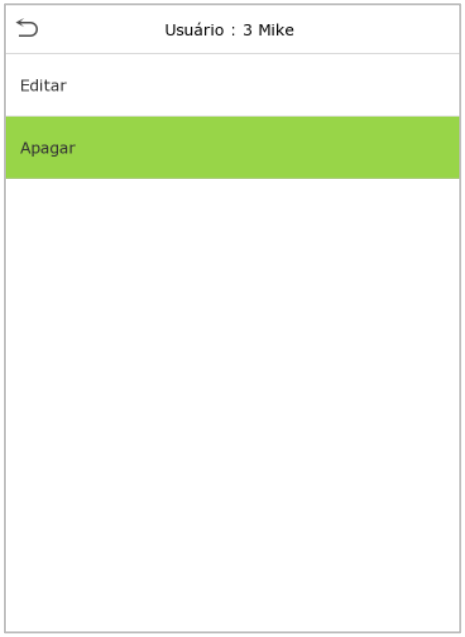


Nota: O processo de edição das informações do usuário é igual aos de adição de um novo usuário, exceto que o ID do usuário não pode ser modificado ao editar um usuário. Mais detalhes em "3.1 Cadastro de Usuários".

3.4 Excluir Usuário

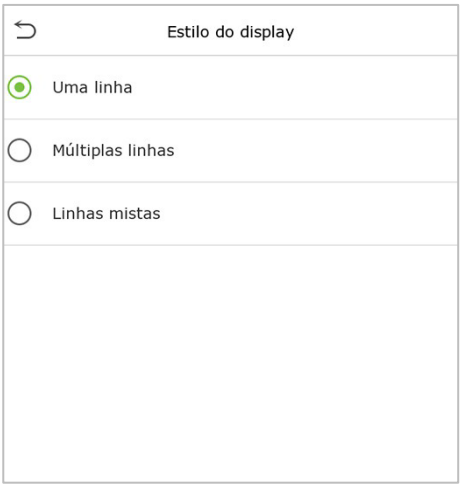
Na interface Todos os Usuários, toque no usuário escolhido na lista e toque em Excluir para excluir o usuário ou uma informação específica.

Nota: Se você selecionar **Deletar Usuário**, toda a informação do usuário será deletada.

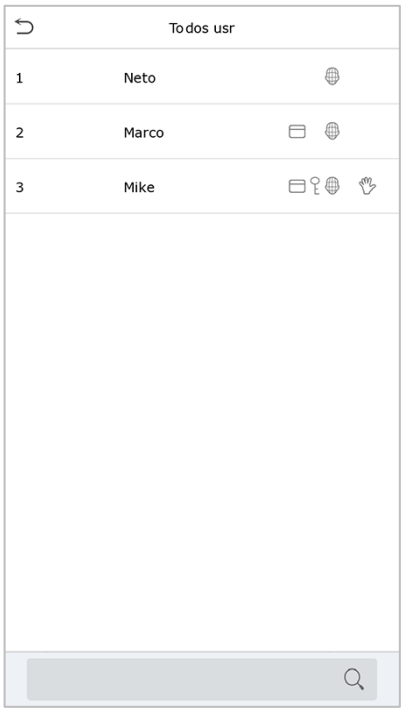


3.5 Estilo de Display

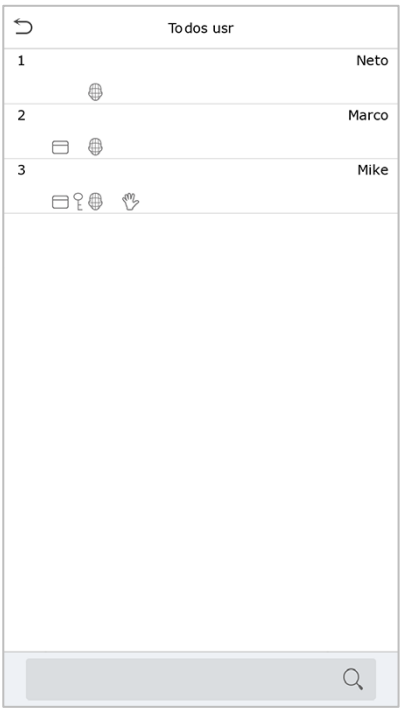
No **menu principal**, clique em **Usuário Adm.** e, em seguida, clique em **Estilo de exibição** para entrar na interface de configuração do Estilo de exibição.



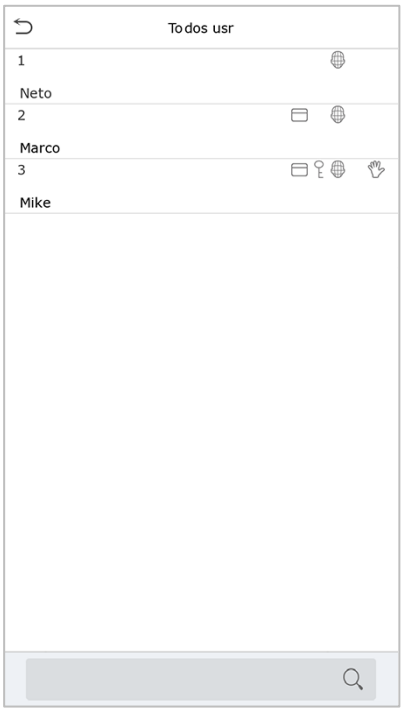
Todos os estilos de exibição são mostrados como abaixo:



Uma Linha



Múltiplas Linhas



Linha Mista

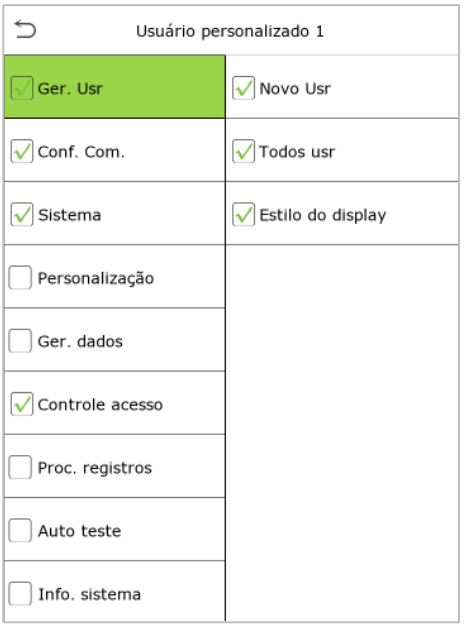
4 Privilégio do Usuário

O Privilégio do Usuário facilita a atribuição de algumas permissões específicas a determinados usuários, com base no que foi selecionado.
A delimitação de permissão da função personalizada pode ser configurada em até 3 grupos.

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

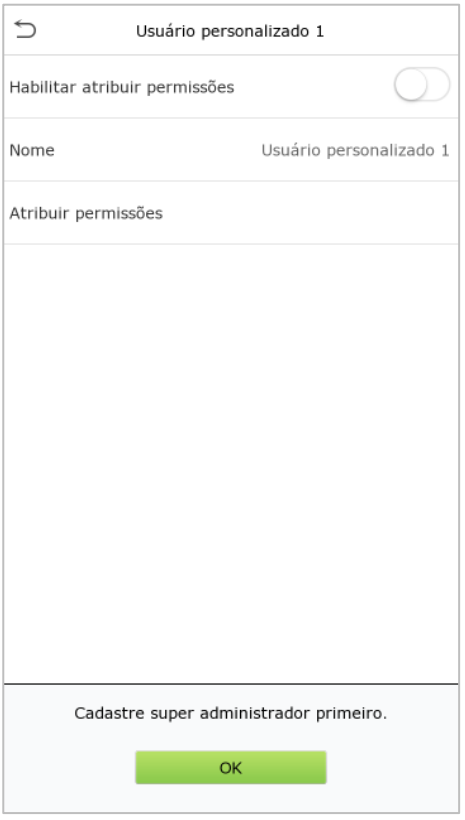
1. Clique em qualquer Usuário Personalizado, em seguida, selecione o botão Habilitar Atribuir Permissões, para ativar ou desativar a função do grupo selecionado.
   Toque em Nome para inserir o nome personalizado da função.

2. Em seguida, toque em Atribuir Permissões e selecione os privilégios necessários a serem atribuídos à nova função. Em seguida, toque no botão Retornar.



Nota: Durante a atribuição de permissões, o menu principal fica à esquerda e seus submenus à direita. Você só precisa selecionar os recursos nos submenus. Se o dispositivo tiver um usuário personalizado, você pode atribuir esses privilégios a usuários clicando em Usuário **Adm. > Novo usuário > Função do usuário.**

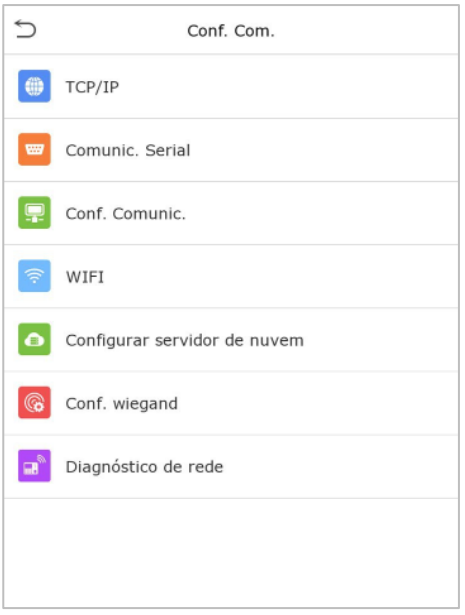
Se nenhum super administrador estiver registrado, o dispositivo solicitará "Cadastre super administrador primeiro!" depois de clicar na barra de ativação, conforme mostrado abaixo.



5 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.

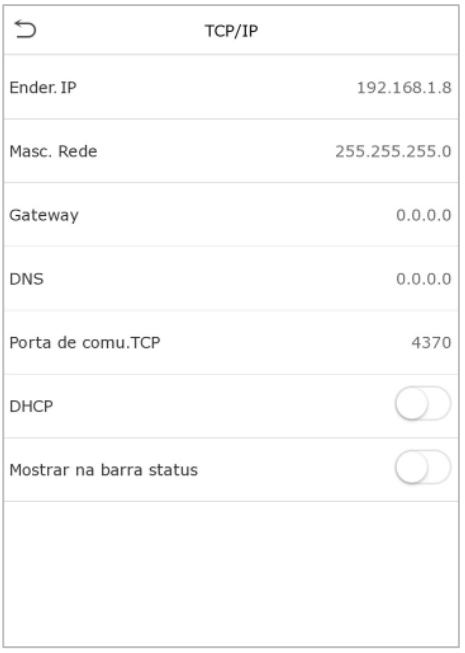
Toque em Conf. Com. no Menu Principal.



5.1 Configurações TCP/IP

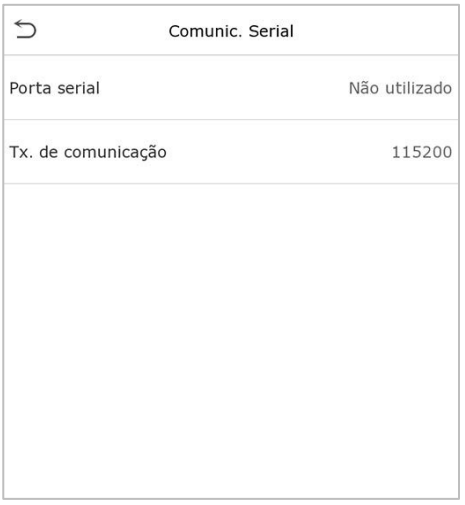
Quando o dispositivo precisa se comunicar com um PC por TCP/IP, você precisará definir as configurações de rede e garantir que o dispositivo e o PC estejam se conectando no mesmo segmento de rede.

Toque em TCP/IP em Conf. Com. para definir as configurações.



Menu	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, não recomendamos modificar.
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.

5.2 Comunicação Serial

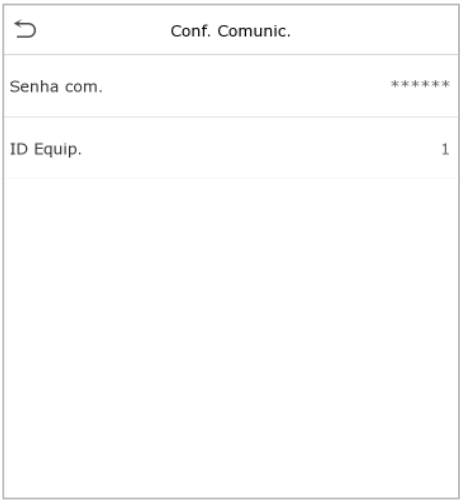


Menu	Descrição
Porta Serial	Sem uso: Não se comunica com nenhum dispositivo através da porta serial. Selecione RS232(PC) para comunicar com o dispositivo através de uma porta serial RS232. Selecione RS485(PC) para comunicar com o dispositivo através de uma porta serial RS485.
Taxa de Transmissão	A taxa na qual os dados são transmitidos na comunicação com o PC; existem 5 opções de taxa de transmissão: 115200 (padrão), 57600, 38400, 19200 e 9600. Quanto maior a taxa de transmissão, mais rápida é a velocidade de comunicação, mas também menos confiável. A taxa de transmissão mais alta pode ser usada quando a distância de comunicação é curta; quando a distância de comunicação é longa, escolher uma taxa de transmissão mais baixa é mais confiável.

5.3 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.

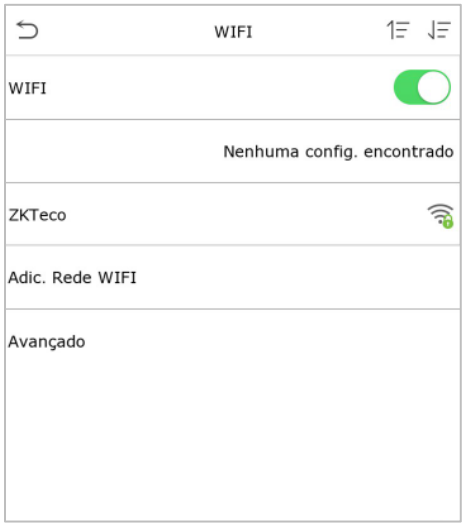


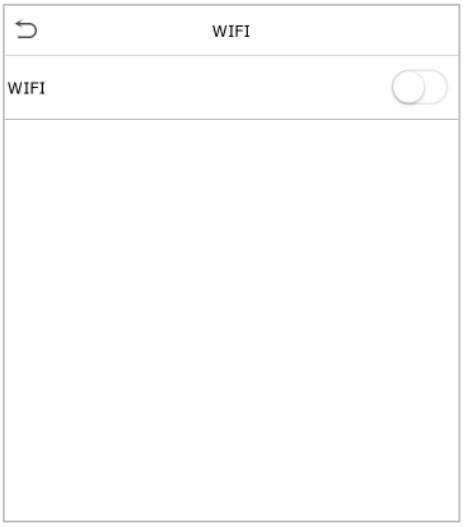
Menu	Descrição
Senha de Comunicação	A senha padrão é 0, que pode ser alterada. A senha de comunicação pode conter de 1 a 6 dígitos.
ID do aparelho	Número de identificação do dispositivo na rede serial, que varia entre 1 e 254. Se o método de comunicação for RS232/RS485, você precisa inserir este ID do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

5.4 Rede sem fio (Wi-Fi)

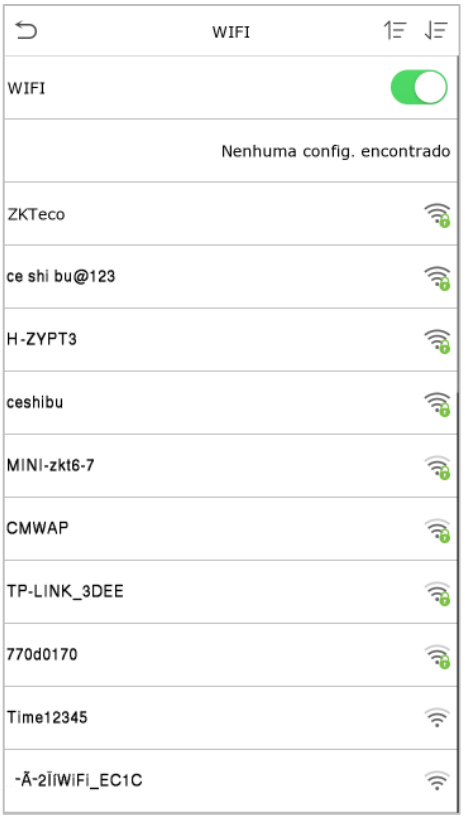
O dispositivo possibilita a conexão através do módulo Wi-Fi, que é um item opcional, podendo ser acoplado no dispositivo interna ou externamente, para permitir a transmissão de dados via Wi-Fi e estabelecer um ambiente com rede sem fio

O Wi-Fi está ativado por padrão no dispositivo. Se você não precisar usar a rede Wi-Fi, poderá alternar o botão para desabilitá-la.





Quando o Wi-Fi estiver ativado, clique na rede desejada. Toque na caixa de texto para inserir a senha e clique em Conectar ao Wi-Fi (OK).

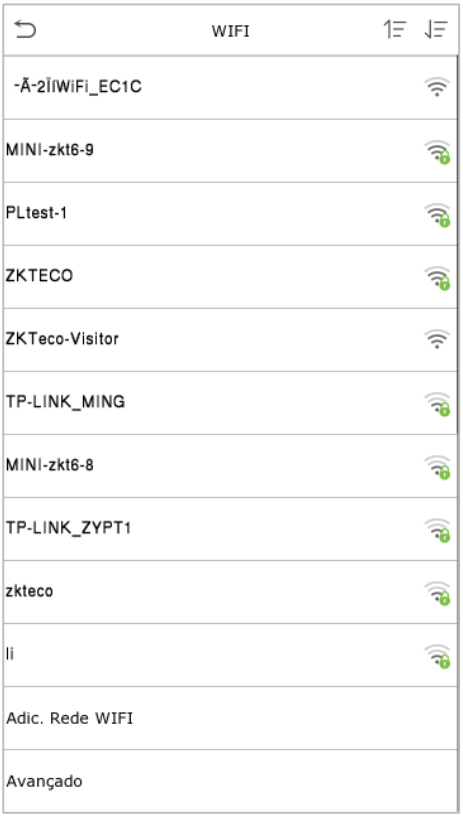


Se a conexão for bem-sucedida, o status é exibido na barra de ícones.

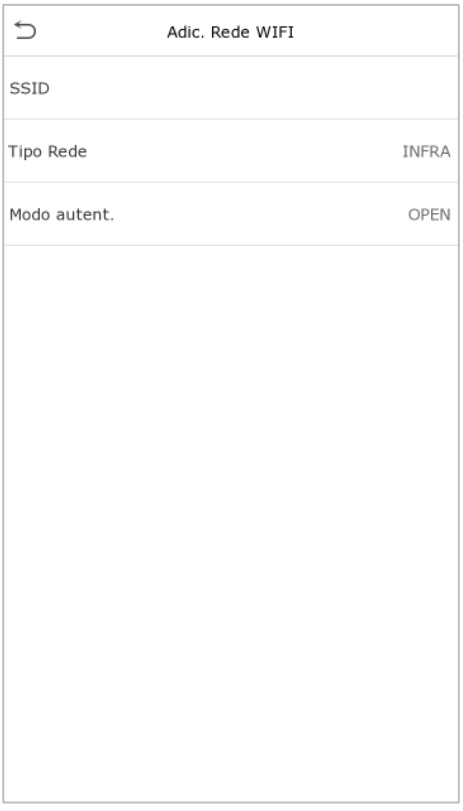
Adicionar rede Wi-Fi manualmente

O Wi-Fi também pode ser adicionado manualmente se o Wi-Fi desejado não for exibido na lista.

Clique e **Adic. Rede Wi-Fi**.



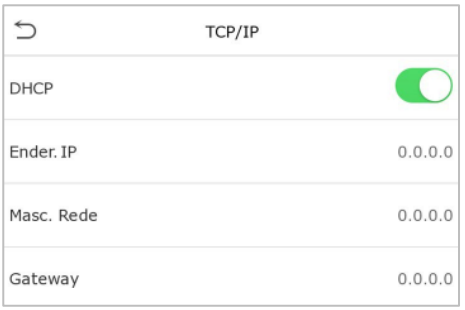
Nesta interface, insira os parâmetros de rede Wi-Fi (A rede adicionada precisa existir).



Depois de adicionar, encontre a rede Wi-Fi adicionada na lista e conecte-se à rede da maneira acima.

Configurações Avançadas

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

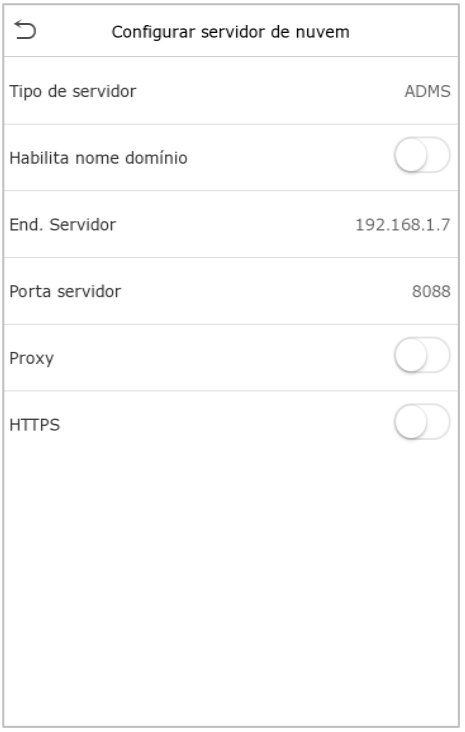


Menu	Descrição
DHCP	O protocolo de configuração dinâmica de host (DHCP) aloca dinamicamente endereços IP para clientes de rede. Se o DHCP estiver ativado, o IP não poderá ser definido manualmente.
IP Address	Endereço IP para a rede WIFI, o padrão é 192.168.1.201 (0.0.0.0 caso o DHCP esteja ativado).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

5.5 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.

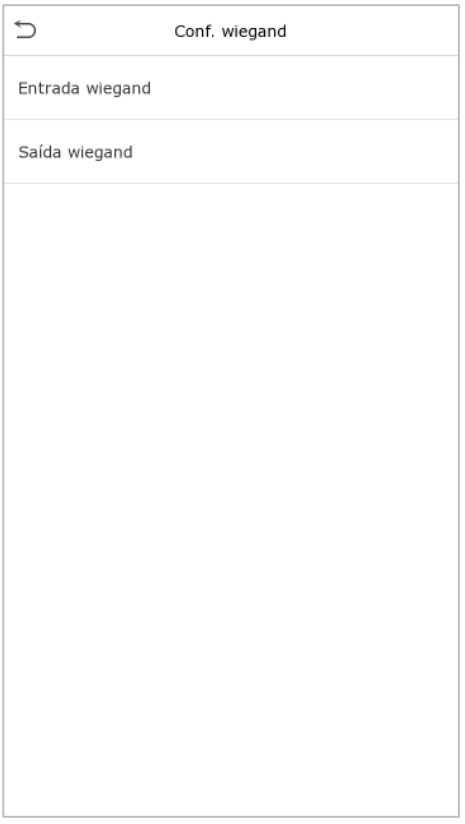


Menu		Descrição
Ativar nome de domínio	**Endereço do servidor**	Uma vez habilitada esta função, será utilizado o modo de nome de domínio "http://..." como http:www.XYZ.com, enquanto "XYZ" será o nome de domínio (quando este modo está LIGADO)
Desativar nome de domínio	**Endereço do servidor**	O endereço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

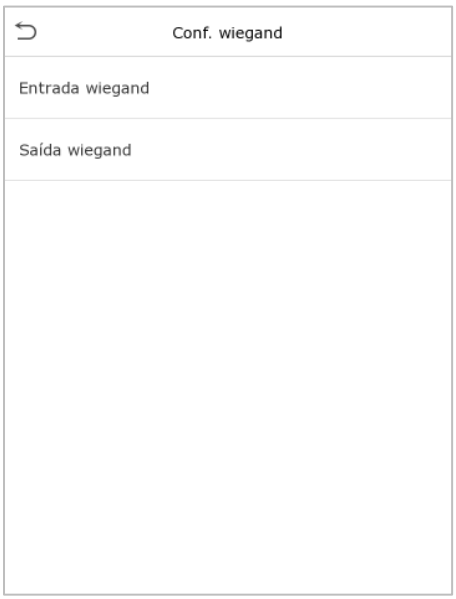
5.6 Configuração de Wiegand

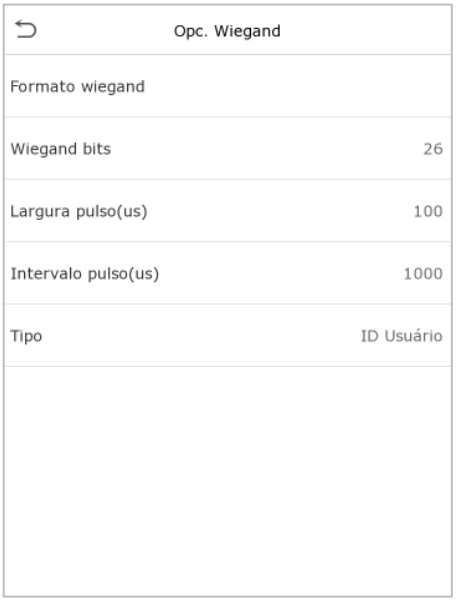
Este menu é usado para definir os parâmetros de entrada e saída Wiegand.

Toque em Configuração Wiegand na Interface de Configurações de Comunicação.



Entrada Wiegand





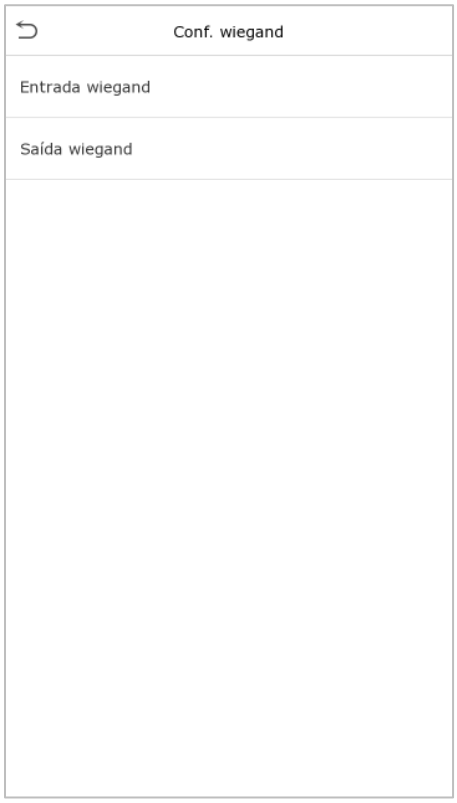
Menu	Descrição
Formato Wiegand	Os valores variam de 26 bits, 34 bits, 36 bits, 37 bits e 50 bits.
Bits de saída Wiegand	Após selecionar o formato Wiegand necessário, selecione os dígitos de bit de saída correspondentes do formato Wiegand
Largura do pulso (us)	O valor da largura de pulso enviado pelo 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	ECCCCCCCCCCCCCCCCCCCCCCCCO Consiste em 26 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 13º bits, enquanto o 26º bit é o bit de paridade ímpar do 14º ao 25º bits. O 2º ao 25º bits são os números do cartão
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO Consiste em 26 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 13º bits, enquanto o 26º bit é o bit de paridade ímpar do 14º ao 25º bits. Os 2º a 9º bits são os site code, enquanto os 10º a 25º bits são os números do cartão.
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO Consiste em 34 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 17º bits, enquanto o 34º bit é o bit de paridade ímpar do 18º ao 33º bits. O 2º ao 25º bits são os números do cartão.

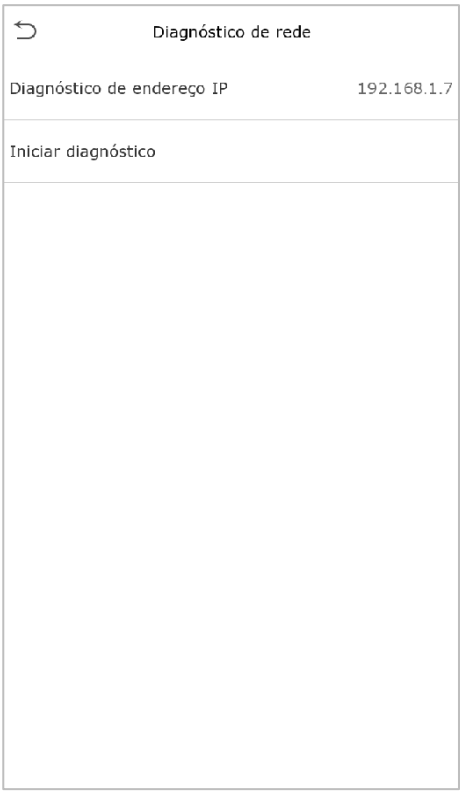
Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO Consiste em 34 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 17º bits, enquanto o 34º bit é o bit de paridade ímpar do 18º ao 33º bits. Os 2º a 9º bits são o site code, enquanto os 10º a 25º bits são os números do cartão
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME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

Saída Wiegand



Menu	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.

5.7 Diagnóstico de Rede

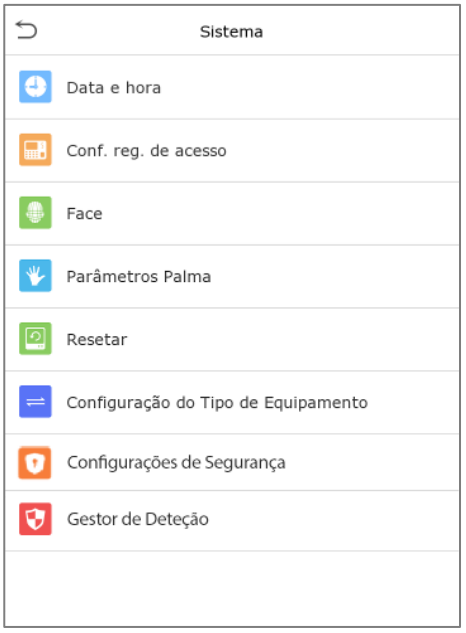


Menu	Descrição
Teste de diagnóstico de endereço IP	O endereço padrão de fábrica é 0.0.0.0. Por favor, defina o valor de acordo com os requisitos.
Iniciar Diagnóstico	Clique em Iniciar para diagnosticar automaticamente a rede.

6 Configurações de Sistema

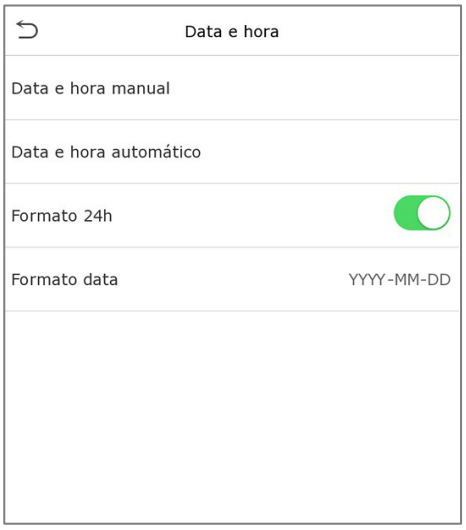
As configurações do sistema são usadas para definir os parâmetros do sistema relacionados para otimizar o desempenho do dispositivo.

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

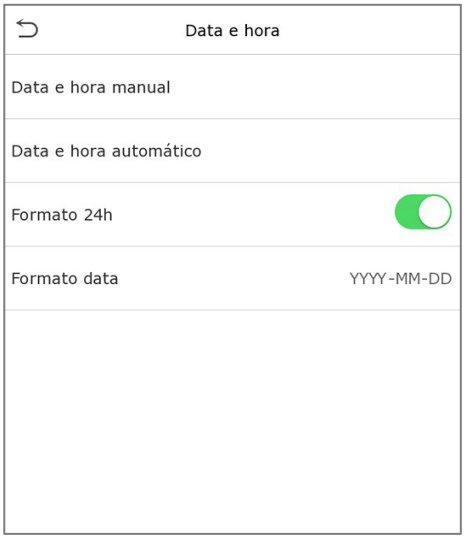


6.1 Data e Hora

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



1. 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.
2. 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.



3. Toque em **Formato 24h** para ativar ou desativar este formato.

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

Nota: Por exemplo, se o usuário define a hora do dispositivo (18h35 de 15 de março de 2020) para 18h30 de 1º de janeiro de 2021, após restaurar as configurações de fábrica, a hora do dispositivo mudará para 18h30 de janeiro 1, 2021.

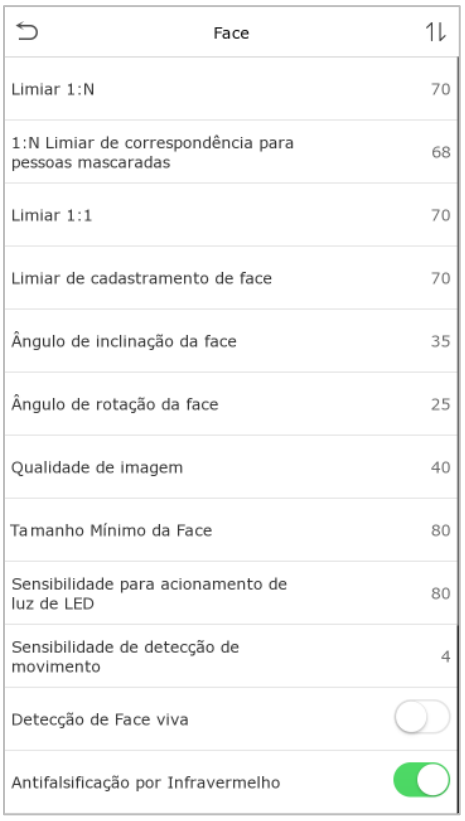
6.2 Configuração de Registros de Acesso

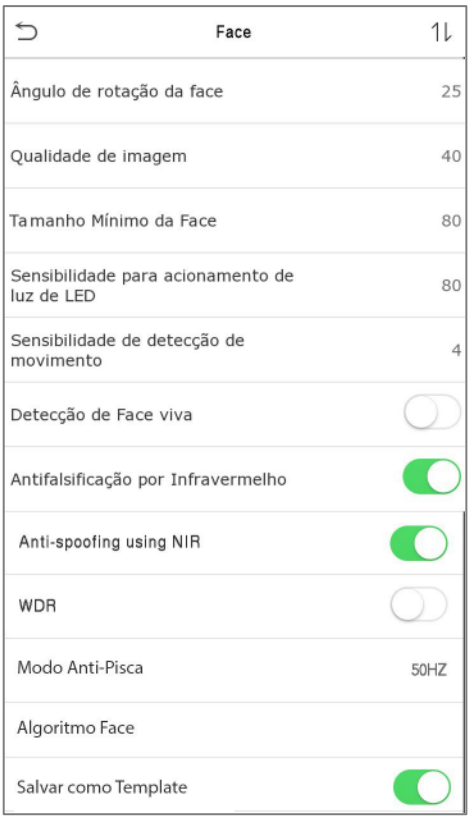
Clique nas **configurações de registros de acesso** na interface do sistema

Nome da 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.
ID de usuário alfanumérico	Whether to support letters in employee ID.
Aviso de logs de acesso	Quando o espaço de registro do acesso atingir o valor limite máximo, o dispositivo exibirá automaticamente o aviso de espaço de memória. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 9999.
Exclusão cíclica dos registros de acesso	Quando os registros de acesso atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de registros de acesso antigos. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 999.
Exclusão cíclica de fotos de ponto	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 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)	Depois que a identificação do intervalo for clicada (selecionada), por exemplo, se o intervalo de comparação for definido como 5 segundos, o reconhecimento facial verificará o rosto a cada 5 segundos. Valor válido: 0 a 9 segundos. 0 significa identificação contínua, 1 a 9 significa identificação em intervalos.

6.3 Parâmetros de Face

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





Menu	Descrição
Limiar 1:N	No modo de autenticação 1:N, a autenticação só será bem-sucedida quando a semelhança entre a imagem facial adquirida e todos os modelos faciais registrados for maior que o valor definido. Esse valor varia de 0 a 100. Quanto mais alto o limite, menor a taxa de erro de julgamento e maior a taxa de rejeição e vice-versa. Recomenda-se definir o valor padrão de 47.
Limiar 1:N para Usuários de Máscara Facial	No modo de autenticação 1:N, o dispositivo executará correspondência de similaridade entre o rosto que está usando a máscara e o modelo de rosto registrado no dispositivo. Quando a similaridade for maior que esse valor, significa que a correspondência foi bem-sucedida, caso contrário, significa que a correspondência falhou. O valor válido varia de 0 a 100. Quanto mais altos os limites, menor a taxa de erro de julgamento e maior a taxa de rejeição e vice-versa. Recomenda-se definir o valor padrão de 68.

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	A tolerância do ângulo de inclinação de uma face para cadastro e autenticação facial. Se o ângulo de inclinação de uma face exceder esse valor, ele será filtrado pelo algoritmo, ou seja, ignorado pelo terminal, portanto, nenhuma mensagem de cadastro e autenticação será mostrada
Ângulo de rotação da face	A tolerância do ângulo de rotação de uma face para cadastro e autenticação facial. Se o ângulo de rotação de uma face exceder este valor, ele será filtrado pelo algoritmo, ou seja, ignorado pelo terminal, portanto, nenhuma mensagem de cadastro e autenticação será mostrada.
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.
Limiar de detecção binocular ao vivo	Parâmetro para ajustar a antifalsificação por infravermelho. Quanto maior o valor, melhor o desempenho antifalsificação da imagem espectral de infravermelho.
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.**"
Notas	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.

6.4 Parâmetros da palma

Toque em **Palma** na interface do Sistema para definir as configurações da palma.

Menu	Descrição
Limiar de palma 1:1	Somente quando a similaridade entre a palma capturada e a palma cadastrada do usuário for maior que este valor, a autenticação será bem-sucedida.
Limiar de palma 1:N	No método de autenticação 1:N, somente quando a similaridade entre a palma capturada e todas as palmas cadastradas for maior que este valor, a autenticação será bem-sucedida.

6.5 Restauração dos padrões de fábrica

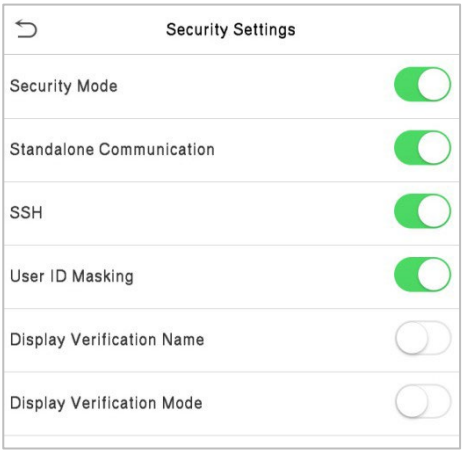
A função de Restauração de Fábrica restaura as configurações do dispositivo, como configurações de comunicação e configurações do sistema para as configurações padrão de fábrica (esta função não limpa os dados de cadastro do usuário e nem logs de acesso).

Toque em **Resetar** na interface do Sistema.

Toque em **OK** para restaurar as configurações padrão de fábrica.

6.6 Configurações de Segurança

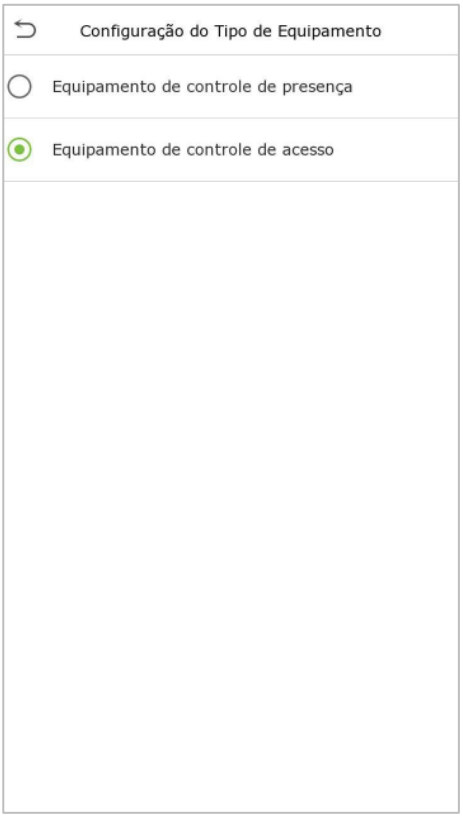
Clique em **Configurações de Segurança** na interface do **Sistema**.



Nome da 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. **Nota**: 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.

6.7 Configuração do tipo de dispositivo

Toque em **Configuração do Tipo de Dispositivo** na interface do **Sistema**.

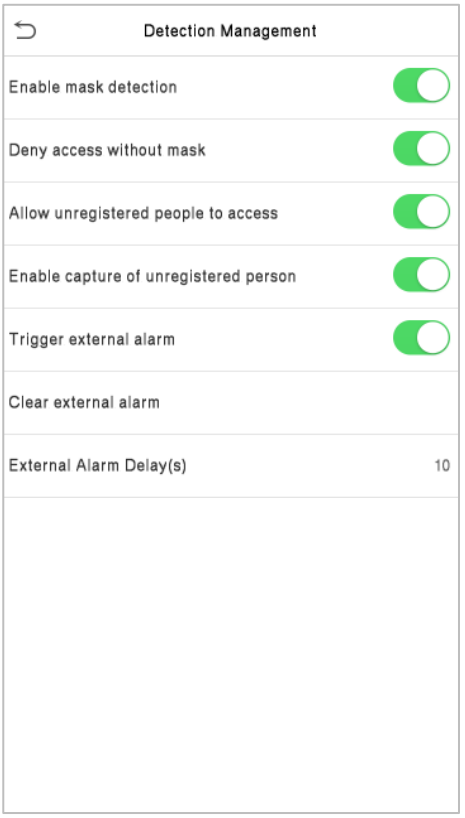


Nome da Função	Descrição
Terminal de Ponto e Presença	Defina o dispositivo como terminal ponto e presença.
Terminal de Controle de Acesso	Defina o dispositivo como terminal de controle de acesso.

Nota: Depois de alterar o tipo de dispositivo, o dispositivo excluirá todos os dados e reiniciará, e algumas funções serão ajustadas de acordo

6.8 Gestão de Detecção

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



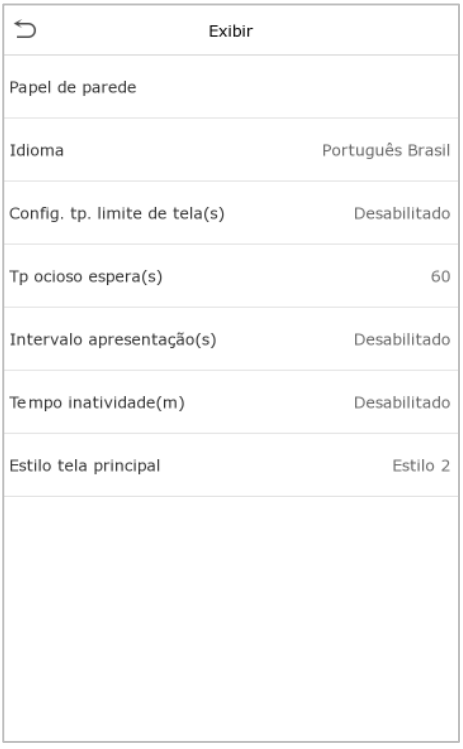
Nome da Função	Descrição
Ativar detecção de máscara	Habilita ou desabilita a função de detecção de máscara. Quando habilitado, o dispositivo identifica se o usuário está usando máscara ou não durante a verificação.
Negar acesso sem máscara	Habilita ou desabilita o acesso de uma pessoa sem máscara. Quando ativado, o dispositivo nega o acesso de uma pessoa, se ela não estiver usando máscara.
Permitir acesso a pessoas não registradas	Habilita ou desabilita o acesso de pessoa não cadastrada. Quando habilitado, o aparelho permite que a pessoa entre sem cadastro.
Ativar captura de foto de pessoas não registradas	Habilitar ou desabilitar a captura de foto da pessoa não cadastrada. Quando ativado, o dispositivo irá capturar automaticamente a foto da pessoa não cadastrada, habilitar este recurso requer **permitir o acesso de pessoas não cadastradas**.
Acionar Alarme Externo	Quando habilitado, se o usuário não estiver usando máscara, o sistema acionará um alarme.
Limpar registro de alarme	Elimina os registros de alarme acionados do dispositivo.
Atraso de Alarme Externo (s)	É o tempo de atraso (s) de acionamento de um alarme externo. Pode ser definido em segundos. Os usuários podem desativar a função ou definir um valor entre 1 a 255.

7 Configurações de Personalização

Toque em Personalização na interface do Menu principal para personalizar as configurações da interface, voz e campainha.

7.1 Configurações de Exibição

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

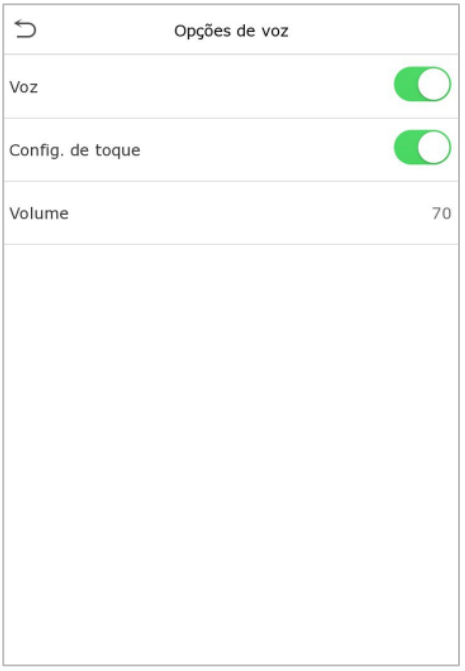


Menu	Descrição
Papel de parede	Permite selecionar o papel de parede da tela principal.
Idioma	Permite selecionar o idioma do dispositivo.
Tempo limite da tela do menu (s)	Quando não há utilização e o tempo excede o valor definido, o dispositivo retornará automaticamente à tela inicial. A função pode ser desativada ou definir o valor necessário entre 60 e 99999 segundos.

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.

7.2 Configurações de voz

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



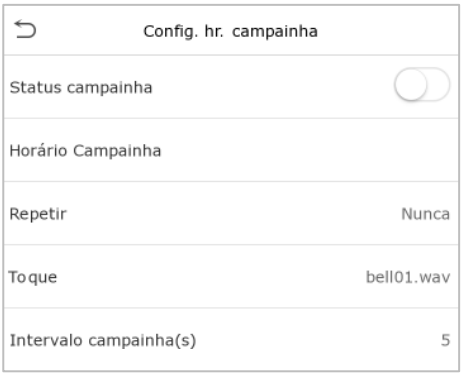
Menu	Descrição
Voz	Alterne para ativar ou desativar os comandos de voz durante as operações de funções.
Confi. de toque	Alterne para ativar ou desativar os sons do teclado
Volume	Ajuste o volume do dispositivo que pode ser definido entre 0-100.

7.3 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.



Menu	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.

2. 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 Gerenciamento de Dados

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

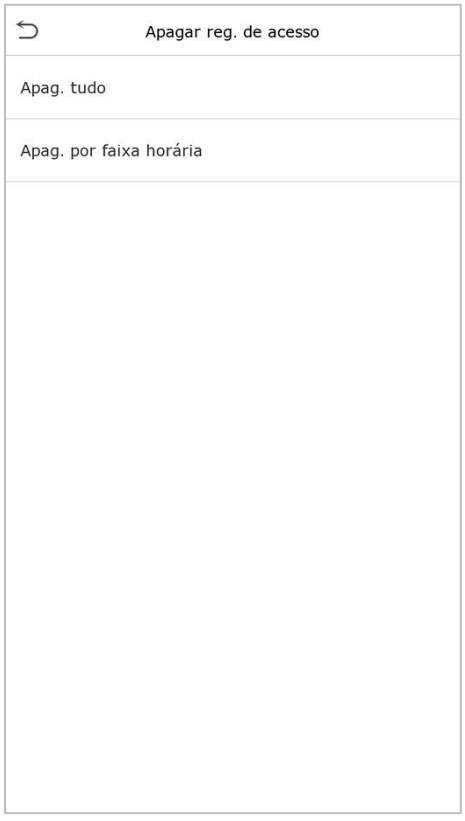
8.1 Excluir dados

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

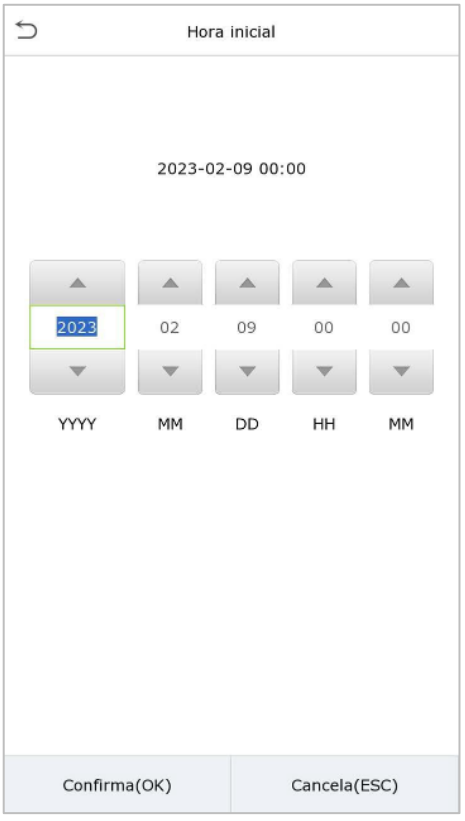
Nome da função	Descrição
Apagar reg. de acesso	Para apagar dados de frequência/registros de acesso
Apagar foto ponto	Para apagar fotos de ponto registradas.
Apagar foto lista bloqueio	Para apagar as fotos tiradas durante verificações com falha.
Apagar todos os dados	Para apagar informações e registros 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.



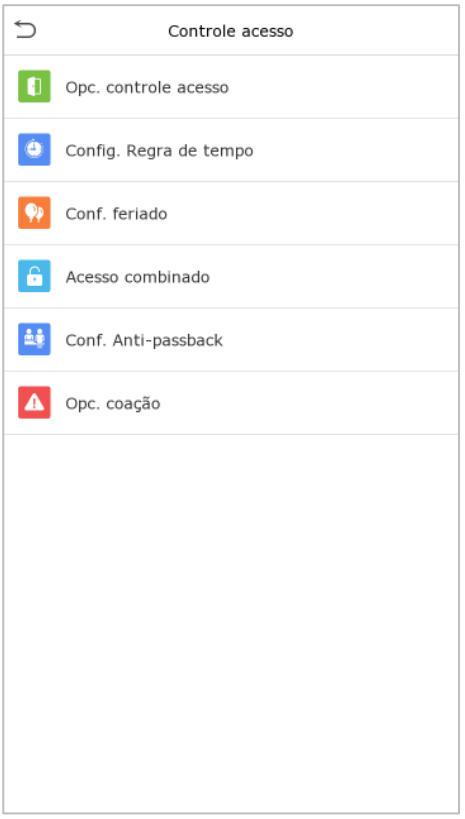
Selecione Apagar por intervalo de tempo.



Defina o intervalo de tempo e clique em OK.

9 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:

1. O tempo atual de desbloqueio da porta deve estar dentro de qualquer fuso horário válido do período de tempo do usuário.
2. 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).
3. 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.

9.1 Opções de controle de acesso

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

Nome da função	Descrição
Modo de controle de portão/catraca	Alterne entre **ON** ou **OFF** para entrar no modo de controle do portão ou não. Quando definido como **LIGADO**, nesta interface removerá as opções de relé de trava de porta, sensor de porta e tipo de sensor de porta.
Tempo de trava (s)	Tempo de acionamento do relé após uma autenticação válida. Valor válido: 1~10 segundos; 0 segundo representa função desativada.
Atraso do sensor da porta (s)	Se a porta não estiver travada e for deixada aberta por um determinado período (Atraso do sensor da porta), um alarme será acionado. O valor válido do Atraso do Sensor da Porta varia de 1 a 255 segundos
Tipo de sensor de porta	Existem três opções de Sensores: **Nenhum, Normal Aberto e Normal Fechado.** **Nenhum**: significa que o sensor da porta não está em uso. **Normal Aberta**: Com a porta fechada, o equipamento espera um sinal aberto. **Normal Fechado**: Com a porta fechada, o equipamento espera um sinal fechado
Modo de verificação	Os modos de verificação suportados incluem face, ID do usuário, senha, senha/face e rosto + 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".
Verify Mode by RS485	O modo de verificação é usado quando o dispositivo é usado como host ou auxiliar. Os modos de verificação suportados são cartão e cartão + senha.
Alarme	Emite um alarme sonoro quando a porta estiver fechada ou a verificação for bem-sucedida, o sistema cancelará o alarme do local.
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.

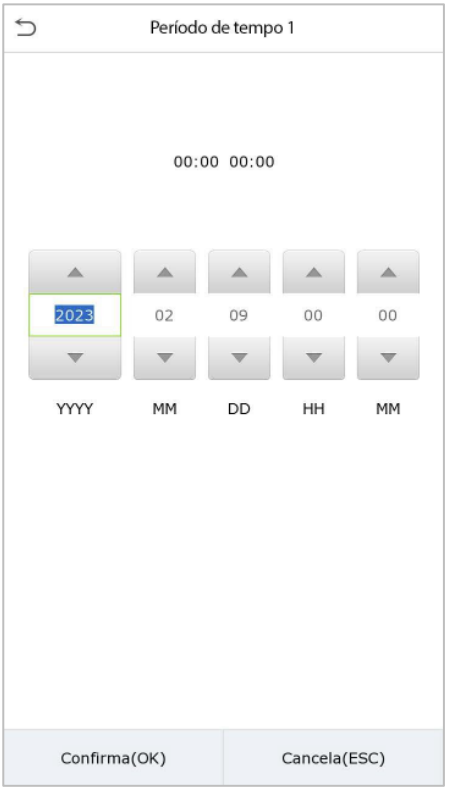
9.2 Configuração de regra de tempo

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**.

Nota:

1) Quando o horário de término é anterior ao horário de início (como 23:57~23:56), indica que o acesso está proibido o dia todo.

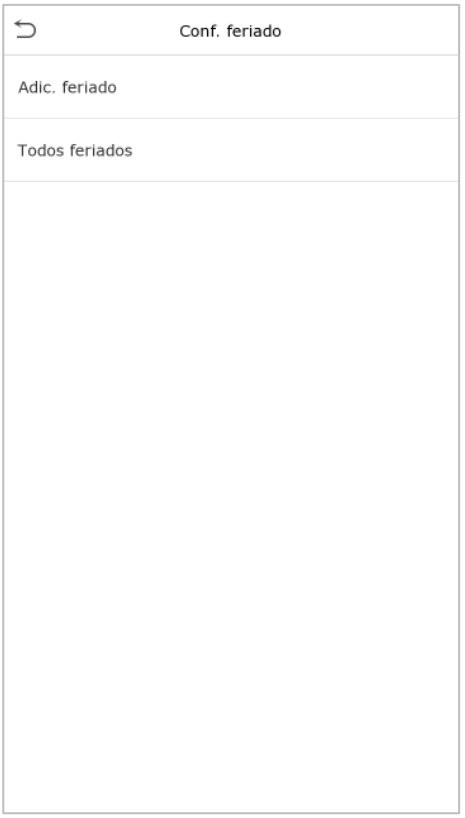
2) Quando a hora de término for posterior à hora de início (como 00:00~23:59), isso indica que o intervalo é válido.

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

4) A faixa horária padrão 1 indica que a porta está aberta o dia todo.

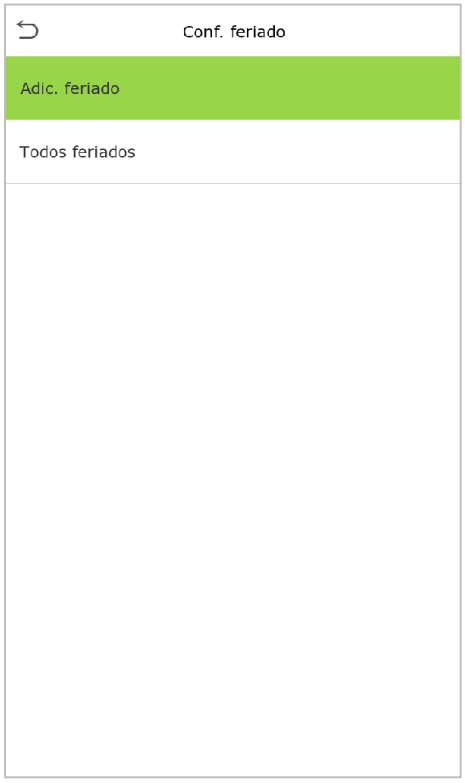
9.3 Feriados

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

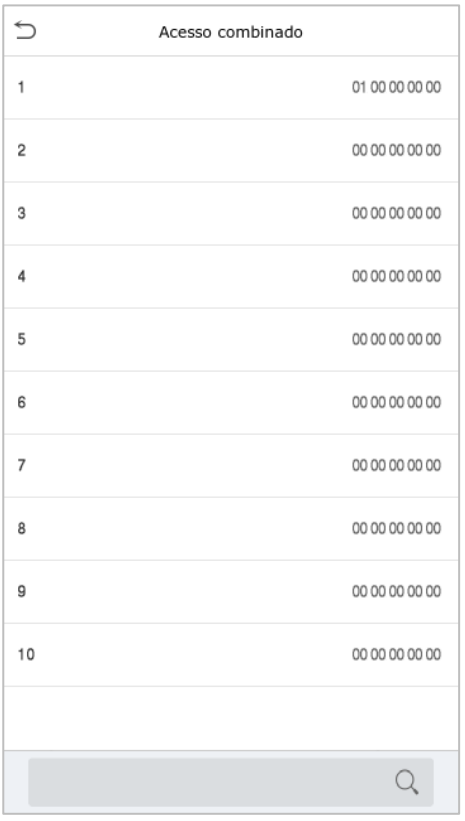
Na interface de Feriados, selecione um item de feriado a ser excluído e toque em **Apagar**. Pressione **OK** para confirmar a exclusão. Após a exclusão, este feriado não é mais exibido na interface Todos os feriados.

9.4 Acesso combinado

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

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

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



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

Examples:

A combinação de destravamento da porta 1 é definida como (01 03 05 06 08), indicando que a combinação de desbloqueio 1 é composta por 5 pessoas, e os 5 indivíduos são de 5 grupos, ou seja, Grupo de Controle de Acesso 1 (AC grupo 1), AC grupo 3, grupo AC 5, grupo AC 6 e grupo AC 8, respectivamente.

A combinação de destravamento da porta 2 é definida como (02 02 04 04 07), indicando que a combinação de destravamento 2 é composta por 5 pessoas; as duas primeiros são do grupo AC 2, as duas próximas são do grupo AC 4 e a última é do grupo AC 7.

A combinação 3 de destravamento da porta é definida como (09 09 09 09 09), indicando que há 5 pessoas nesta combinação; todas o grupo AC 9.

A combinação de destravamento da porta 4 é definida como (03 05 08 00 00), indicando que a combinação de destravamento 4 é composta por 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.

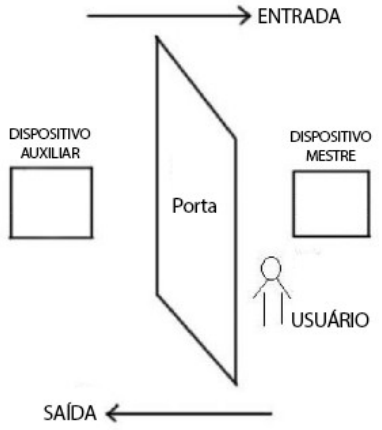
Excluir uma combinação de destravamento de porta

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

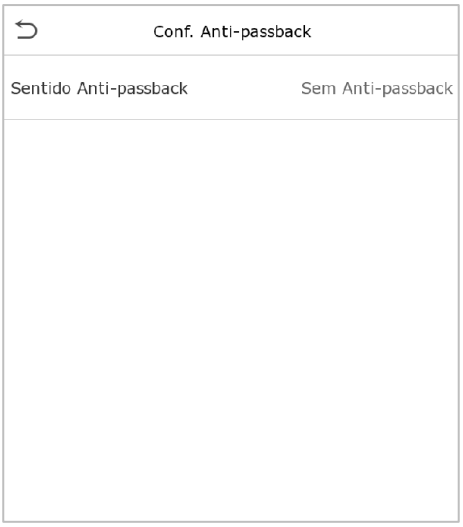
9.5 Configuração Anti-Passback

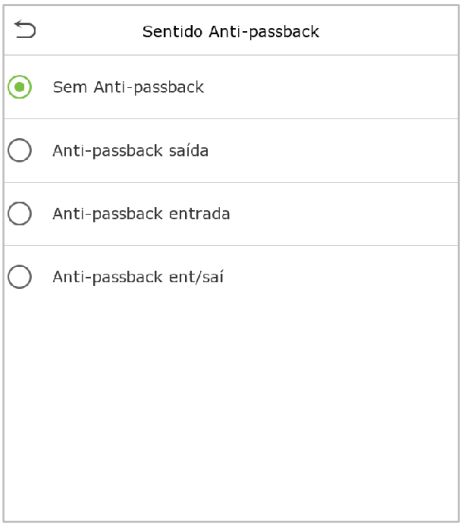
É possível que os usuários sejam seguidos por algumas pessoas para entrar na porta sem verificação, resultando em uma violação de segurança. Assim, para evitar tal situação, foi desenvolvida a opção Anti-Passback. Uma vez habilitado, o registro de check-in deve coincidir com o registro de check-out para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





Nome da Função	Descrição
Direção Anti-Passback	**Sem Anti-passback:** A função anti-passback está desativada, o que significa que a verificação bem-sucedida através do dispositivo mestre ou do dispositivo auxiliar pode desbloquear a porta. O status de entrada ou saída não é salvo nesta opção para o próximo desbloqueio. **Anti-passback 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.

9.6 Opções de Coação

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

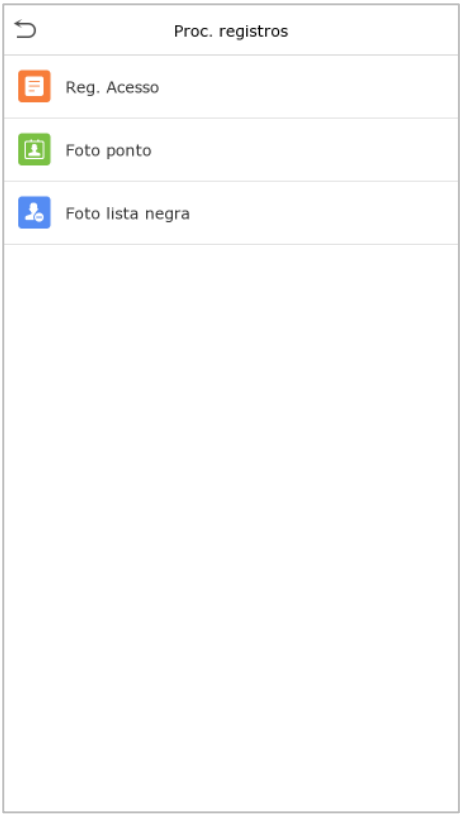
Na interface de controle de acesso, toque em **Opções de Coação** para definir as configurações de coação.

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

10 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.

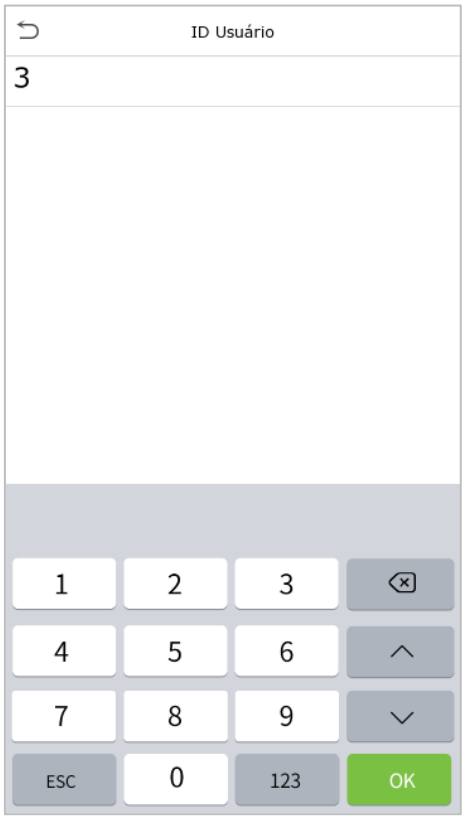
Clique em **Procurar Registros** na interface do **Menu Principal** para pesquisar o registro de Acesso/Presença necessário.



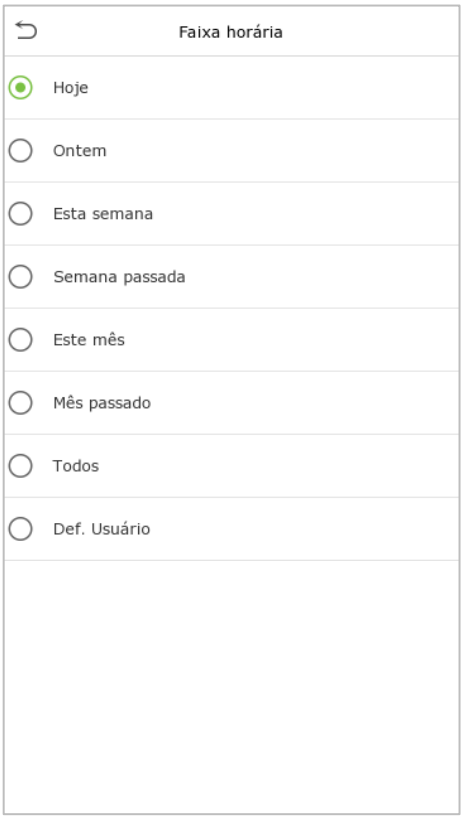
O processo de pesquisa de fotos de presença e lista de bloqueio é semelhante ao da pesquisa de logs de eventos. Veja a seguir um exemplo de pesquisa de logs de eventos.

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.

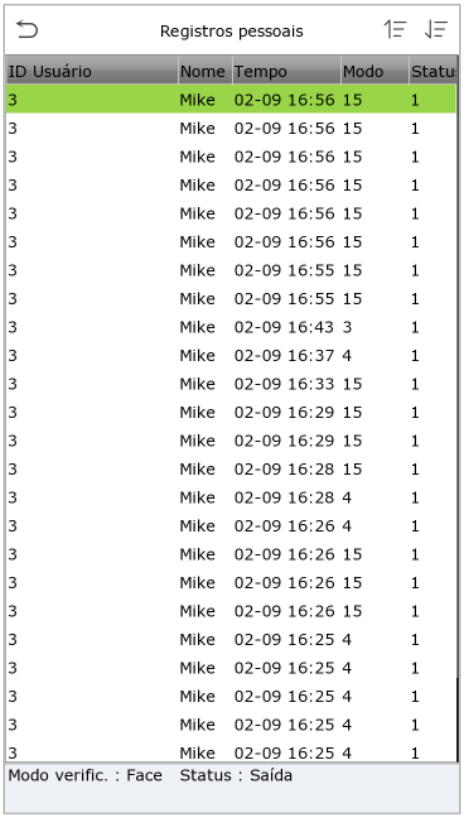


2. Selecione o intervalo de tempo em que os logs precisam ser pesquisados.



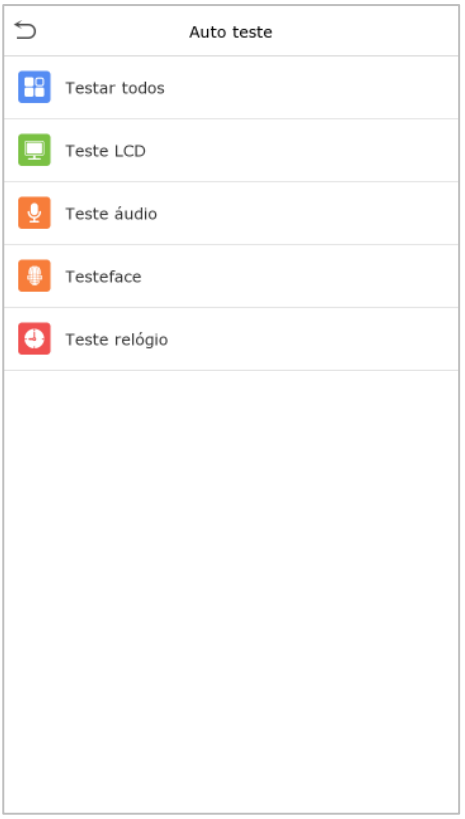
3. Depois que a pesquisa de log for bem-sucedida, toque no registro destacado em verde para visualizar seus detalhes.

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



11 Auto teste

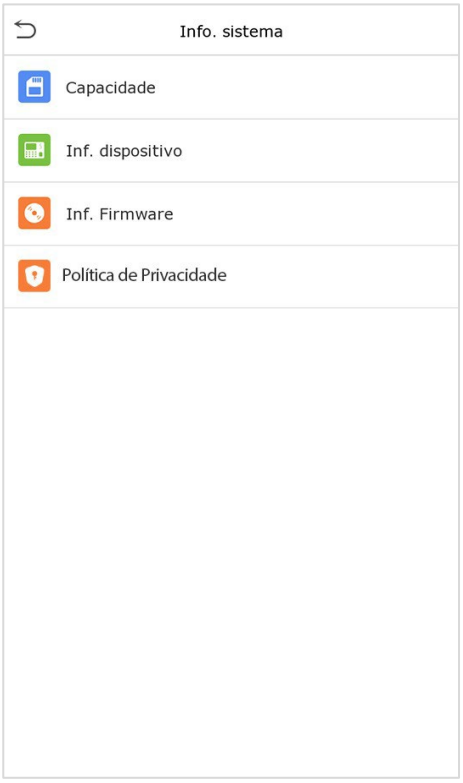
No Menu Principal, toque em **Auto teste** para testar automaticamente se todos os módulos do dispositivo funcionam corretamente, incluindo LCD, áudio, câmera e relógio em tempo real (RTC).



Menu	Descrição
Testar tudo	Para testar automaticamente se o LCD, áudio, câmera e relógio em tempo real (RTC) estão normais.
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 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.

12 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.

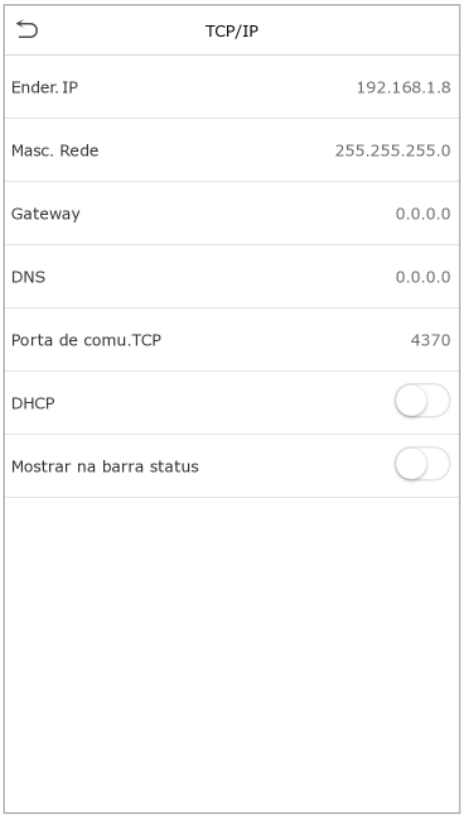
13 Conecte-se ao software ZKBioAccess IVS

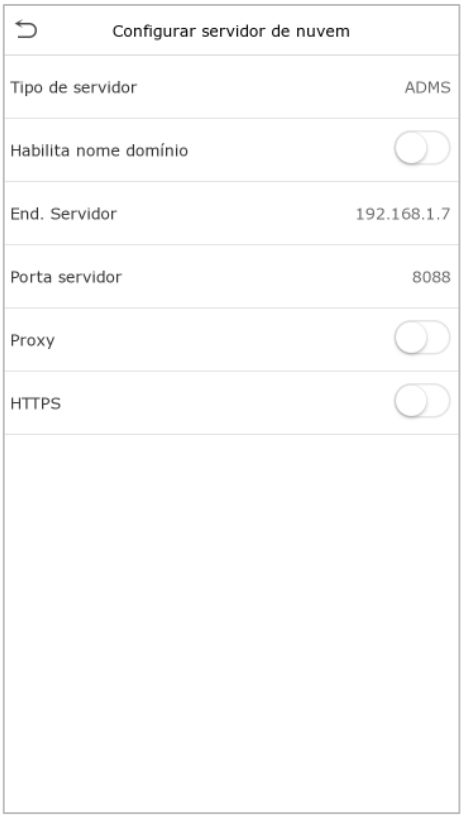
13.1 Defina o endereço de comunicação

Lado do dispositivo

1. Toque em **Conf. COMM. > TCP/IP** no menu principal para definir as configurações de rede. (Nota: O endereço IP deve ser capaz de se comunicar com o servidor ZKBioAccess IVS, preferencialmente no mesmo segmento de rede com o endereço do servidor)
2. No menu principal, clique em **Conf. COMM. >Configurar servidor de nuvem** para definir o endereço do servidor e a porta do servidor.

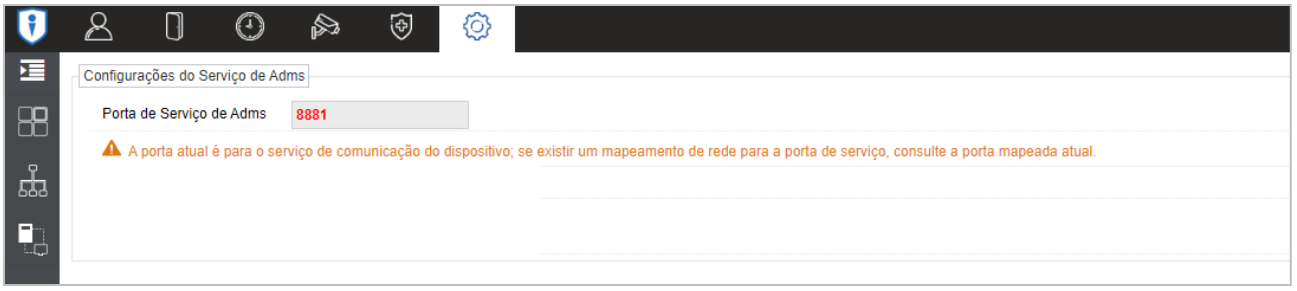
   Endereço do servidor: Defina o endereço IP do servidor ZKBioAccess IVS.
   Porta do servidor: Defina a porta do servidor como ZKBioAccess IVS (o padrão é 8088).





Lado do software

Faça login no software ZKBioAccess IVS, clique em **Sistema > Comunicação > Monitor de Comunicação** para conferir se a porta de serviço ADMS é a mesma definida no equipamento, conforme mostrado na figura abaixo:



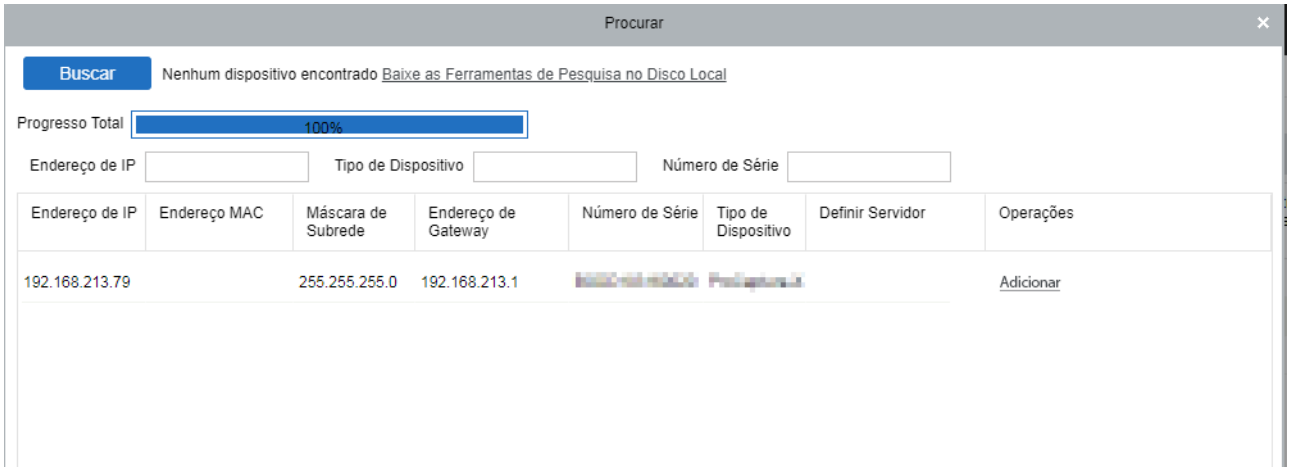
13.2 Adicionar dispositivo no software

Adicione o dispositivo por pesquisa. O processo é o seguinte:

1) Clique em **Acesso > Dispositivo > Procurar** para abrir a tela de pesquisa no software.

2) Clique em Pesquisar e ele mostrará [Pesquisando……].

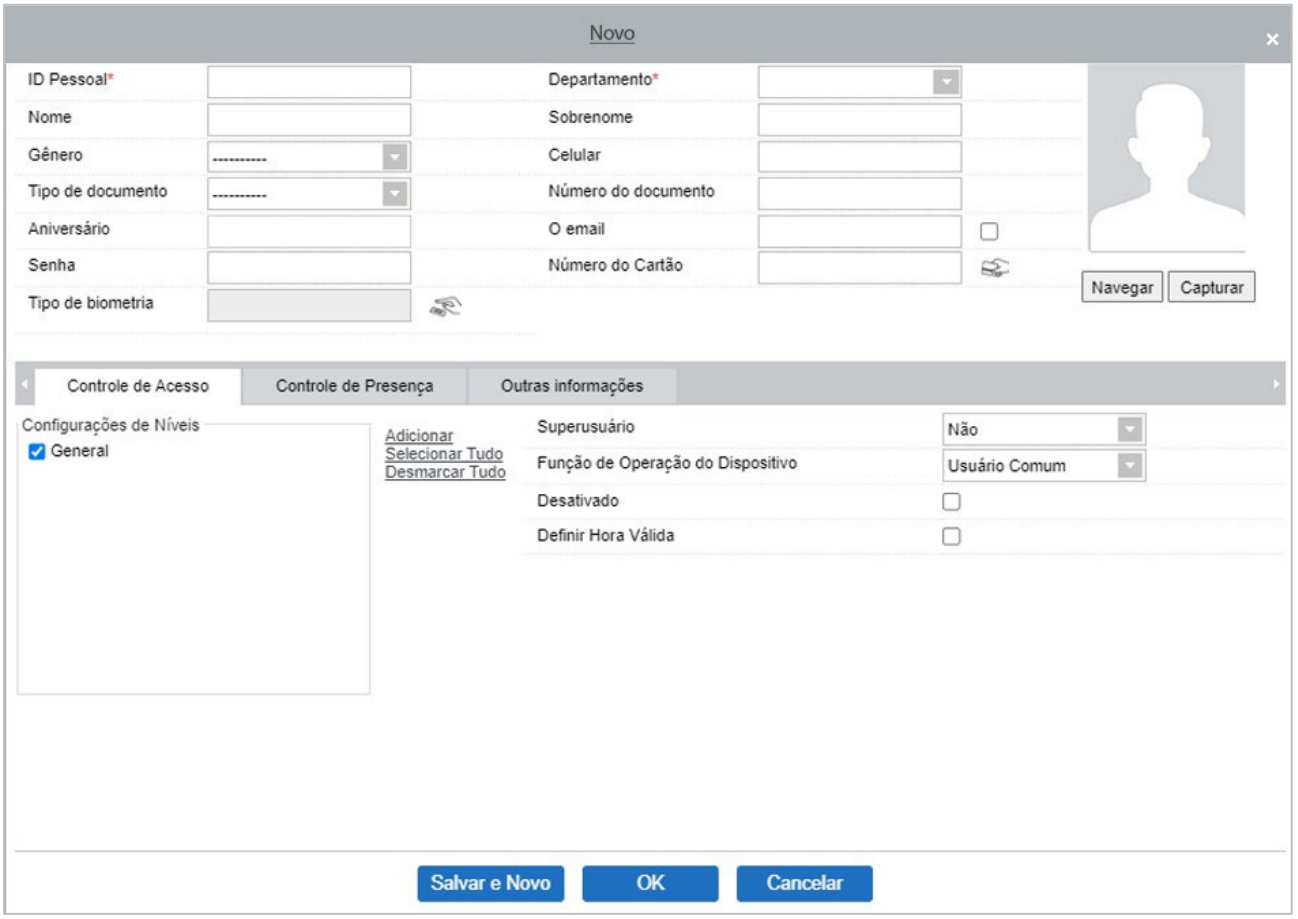
3) Após a pesquisa, a lista e o número total de equipamentos serão exibidas.



4) Clique em [**Adicionar**] na coluna de operações, uma nova janela aparecerá. Defina um Nome, selecione Tipo de ícone, Área e Adicionar ao nível e clique em [**OK**] para adicionar o dispositivo.

13.3 Adicionar uma pessoa fixa

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



2. Preencha todos os campos obrigatórios e clique em [**OK**] para cadastrar um novo usuário.
3. Clique em Acesso > Dispositivo > Controle de dispositivo > Sincronizar todos os dados com dispositivos para sincronizar todos os dados com o dispositivo, incluindo os novos usuários.

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

14 SIP

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

Apêndice 1

Requisitos para cadastro no equipamento e Upload de fotos no software

Cadastro no equipamento:

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

Upload de fotos no software

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

Distância dos olhos

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

Apêndice 2

Política de Privacidade

Aviso:

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.

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