Manual do Usuário

ProFaceX [P]

Versão: 1.0

Português

Green Label

Marca Registrada

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

Responsabilidade

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

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

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

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

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

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

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

ZKTeco filial Brasil

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

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

Sobre a empresa

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

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

Sobre o Manual

Este manual apresenta as operações do produto ProFace-X [P].

Todas as figuras exibidas são apenas para fins ilustrativos. Os números/medidas deste manual podem não ser exatamente consistentes com os produtos reais.

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

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

ANATEL 01094-23-12720	Módulo: IC11 "Incorpora produto homologado pela ANATEL sob número 01094-23-12720"
ANATEL 07935-23-12720	Módulo: MTR11 "Incorpora produto homologado pela ANATEL sob número 07935-23-12720"
ANATEL 07937-23-12720	Módulo: MTR10 "Incorpora produto homologado pela ANATEL sob número 07937-23-12720"
ANATEL 12509-20-12720	Módulo: IC01 (M330-L_V3.4) "Incorpora produto homologado pela ANATEL sob número 12509-20-12720"
ANATEL 14815-21-12720	Módulo: EM05 (V2.01) "Incorpora produto homologado pela ANATEL sob número 14815-21-12720"
ANATEL 11891-22-11470	Módulo: L287B-SR "Incorpora produto homologado pela ANATEL sob número 11891-22-11470"

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

Padronização dos documentos

Os padrões usados neste manual estão listados abaixo:

Convenções de Interface Gráfica do Usuário:

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

Símbolos

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

Índice

1 VISÃO GERAL 7

2 INSTRUÇÕES DE USO 7

2.1 POSIÇÃO EM PÉ, POSTURA E EXPRESSÃO FACIAL 7
2.2 CADASRO DE PALMA 8
2.3 CADASTRO DE FACE 9
2.4 TELA PRINCIPAL 10
2.5 TECLADO VIRTUAL 11
2.6 MODO DE AUTENTICAÇÃO 12
2.6.1 AUTENTICAÇÃO DE PALMA 12
2.6.2 AUTENTICAÇÃO DE SENHA 14
2.6.3 AUTENTICAÇÃO FACIAL 17
2.6.4 AUTENTICAÇÃO COMBINADA 20

3 MENU PRINCIPAL 21

4 GESTÃO DE USUÁRIO 22

4.1 CADASTRO DE USUÁRIOS 22
4.2 PROCURA DE REGISTROS 26
4.3 EDITAR USUÁRIOS 27
4.4 EXCLUIR USUÁRIOS 27

5 PRIVILÉGIO DO USUÁRIO 28

6 CONFIGURAÇÕES DE COMUNICAÇÃO 31

6.1 CONFIGURAÇÕES TCP/IP 31
6.2 CONEXÃO DO PC 33
6.3 CONFIGURAÇÕES DO SERVIDOR NUVEM 33
6.4 CONFIGURAÇÃO DE WIEGAND 34

7 CONFIGURAÇÕES DO SISTEMA 38

7.1 DATA E HORA 38
7.2 CONFIGURAÇÃO DE REGISTROS DE ACESSO 39
7.3 PARÂMETROS DE FACE 40
7.4 PARÂMETROS DE PALMA 42
7.5 RESTAURAÇÃO DOS PADRÕES DE FÁBRICA 43
7.6 GERENCIAMENTO DE TEMPERATURA 44

8 CONFIGURAÇÕES DE PERSONALIZAÇÃO 45

8.1 CONFIGURAÇÕES DE EXIBIÇÃO 45
8.2 CONFIGURAÇÕES DE VOZ 46
8.3 HORÁRIOS 46
8.4 CONFIGURAÇÕES DE STATUS DE REGISTRO DE PRESENÇA 48

8.5 MAPEAMENTOS DE TECLAS DE ATALHOS 49
9 GERENCIAMENTO DE DADOS 50
9.1 EXCLUIR DADOS 50
10 CONTROLE DE ACESSO 52
10.1 OPÇÕES DE CONTROLE DE ACESSO 53
10.2 REGRAS DE HORÁRIO 55
10.3 FERIADOS 57
10.4 ACESSO COMBINADO 57
10.5 ANTI-PASSBACK 59
10.6 OPÇÕES DE COAÇÃO 60
11 PROCURAR REGISTROS 61
12 AUTO TESTE 64
13 INFORMAÇÃO DO SISTEMA 65
14 CONECTE-SE AO SOFTWARE ZKBIOACCESS IVS 66
14.1 DEFINA O ENDEREÇO DE COMUNICAÇÃO 66
14.2 ADICIONAR DISPOSITIVO NO SOFTWARE 67
14.3 ADICIONAR UMA PESSOA FIXA 68
APÊNDICE 1 69
GARANTIA 72

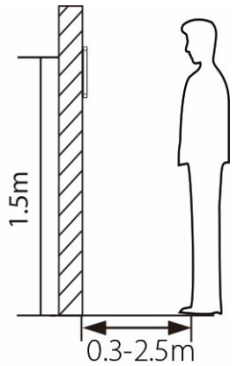
1 Visão Geral

Este documento descreve o procedimento operacional do dispositivo ProFace X [P]. Os módulos operacionais do dispositivo incluem gerenciamento de usuário, atribuição de função do usuário, comunicação do dispositivo, controle de acesso e assim por diante. O dispositivo suporta o acesso sem complicações dos usuários às instalações, sem comprometer nenhum aspecto de segurança, garantindo a proteção.

2 Instruções de Uso

2.1 Posição em Pé, Postura e Expressão Facial

A distância recomendada



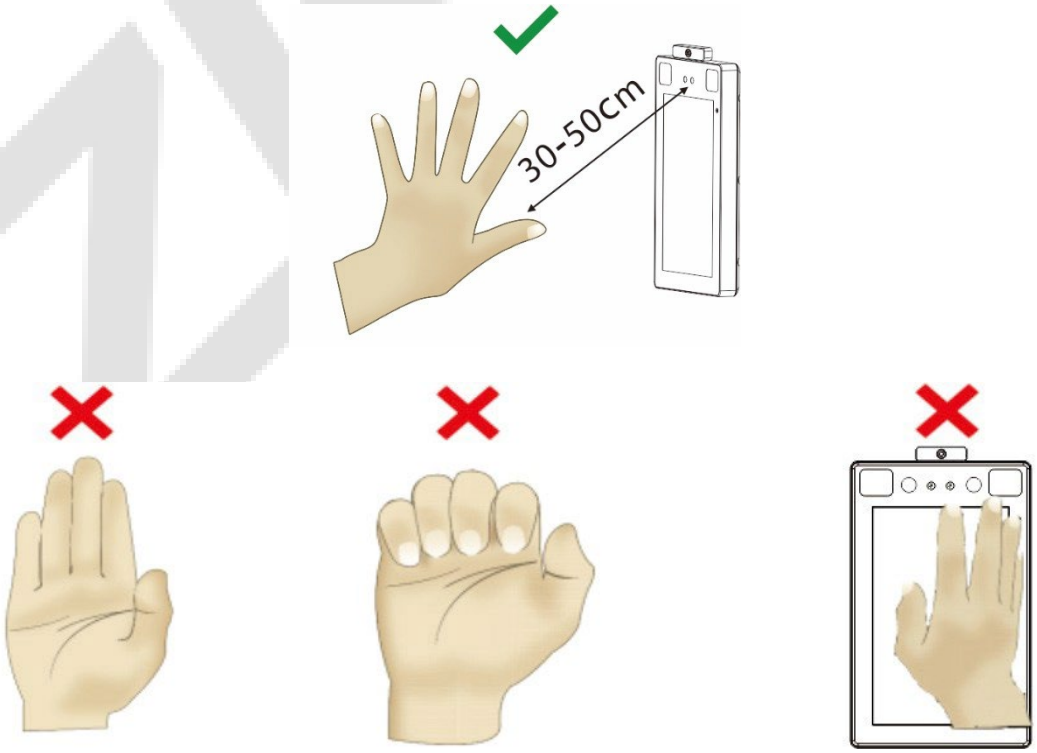
Recomenda-se que a distância entre o dispositivo e um usuário cuja altura esteja entre 1,55 m e 1,85 m seja de 0,3m a 2m. Os usuários podem se aproximar ou se afastar um pouco para melhorar a qualidade das imagens faciais capturadas.

Postura em pé e expressão facial recomendadas

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

2.2 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.



2.3 Cadastro de face

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

Modo correto de cadastro de face e método de autenticação

Recomendação para cadastro de face

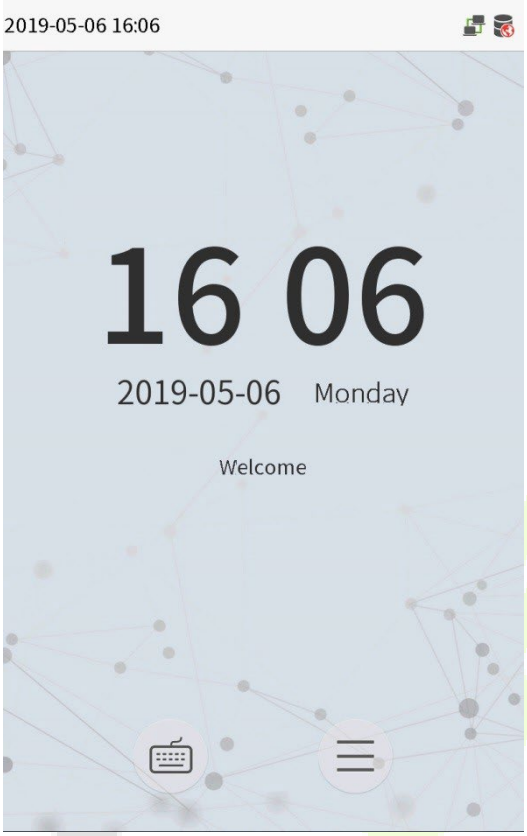
- Ao cadastrar uma face, mantenha uma distância de 40 cm a 80 cm entre o dispositivo e a face.
- Tenha cuidado para não mudar sua expressão facial. (Ex.: sorriso, etc.)
- Se você não seguir as instruções na tela, o cadastro de face pode demorar mais ou pode falhar.
- Tenha cuidado para não cobrir os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

Recomendação para autenticar uma face

- Certifique-se de que a face apareça dentro da guia exibida na tela do dispositivo.
- Se os óculos foram trocados, a autenticação pode falhar. Se a face sem óculos tiver sido cadastrada, autentique sem óculos. Se a face com óculos foi cadastrada, autentique com os óculos.
- Se uma parte do rosto estiver coberta com um chapéu, boné, máscara, tapa-olho ou óculos de sol, a autenticação pode falhar. Não cubra a face, permita que o dispositivo veja as sobrancelhas e a face.

2.4 Tela principal

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

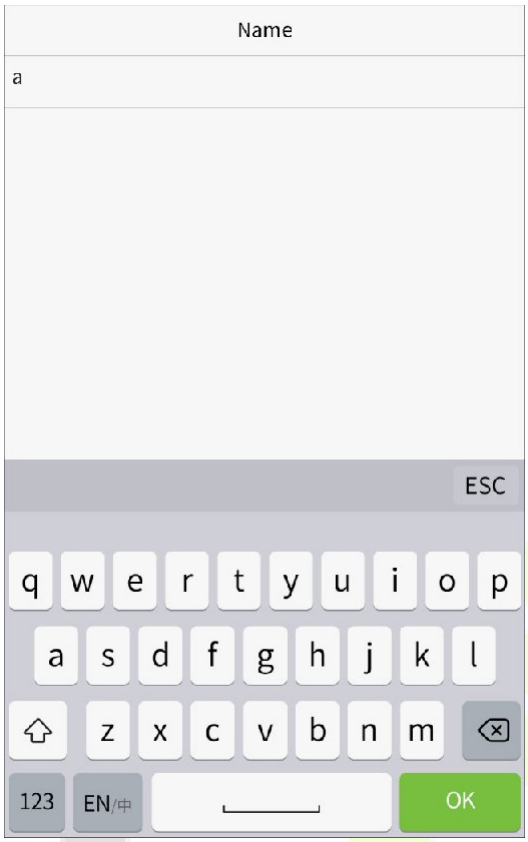


Note:

1）Clique em para autenticar com ID do usuário

Quando não houver um super administrador cadastrado no dispositivo, clique em para configurar o super administrador. O dispositivo passará a requerer a verificação do super administrador antes de entrar na operação do menu. Para a segurança do dispositivo, é recomendável registrar um super administrador na primeira vez que você usar o dispositivo.

2.5 Teclado Virtual



NOTA:

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

• Clique em [**En**] para alternar para o teclado em inglês.

• Pressione [**123**] para alternar para o teclado numérico e simbólico.

• Clique em [**ABC**] para retornar ao teclado alfabético.

• Clique na caixa de entrada para o teclado virtual ser exibido.

• Clique em [**ESC**] para sair do teclado virtual

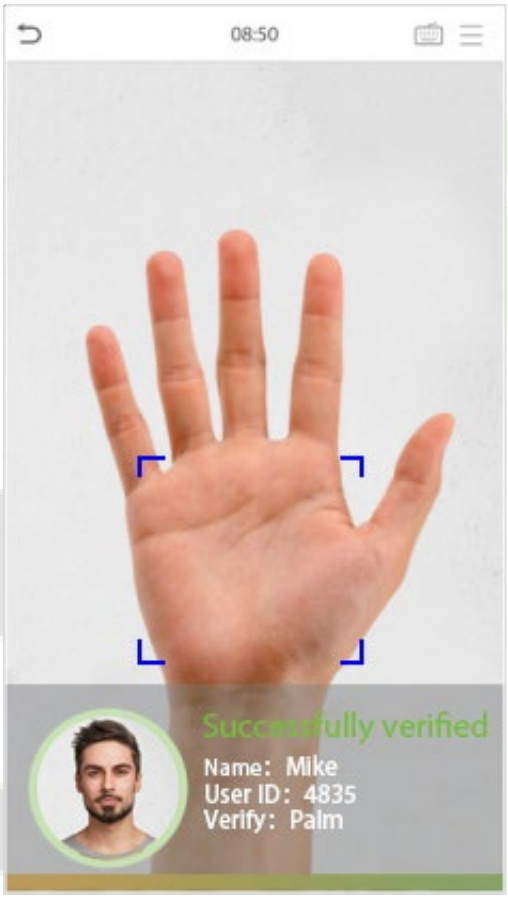
2.6 Modo de autenticação

2.6.1 Autenticação de Palma

Modo de autenticação de Palma 1:N

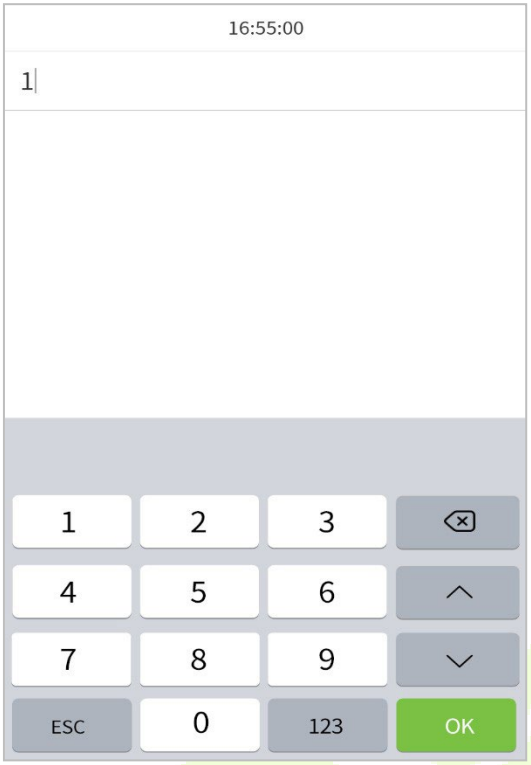
Nesse modo de autenticação, o dispositivo compara a imagem da palma coletada com todos os dados da palma cadastrados no equipamento.

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.

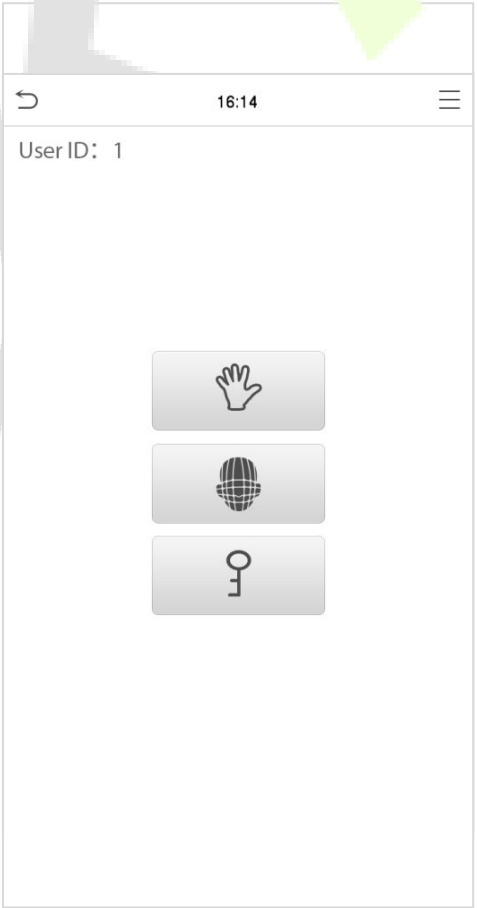


Modo de autenticação de Palma 1:1

Clique no botão na tela principal para entrar no modo de autenticação de palma 1:1, insira o ID do usuário e pressione [**OK**], conforme mostrado na imagem abaixo.



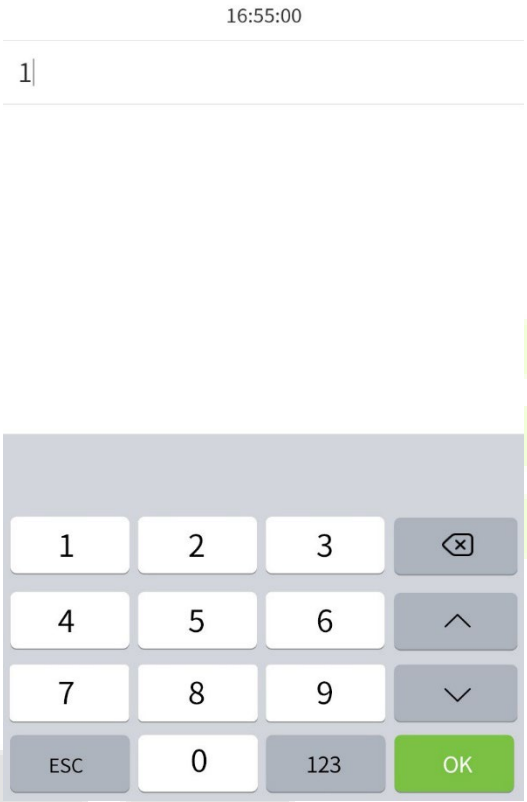
Caso o usuário possua face, cartão e senha cadastrados além de sua palma e o método de autenticação estiver configurado para autenticação palma/ face/ cartão/ senha, a tela a seguir será exibida. Selecione o ícone para entrar no modo de autenticação da palma da mão. Em seguida, posicione a palma para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



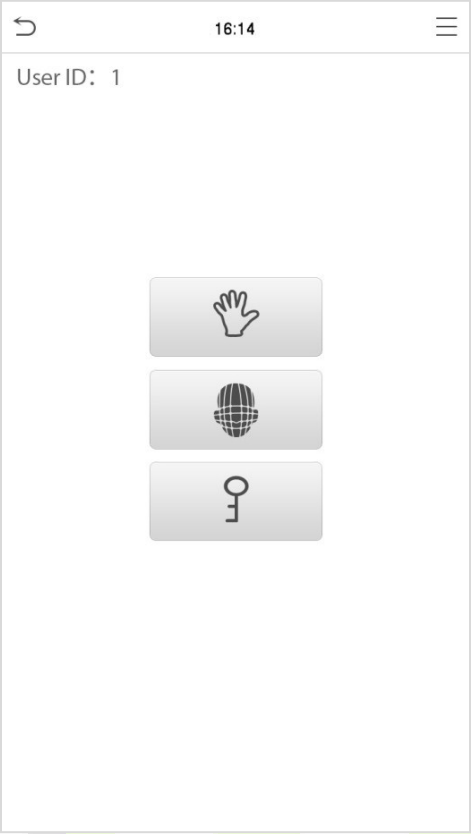
2.6.2 Autenticação de senha

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

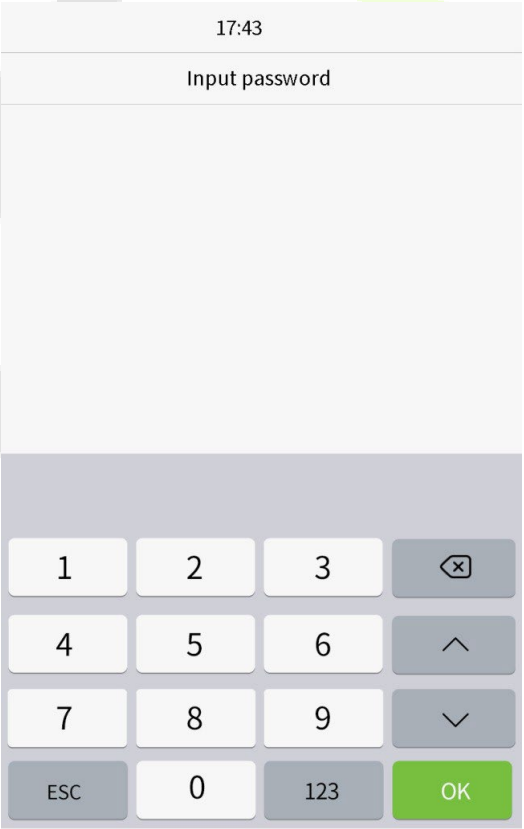
Clique no botão na tela principal para entrar no modo de autenticação de senha 1:1. Em seguida, insira o ID do usuário e pressione [**OK**].



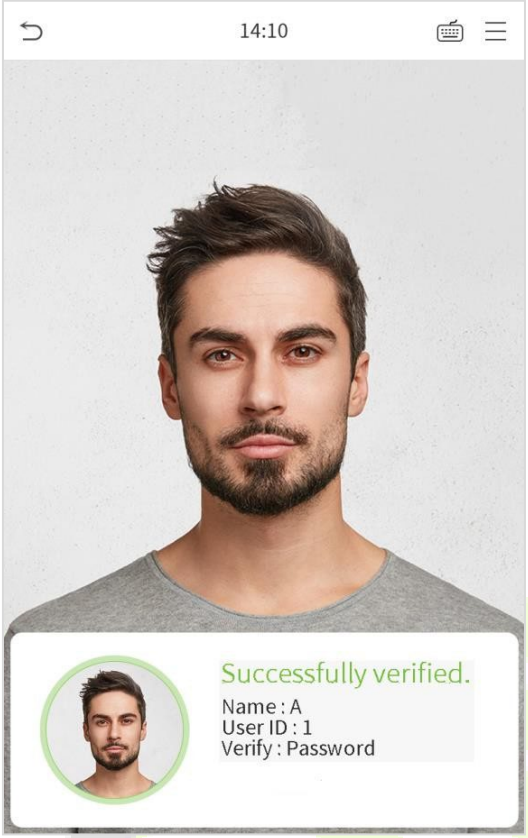
Se o usuário tiver cadastrado palma, face e cartão, além da senha e o método de autenticação estiver configurado para palma/face/cartão/senha, a tela a seguir será exibida. Selecione para acessar o modo de autenticação por senha.



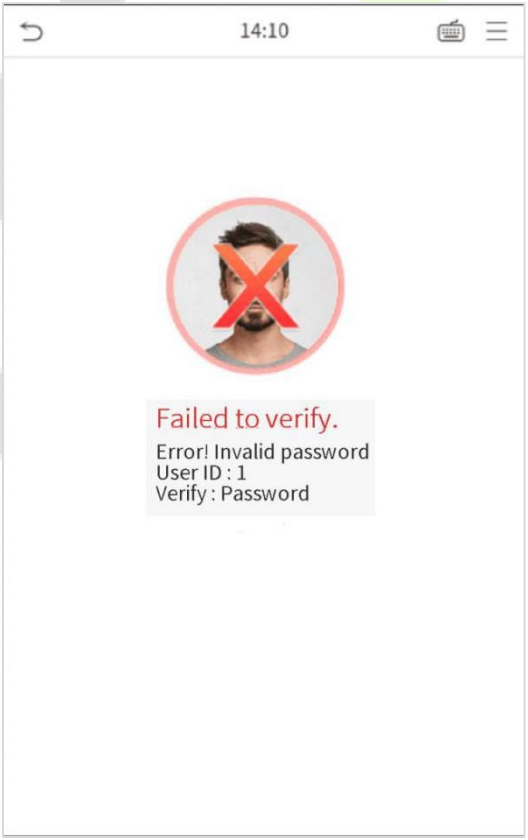
Insira a senha e pressione [**OK**].



A autenticação foi bem-sucedida:



A autenticação falhou:

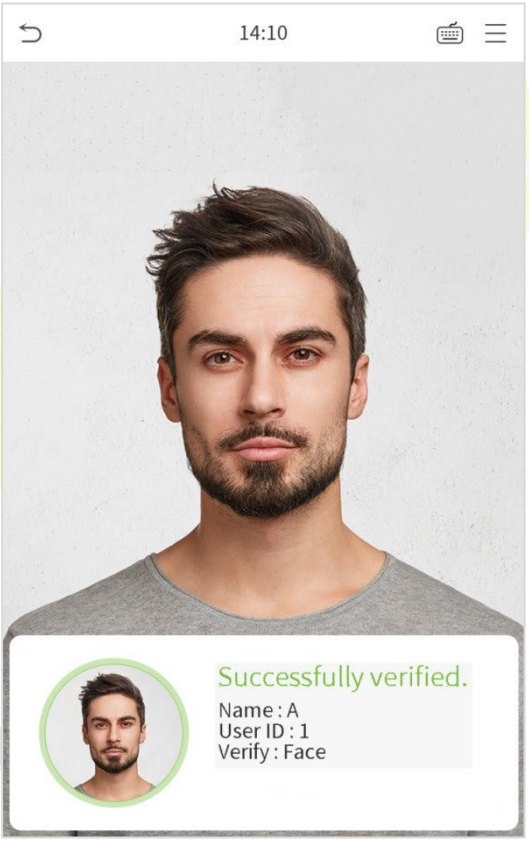


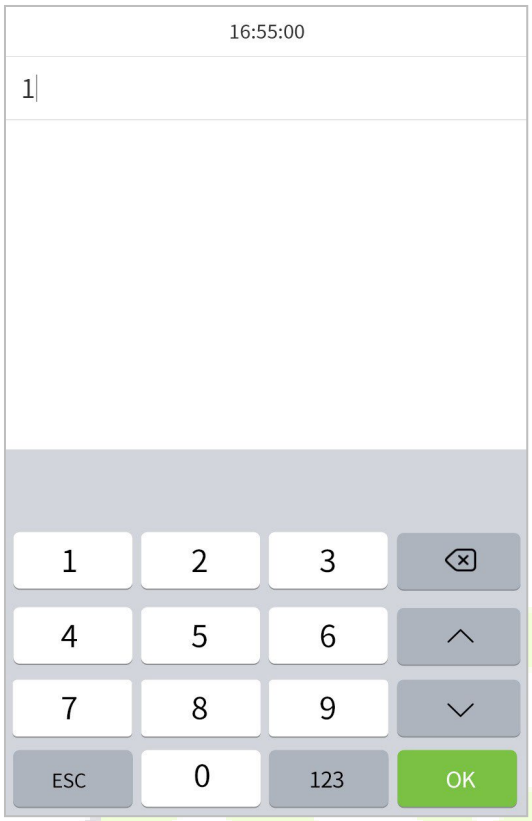
2.6.3 Autenticação Facial

Autenticação facial 1:N (um para muitos)

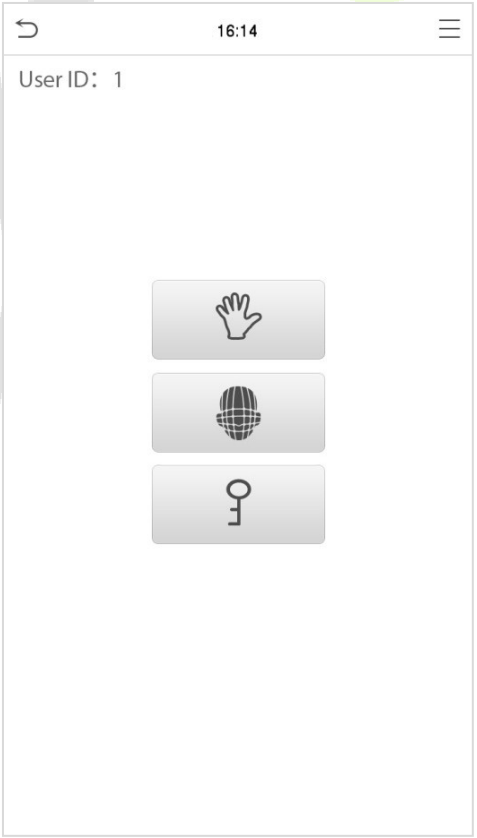
1. **Autenticação Convencional**

Este modo de verificação compara as imagens faciais adquiridas com todos os dados faciais registrados no dispositivo. A seguir está a caixa de mensagem do resultado da comparação

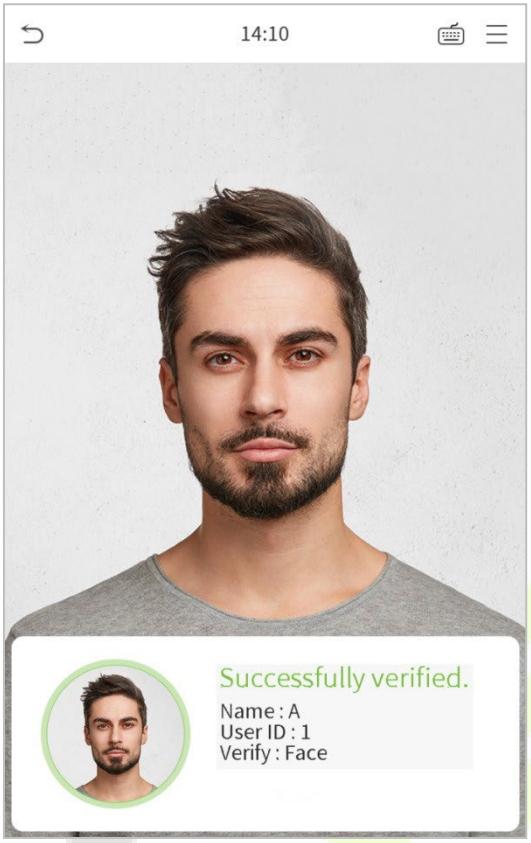




Se o usuário tiver registrado palm, cartão e senha além do seu rosto, e o método de verificação estiver configurado para palma/face/cartão/senha de verificação, a tela a seguir será exibida. Selecione para entrar no modo de verificação facial.



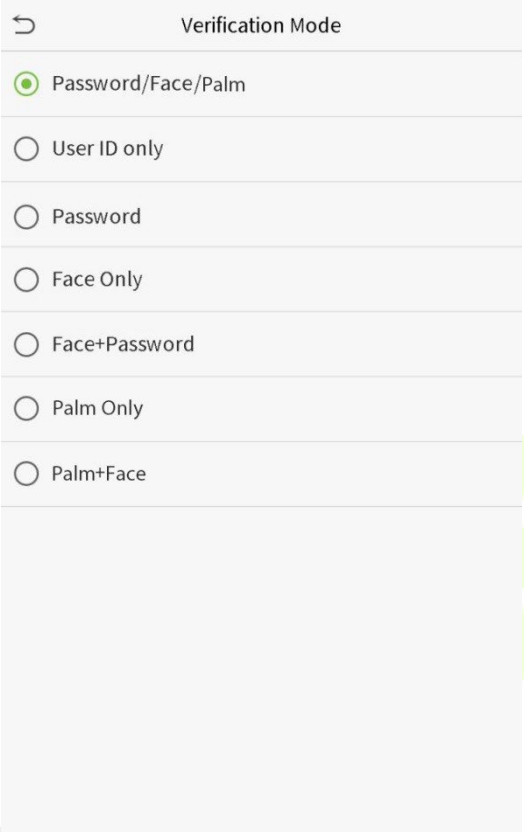
Após a verificação bem-sucedida, será exibida a mensagem "Verificado com sucesso", conforme mostrado abaixo:



Se a verificação falhar, ele solicitará “Ajuste sua posição!”.

2.6.4 Autenticação Combinada

Para aumentar a segurança, este dispositivo oferece a opção de usar vários métodos de autenticação. Um total de 7 combinações de autenticações diferentes podem ser usadas, conforme mostrado abaixo:



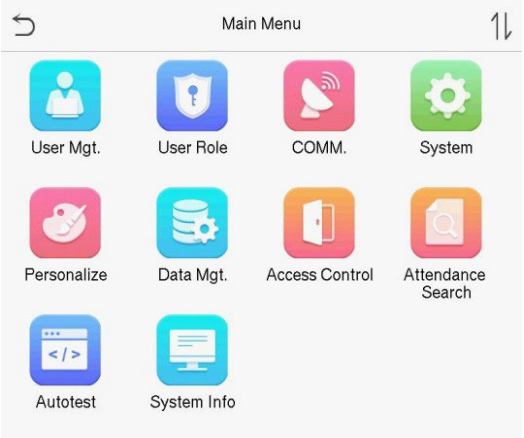
Nota:

1） "/" significa “ou”, e "+" significa “e”.

2） Você deve registrar as informações de verificação necessárias antes de usar o modo de verificação de combinação, caso contrário, a verificação poderá falhar. Por exemplo, se um usuário usar o Registro de Face, mas o modo de verificação for Face + Senha, esse usuário nunca passará na verificação.

3 Menu Principal

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

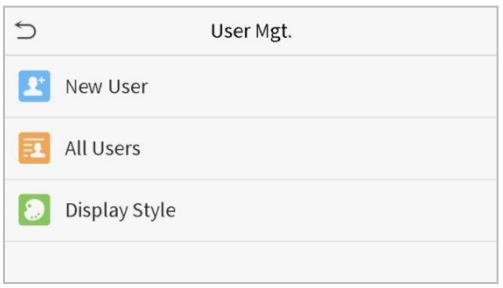


Menu	Descrição
Usuário Adm.	Para adicionar, editar, visualizar e excluir informações básicas de um usuário.
Priv. Usuário	Para definir o escopo de permissão da função personalizada e de cadastrador para os usuários, ou seja, os direitos para utilizar o sistema.
Conf. Com.	Para definir os parâmetros de 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, registros de acesso, modelos faciais, modelos de palma, modelos de impressão digital, redefinir as configurações de fábrica, gerenciamento de temperatura e gerenciamento de detecção.
Personalização	Isso inclui configurações de Interface do Usuário, Voz, Horários, Status de Ponto e Teclas de Atalho.
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, autenticação combinada, 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.
Informações do Sistema	Para visualizar a capacidade de dados, as informações do dispositivo e do firmware do dispositivo atual.

4 Gestão de Usuário

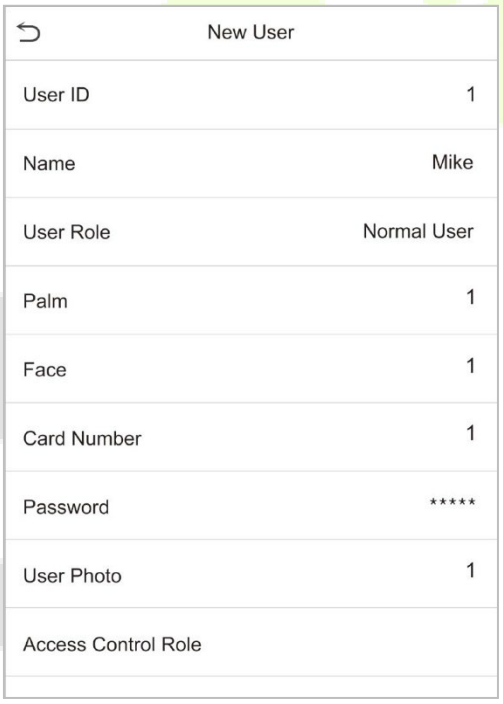
4.1 Cadastro de Usuários

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



ID de usuário e nome

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



Notas:

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.

Configurando os privilégios de usuário

Existem dois tipos de contas de usuário: **usuário normal** e **super administrador**. Se já houver um administrador cadastrado, os usuários normais não têm direitos para gerenciar o sistema e só podem acessar as verificações de autenticação. O Administrador possui todos os privilégios de gerenciamento. Se uma função personalizada for definida, você também poderá selecionar permissões de função definidas pelo usuário para o usuário.

Clique em Privilégio de Usuário para selecionar **Usuário normal** ou **Super administrador**.

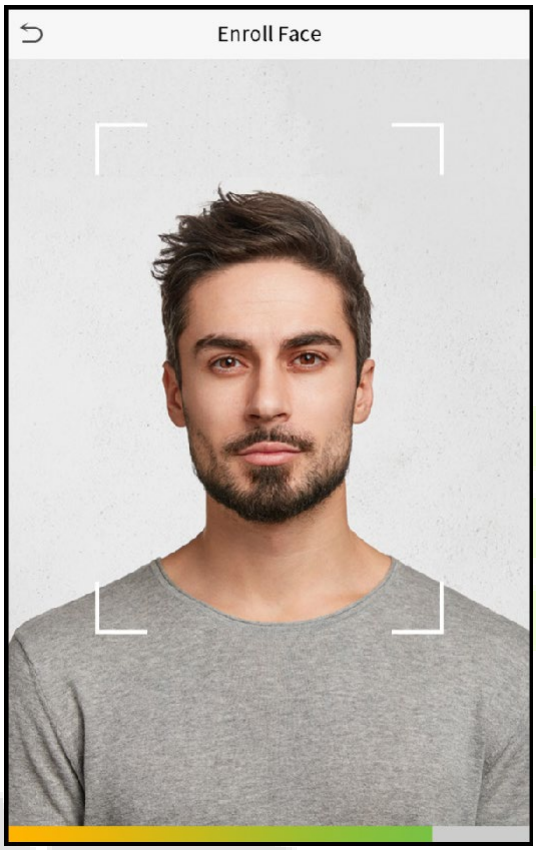
Nota: Se a função de usuário selecionada for o superadministrador, o usuário deve passar pela autenticação de identidade para acessar o menu principal. A autenticação é baseada no(s) método(s) de autenticação que o super administrador registrou. Consulte 2.6 Modo de verificação.

Registrar palma

Clique em Palma para abrir a página de registro de palma. Selecione a palma a ser cadastrada.

Registrar palma

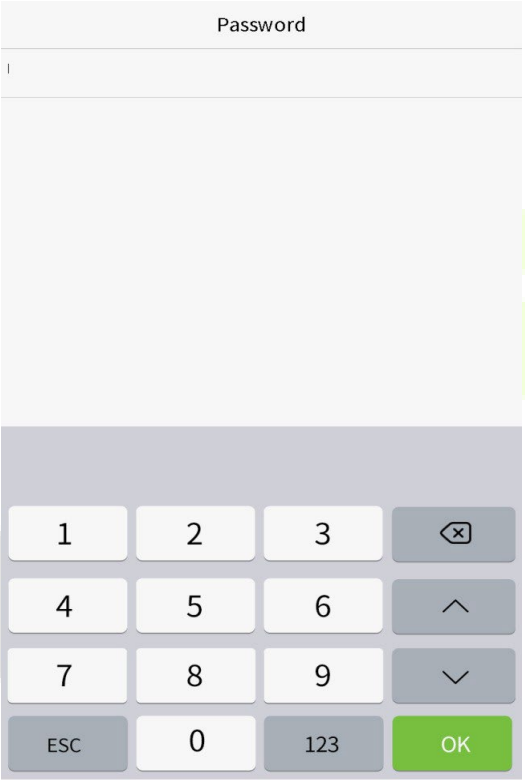
Clique em Face para entrar na página de registro da face. Por favor, fique de frente para a câmera e fique parado durante o registro da face. A interface de registro é a seguinte



Cadastrar senha

Clique em Senha para abrir a página de registro de senha. Digite uma senha e, em seguida, digite-a novamente. Clique OK. Se as duas senhas inseridas forem diferentes, o prompt "Senha não corresponde" aparecerá.

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



Cadastrar foto do usuário

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

Toque em **Foto do Usuário** na interface do **Novo Usuário** para ir para a página de cadastro de 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

Função de controle de acesso

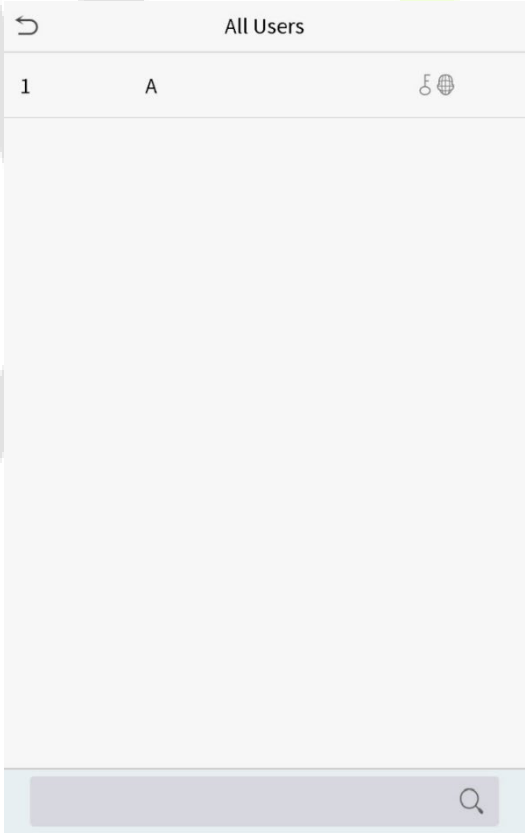
A **Função de Controle de Acesso** define o privilégio de acesso à porta para cada usuário. Isso inclui o grupo de acesso, o modo de verificação e, também, facilita a definição do período de acesso do grupo.

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.

Toque em **Período de Tempo** para selecionar o período de tempo a ser usado.

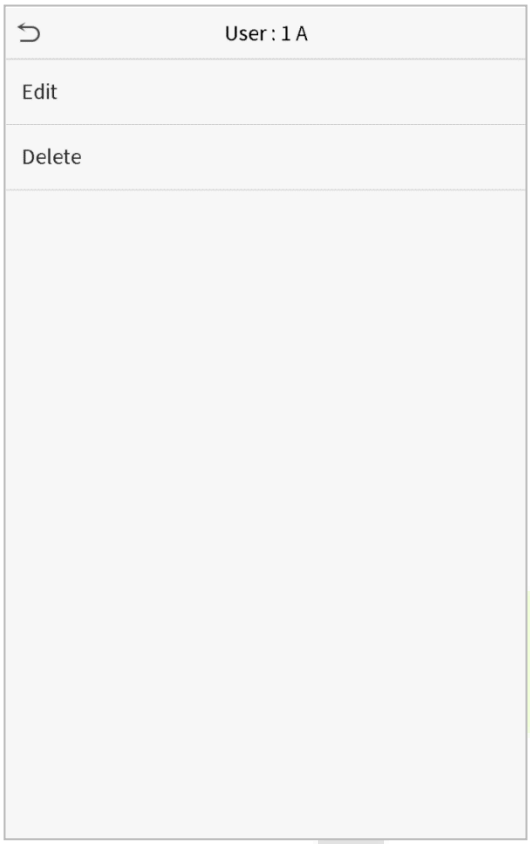
4.2 Procura de registros

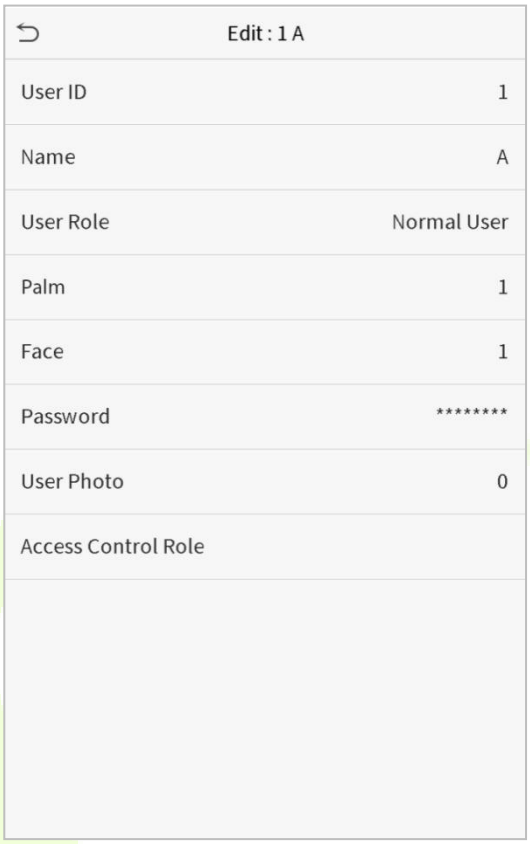
Clique na barra de pesquisa na lista de usuários e digite a palavra-chave de recuperação (A palavra-chave pode ser um ID, sobrenome ou nome completo). O sistema buscará os usuários relacionados às informações.



4.3 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. O processo em detalhe refere-se a 4.1 Cadastro de Usuários

4.4 Excluir Usuários

Selecione um usuário na lista e clique em Excluir para entrar na interface do usuário de exclusão. Selecione as informações do usuário a serem excluídas e clique em OK.

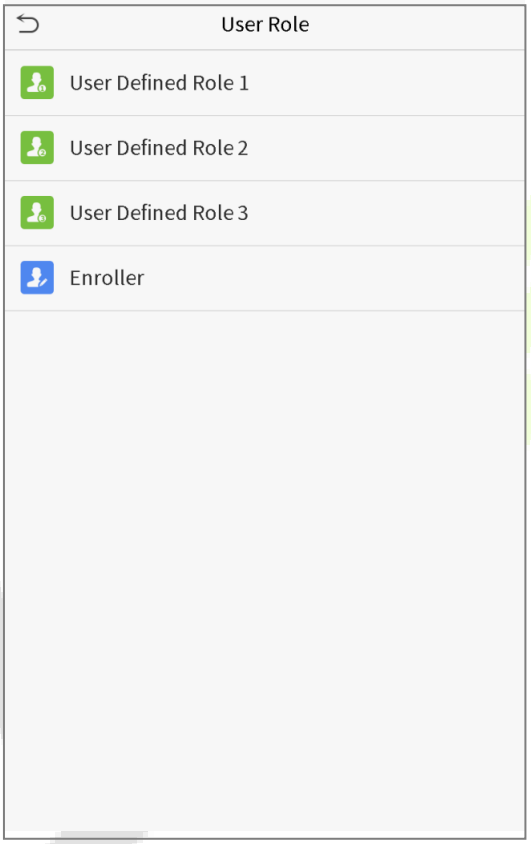
Nota: Se você selecionar Excluir usuário, todas as informações do usuário serão excluídas.

5 Privilégio do Usuário

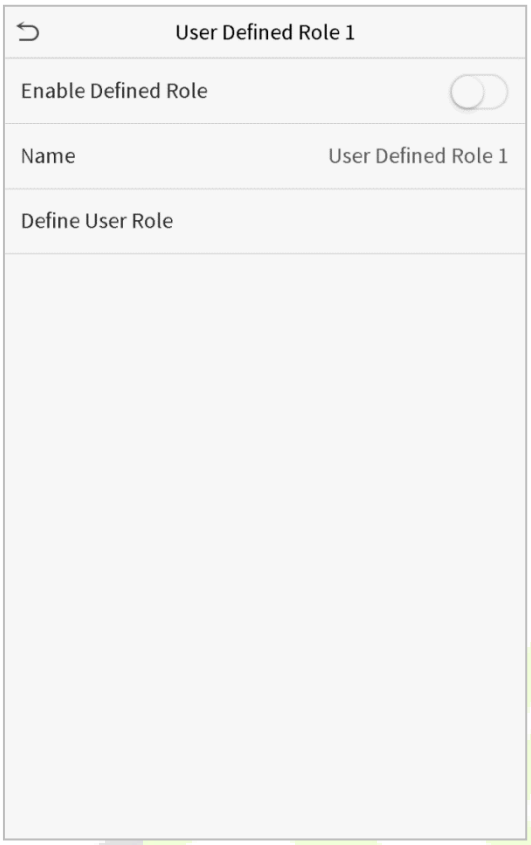
O **Privilégio do Usuário** facilita a atribuição de algumas permissões específicas a determinados usuários, com base no que foi selecionado.

- No **Menu Principal**, toque em **Priv. Usuário** e, em seguida, toque em **Usuário Personalizado** para definir as permissões desse grupo.

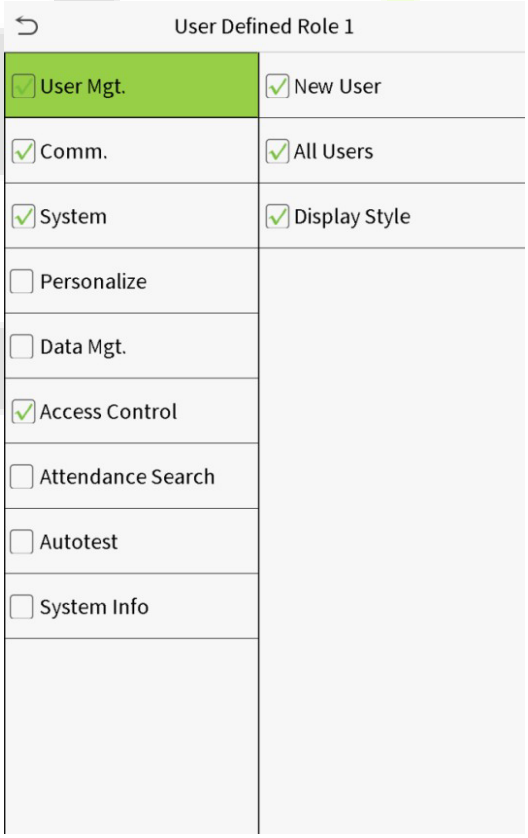
A delimitação de permissão da função personalizada pode ser configurada em até 3 grupos



1. Na interface **Usuário Personalizado**, selecione em **Habilitar Usuário Personalizado** para ativar ou desativar a função do grupo selecionado.
2. Toque em **Nome** e insira o nome personalizado da função.



3. Clique em **Definir privilégio de usuário** para atribuir privilégios à função. Quando a atribuição de privilégio for concluída, clique em Retornar.



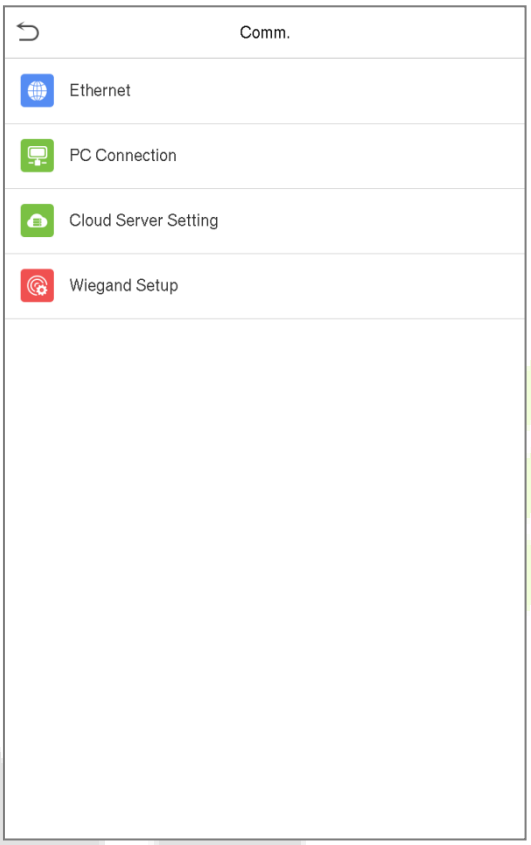
Nota: Durante a atribuição de privilégios, o menu principal fica à esquerda e seus submenus à direita. Você só precisa selecionar os recursos nos submenus. Se o dispositivo tiver uma função habilitada, você poderá atribuir as funções que definiu aos usuários clicando em **Gestão de usr. > Novo usuário > Função de usuário**.

Se nenhum super administrador estiver registrado, o dispositivo solicitará "Registre primeiro o usuário super administrador!" depois de clicar na barra de ativação.

6 Configurações de comunicação

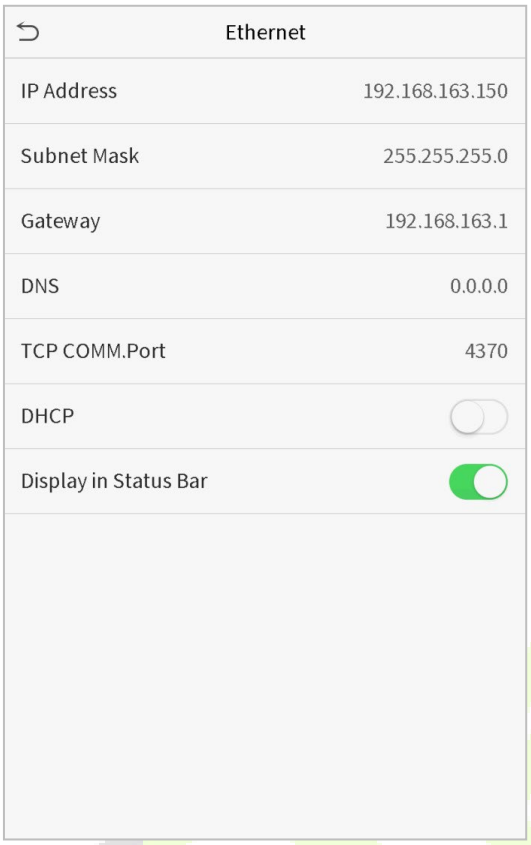
Toque em **Conf. Com.** no **Menu Principal** para definir a conexão com o PC, configuração da Nuvem e de Wiegand.

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



6.1 Configurações TCP/IP

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

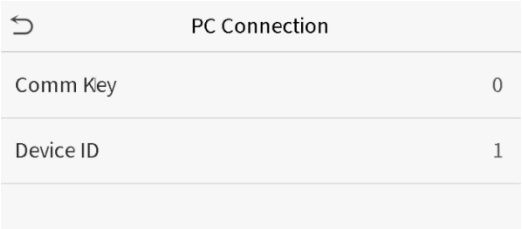


Nome da função	Descrição
TCP/IP	O valor de fábrica é 192.168.1.201 e pode ser editado;
Máscara de Rede	O valor de fábrica é 255.255.255.0 e pode ser editado;
Gateway	O valor de fábrica é 0.0.0.0 e pode ser editado;
DNS	O valor de fábrica é 0.0.0.0 e pode ser editado;
Porta de Comunicação TCP	O valor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

6.2 Conexão do PC

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

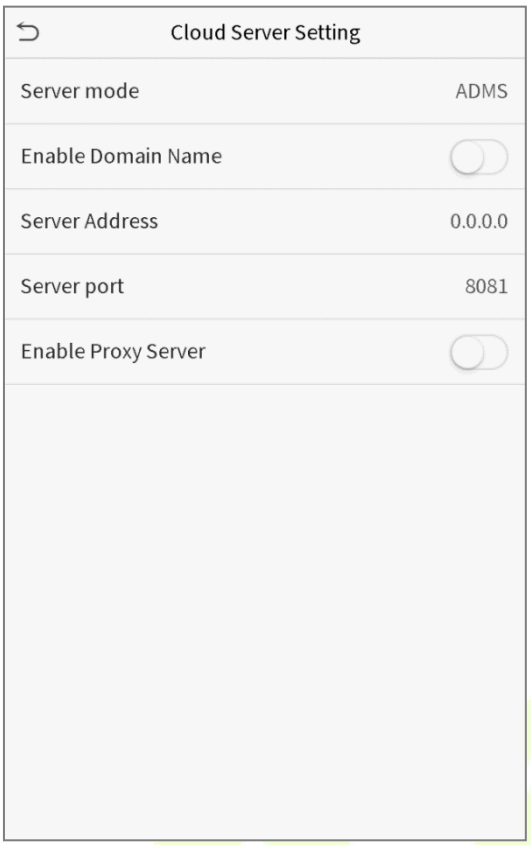
Toque em **Conexão do PC** na interface de configurações de comunicação para defini-las.



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

6.3 Configurações do servidor de nuvem

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

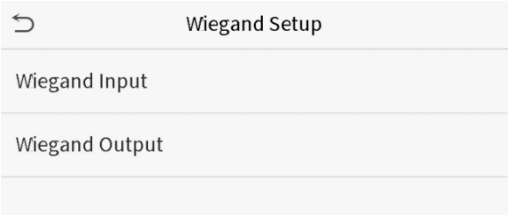


Menu		Descrição
Ativar nome de domínio	**Endereço do servidor**	Uma vez habilitada esta função, será utilizado o modo de nome de domínio "http://...", como http://www.XYZ.com, enquanto "XYZ" será o nome de domínio (quando este modo está **LIGADO**).
Desativar nome de domínio	**Endereço do servidor**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

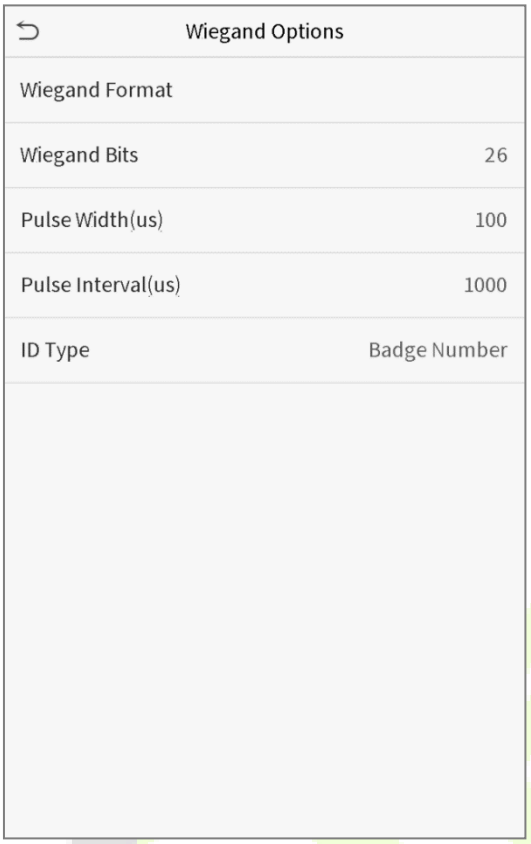
6.4 Configuração de Wiegand

Para definir os parâmetros de entrada e saída Wiegand.

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



Entrada Wiegand



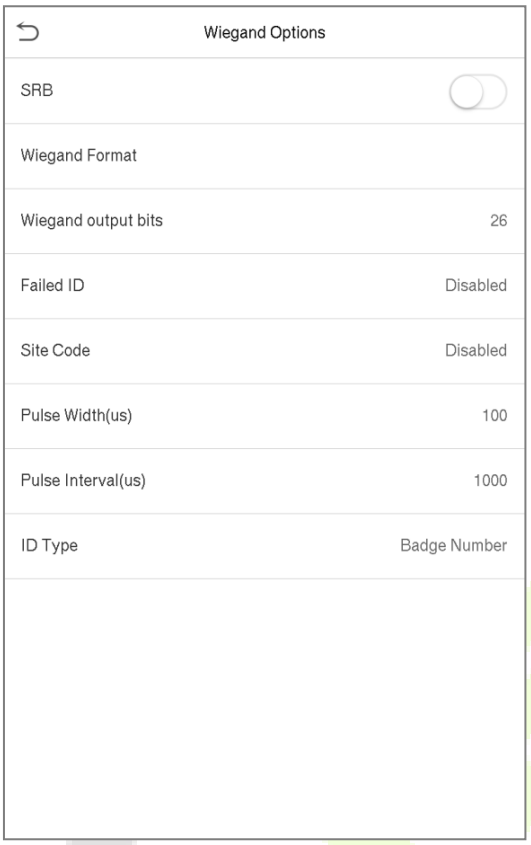
Nome da função	Descrição
Formato Wiegand	Os valores variam de 26 bits, 34 bits, 36 bits, 37 bits e 50 bits.
Bits de saída Wiegand	Após selecionar o formato Wiegand necessário, selecione os dígitos de bit de saída correspondentes do formato Wiegand.
Largura do pulso (us)	O valor da largura de pulso enviado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

Descrição dos formatos mais comuns de Wiegand:

Formato Wiegand	Descrição
Wiegand26	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	OFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME Consiste em 36 bits de código binário. O 1º bit é o bit de paridade ímpar do 2º ao 18º bits, enquanto o 36º bit é o bit de paridade par do 19º ao 35º bits. O 2º ao 17º bits são os códigos do dispositivo. Os bits 18 a 33 são os números do cartão e os bits 34 a 35 são os códigos do fabricante.
Wiegand36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO Consiste em 36 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 18º bits, enquanto o 36º bit é o bit de paridade ímpar do 19º ao 35º bits. O 2º ao 19º bits são os códigos do dispositivo e os 20º ao 35º bits são os números do cartão.
Wiegand37	OMMMMSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE Consiste em 37 bits de código binário. O 1º bit é o bit de paridade ímpar do 2º ao 18º bits, enquanto o 37º bit é o bit de paridade par do 19º ao 36º bits. O 2º ao 4º bits são os códigos do fabricante. O 5º ao 16º bits são os site code e os 21º ao 36º bits são os números do cartão.
Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consiste em 37 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 18º bits, enquanto o 37º bit é o bit de paridade ímpar do 19º ao 36º bits. O 2º ao 4º bits são os códigos do fabricante. O 5º ao 14º bits são os códigos do dispositivo, e o 15º ao 20º bits são os site code e os 21º ao 36º bits são os números do cartão.
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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 e **"S"** site code.	

Saída Wiegand

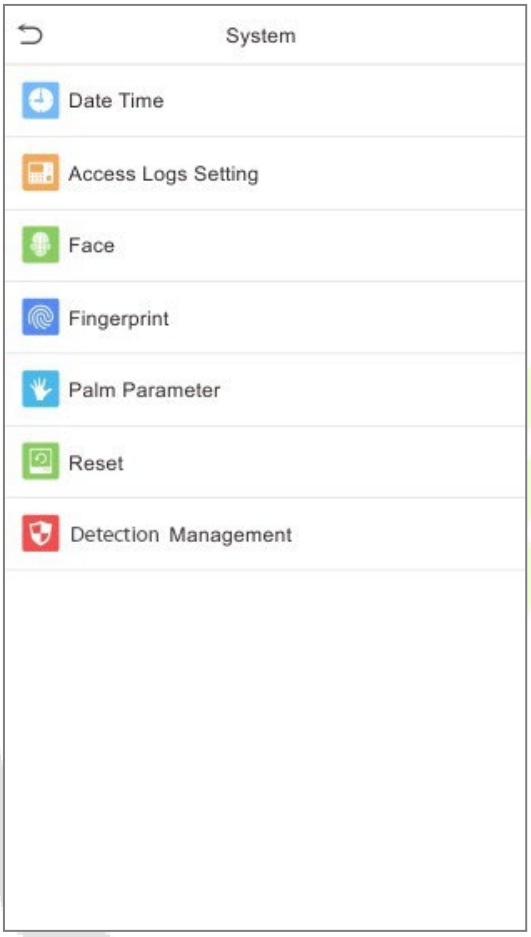


Nome da Função	Descrições
SRB★	Quando o SRB está habilitado, a fechadura é acionada pelo SRB para evitar que a fechadura seja aberta com à remoção do dispositivo da parede
Formato Wiegand	Os valores variam de 26 bits, 34 bits, 36 bits, 37 bits e 50 bits.
Bits de saída Wiegand	Após selecionar o formato 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.

7 Configurações do sistema

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

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



7.1 Data e hora

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

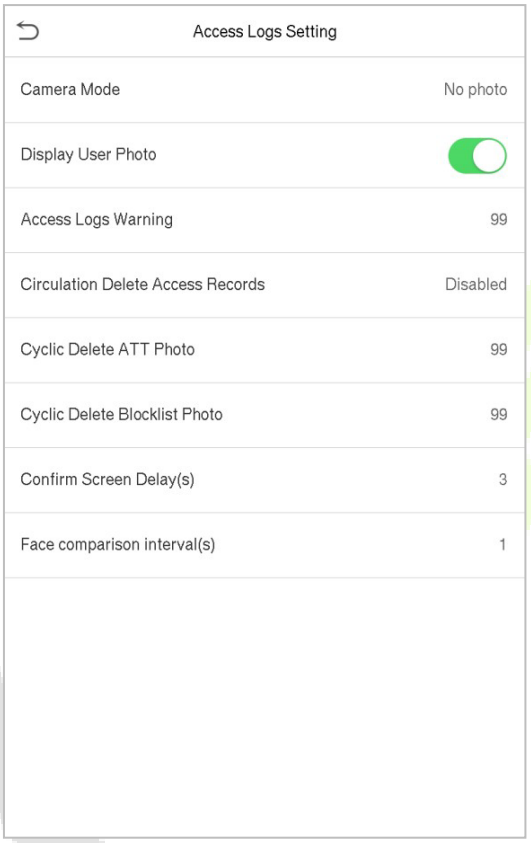
1. Você pode definir manualmente a data e a hora e clicar em **Confirmar** para salvar.
2. Clique em 24 horas para ativar ou desativar este formato e selecione o formato de data.

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

NOTA: Por exemplo, se o usuário configurar o horário do aparelho (18h35 do dia 15 de março de 2019) para as 18h30 do dia 1º de janeiro de 2020. Após restaurar as configurações de fábrica, o horário do equipamento permanecerá 18h30 em 1 de janeiro de 2020.

7.2 Configuração de Registros de Acesso

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

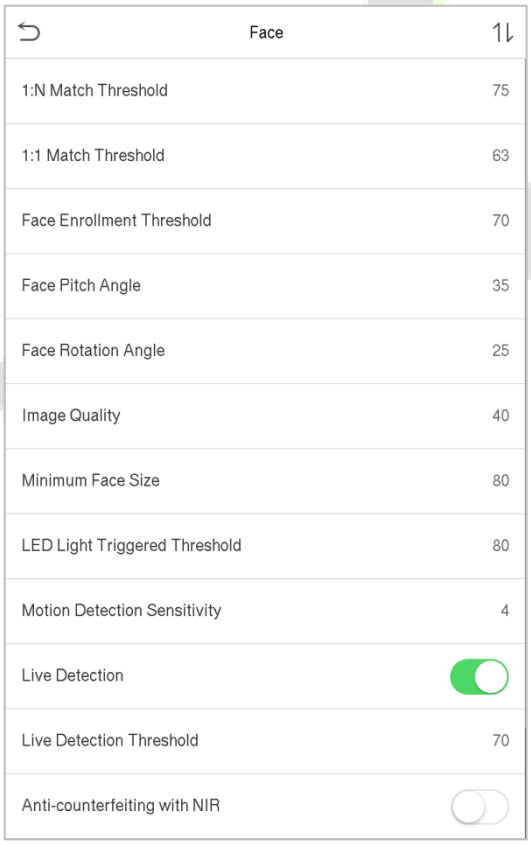


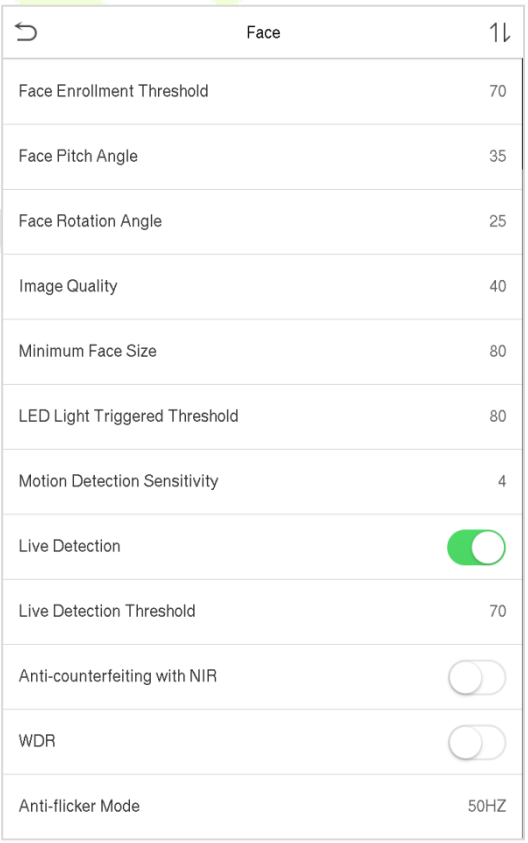
Nome da função	Descrição
Modo de câmera	Para capturar e salvar a imagem durante a autenticação. Existem 5 modos: **Sem Foto**: Nenhuma foto é tirada durante a autenticação do usuário. **Tirar foto, não salvar**: a foto é tirada, mas não salva durante a autenticação. **Tirar foto e salvar**: a foto é tirada e salva durante a autenticação. **Salvar na verificação bem-sucedida**: a foto é tirada e salva para cada autenticação bem-sucedida. **Salvar na verificação com falha**: a foto será tirada e salva apenas para a autenticação com falha.
Exibir foto do usuário	Se a foto do usuário deve ser exibida quando o usuário for autenticado com sucesso.

Aviso de logs de acesso	Quando o espaço de registro do acesso atingir o valor limite máximo, o dispositivo exibirá automaticamente o aviso de espaço de memória. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 9999.
Exclusão cíclica dos registros de acesso	Quando os registros de acesso atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de registros de acesso antigos. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 999.
Excluir Fotos de frequência	Quando as fotos de frequência atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de fotos de ponto antigas. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 99.
Excluir fotos da lista de proibições	Quando as fotos da lista de proibições atingirem a capacidade total, o dispositivo excluirá automaticamente um conjunto de fotos da lista negra antigas. Os usuários podem desabilitar a função ou definir um valor válido entre 1 e 99.
Atraso de tela (s)	A duração da mensagem de autenticação bem-sucedida é exibida. Valor válido: 1~9 segundos.
Intervalo de comparação de faces (s)	Para definir o intervalo de tempo de entre uma autenticação facial válida e outra. Valor válido: 0~9 segundos.

7.3 Parâmetros de face

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





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 cadastrados for maior que o valores definido. O valor válido varia de 65 a 120. Quanto maior o limite, menor a taxa de erro, maior a taxa de rejeição e vice-versa. Recomenda-se definir o valor padrão de 75.
Limiar 1:1	No modo de autenticação 1:1, a autenticação só será bem-sucedida quando a semelhança entre a imagem facial adquirida e os modelos faciais do usuário cadastrados no dispositivo for maior que o valor definido. O valor válido varia de 55 a 120. 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 for maior que esse limite, 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 cadastro facial e autenticação. Se o tamanho mínimo da foto capturada for menor que esse valor, ela será filtrada e não reconhecida como uma face. Este valor pode ser entendido como a distância de comparação de face. Quanto mais distante a pessoa estiver, menor será a face e menor será o pixel obtido pelo algoritmo. Portanto, ajustar este parâmetro pode ajustar a distância de comparação para mais distante ou mais perto. Quando o valor é 0, a distância de comparação de face não é limitada.
Sensibilidade para acionamento da luz de 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	É definido o valor para a 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 se a imagem visível capturada é realmente uma pessoa (um ser humano vivo). Quanto maior o valor, melhor o desempenho de antifalsificação usando luz visível.
Antifraude por infravermelho	Usado para ativar a montagem de imagens infravermelho na autenticação e evitar ataques de fotos e vídeos falsos.
WDR	Amplo Alcance Dinâmico (WDR), que equilibra a luz e amplia a visibilidade da imagem para vídeos de vigilância em cenas de iluminação de alto contraste e melhora a identificação de objetos em ambientes claros e escuros.
Modo Anti-flicker	Usado quando o WDR está desligado. Isso ajuda a reduzir o flicker quando a tela do dispositivo pisca na mesma frequência da luz.
Observação	O ajuste inadequado dos parâmetros de exposição e qualidade pode afetar gravemente o desempenho do dispositivo. Por favor, ajuste o parâmetro de exposição apenas sob a orientação da equipe técnica da ZKTeco.

7.4 Parâmetros de Palma

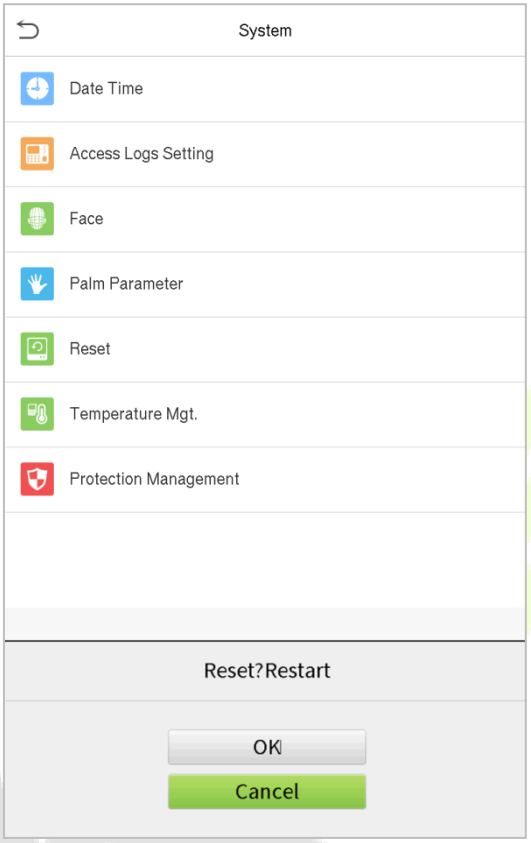
Clique Palma na interface do sistema.

Nome da função	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.

7.5 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** e depois toque em **OK** para restaurar as configurações padrão de fábrica.

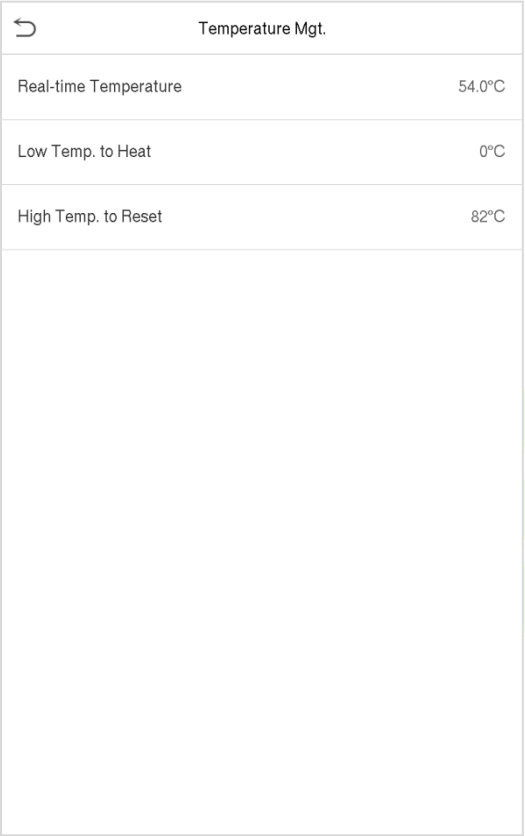


Clique em **OK** para restaurar.

7.6 Gerenciamento de Temperatura

O dispositivo possui um sensor de temperatura embutido quando a temperatura é muito baixa ou muito alta, ele acionará o autoaquecimento ou desligará.

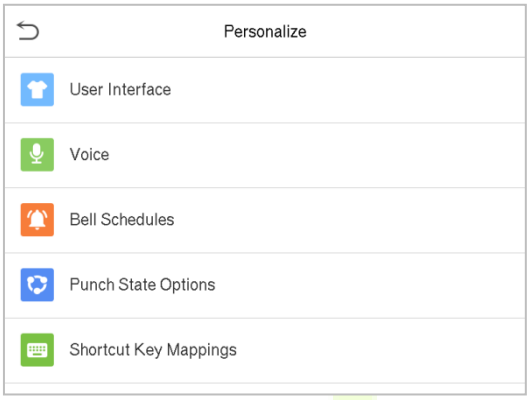
Clique em Gerenciamento de temperatura. na interface do sistema



Menu	Descrição
Temperatura em tempo real	Esta coluna mostra a temperatura interna do dispositivo em tempo real.
Baixa temperatura para aquecer	Quando a temperatura do dispositivo for inferior ao valor definido, o dispositivo iniciará o autoaquecimento, o intervalo definido é de 0 a 10 (°C).
Alta temperatura para redefinir	Quando a temperatura do dispositivo for superior ao valor definido, ele será desligado automaticamente para proteger o hardware, o intervalo definido é de 60 a 80 (°C).

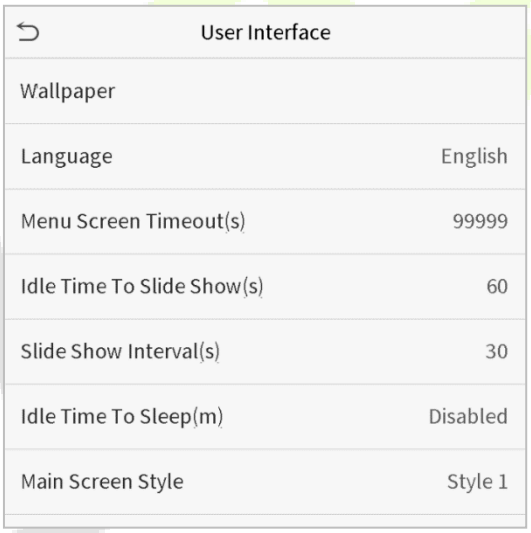
8 Configurações de Personalização

Toque em **Personalização** na interface do **Menu principal** para personalizar as configurações da interface, voz, campainha, opções de ponto e as teclas de atalho.



8.1 Configurações de Exibição

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



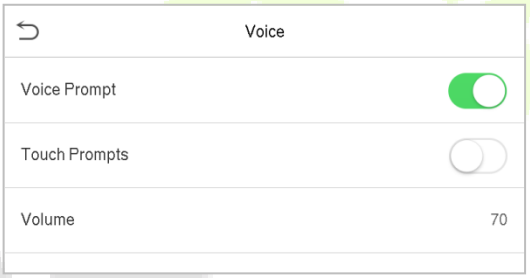
Descrição da Função

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

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

8.2 Configurações de voz

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



Descrição da função

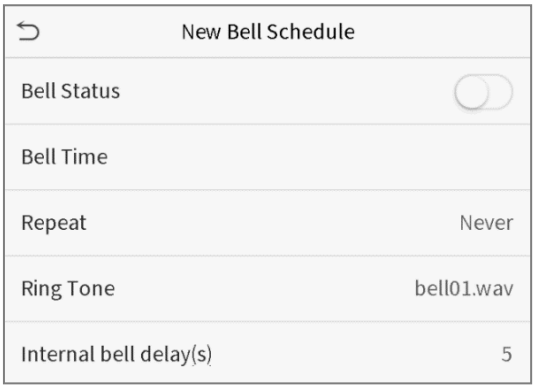
Nome da Função	Descrição
Voz	Alterne para ativar ou desativar os comandos de voz durante as operações de funções.
Confi. de toque	Alterne para ativar ou desativar os sons do teclado.
Volume	Ajuste o volume do dispositivo que pode ser definido entre 0-100.

8.3 Horários

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

Novo Horário

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



Descrição da função

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

Todos os horários de campainha

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

Edite a campainha agendada

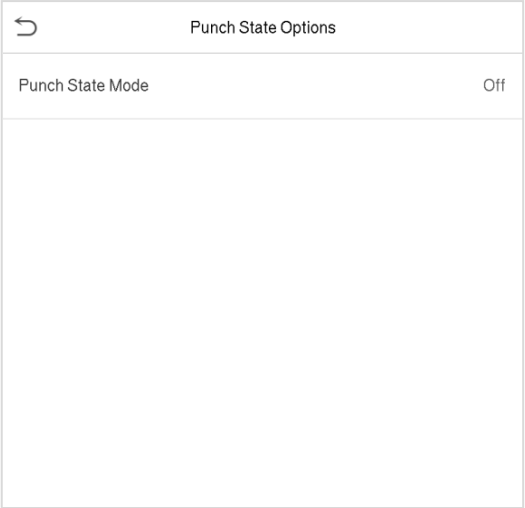
Na interface **Todos os Horários**, toque na programação de campainha e toque em **Editar** para editar a programação de campainha selecionada. O método de edição é o mesmo que as operações de adição de uma nova programação de campainha.

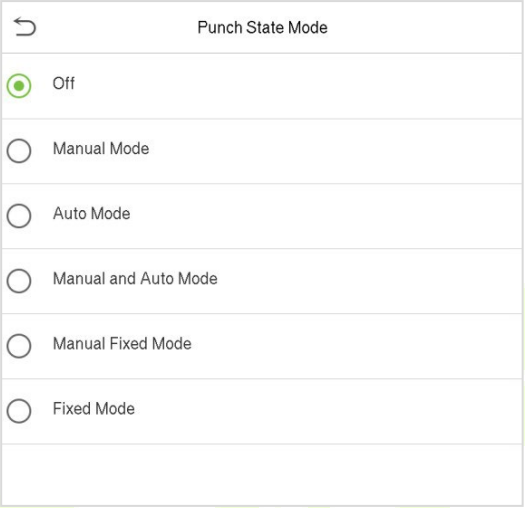
Deletar um horário

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

8.4 Configurações de status de registro de presença

Toque em **Configurações de status de ponto** na interface **Personalização** para definir as configurações de ponto.





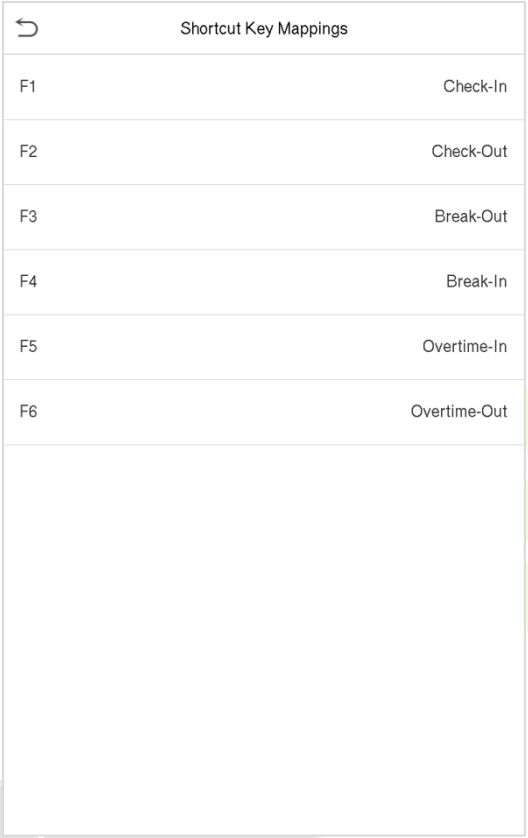
Descrição da função

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

8.5 Mapeamentos de teclas de atalhos

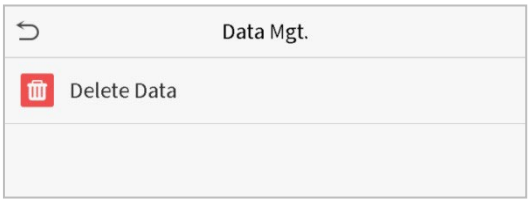
Os usuários podem definir teclas de atalho para status de ponto que serão exibidas na interface principal. Assim, na interface principal, quando as teclas de atalho são pressionadas, o status de ponto ou a interface de funções serão exibidas.

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



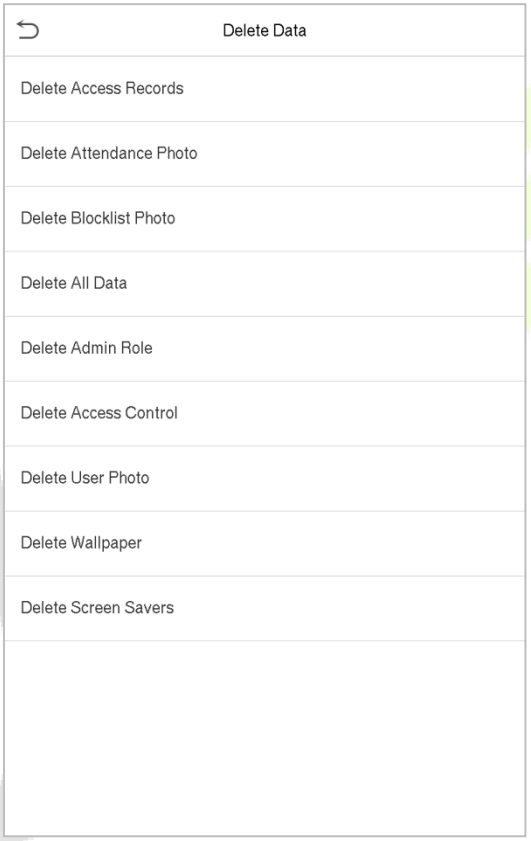
9 Gerenciamento de dados

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



9.1 Excluir dados

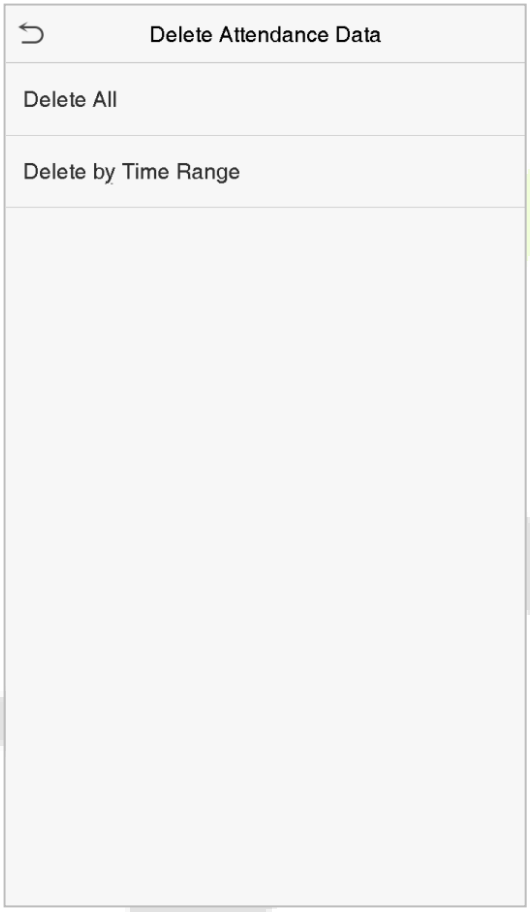
Toque em **Excluir Dados** na interface de **Gerenciamento de dados**



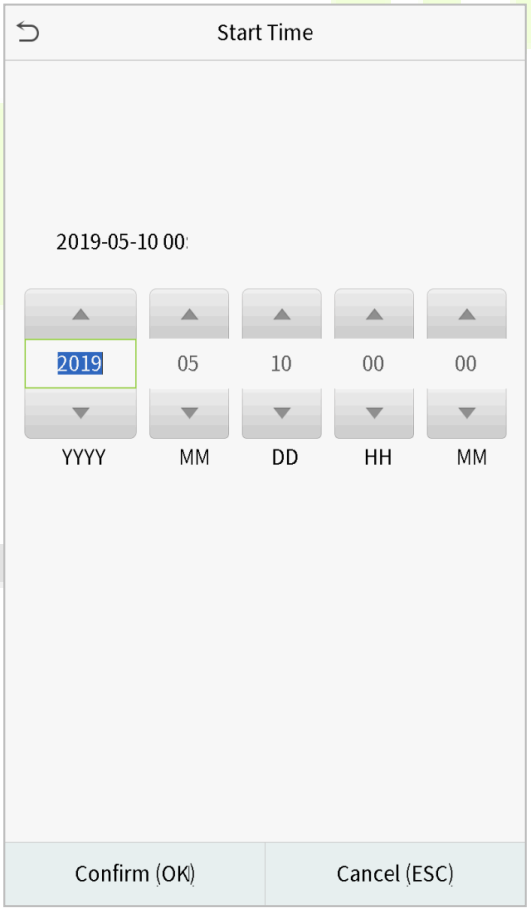
Menu	Descrição
Apagar reg. de acesso	Para apagar dados de frequência/registros de acesso.
Apagar foto de presença	Para apagar fotos de presença registradas.
Apagar foto lista bloqueio	Para apagar as fotos tiradas durante verificações com falha.
Apagar todos os dados	Para apagar informações e registros de presença/registros de acesso de todos os usuários registrados.

Apagar privilégios de administrador	Para remover todos os privilégios de administrador. (não apagar usuários)
Apagar dados de acesso	Para apagar todos os dados de acesso.
Apagar foto do usuário	Para apagar todas as fotos do usuário no dispositivo.
Apagar papel de parede	Para apagar todos os papéis de parede no dispositivo.
Apagar proteção de tela	Para apagar os protetores de tela no dispositivo.

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



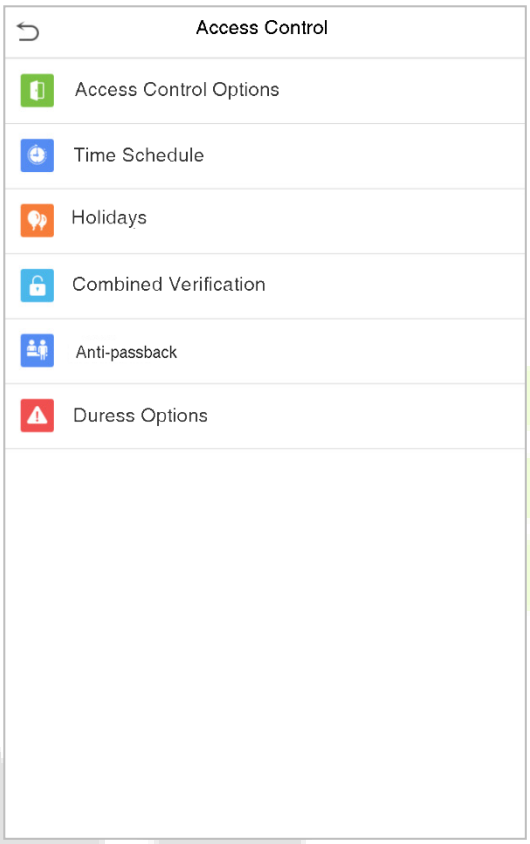
Selecione Apagar por intervalo de tempo



Defina o intervalo de tempo e clique em **OK**

10 Controle de acesso

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



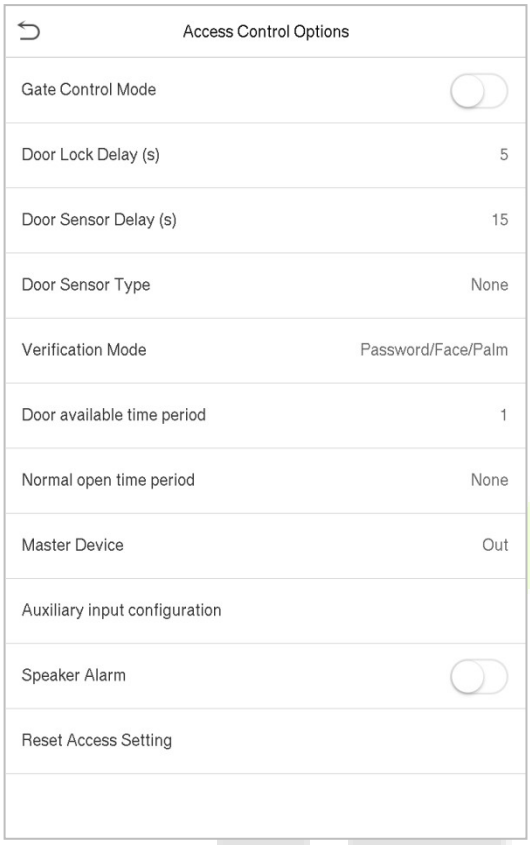
Para ter uma autenticação válida, o usuário cadastrado deve atender às seguintes condições:

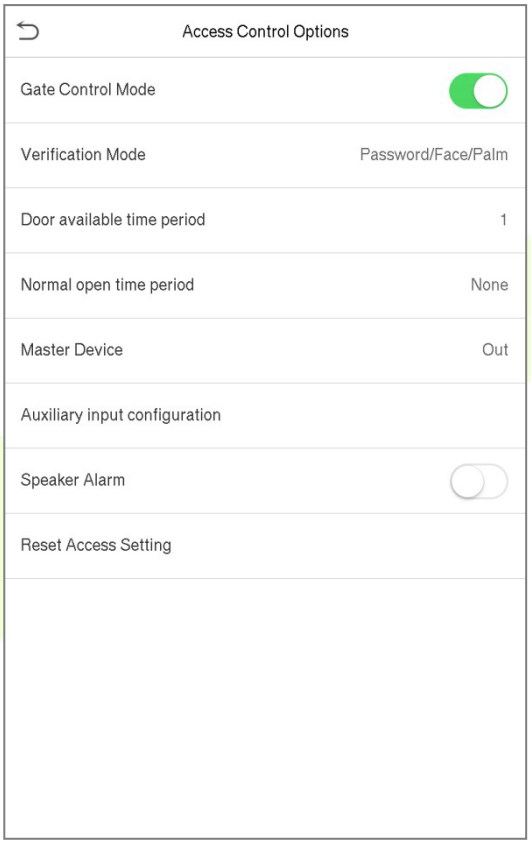
- O tempo atual de desbloqueio da porta deve estar dentro de qualquer fuso horário válido do período de tempo do usuário.
- O grupo do usuário já deve estar definido na combinação de desbloqueio da porta (e se houver outros grupos, sendo configurados na mesma regra de acesso, também é necessária a verificação dos membros desse grupo para destravar a porta).

Na configuração padrão, os novos usuários são alocados no primeiro grupo com o fuso horário do grupo padrão, onde a regra de acesso é "1" e é definida no estado de desbloqueio por padrão.

10.1 Opções de controle de acesso

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





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	No modo de verificação você pode selecionar as diversas opções para autenticação de face, palma, cartão e senha. Sendo combinada ou não
Tempo de acionamento da porta	Para definir o período de tempo para a porta, para que a porta esteja disponível apenas durante esse período.
Período de tempo normalmente aberto	Período de tempo programado para o modo "Normal Aberto", para que a porta fique sempre aberta durante este período.
Equipamento mestre	Ao configurar o equipamento mestre, o status pode ser definido para sair ou entrar. **Saída**: O registro verificado no software é o registro de saída. **Entrada**: O registro verificado no software é o registro de entrada.
Dispositivo auxiliar	Ao configurar o equipamento auxiliar, o status pode ser definido para sair ou entrar. **Saída**: O registro verificado no software é o registro de saída. **Entrada**: O registro verificado no software é o registro de entrada.
Configuração de entrada auxiliar	Define o período de tempo de destravamento da porta e o tipo de saída auxiliar do dispositivo terminal auxiliar. Os tipos de saída auxiliar incluem "Nenhum", "Acionamento da porta", "Acionamento de alarme" e "Acionamento de porta e alarme".
Verificar por RS485	Quando existe a necessidade de adicionar um leitor auxiliar RS485, você pode configurar para o modo de verificação de impressão digital, cartão ou 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 configuração de acesso	O reset dos parâmetros de controle de acesso inclui 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.

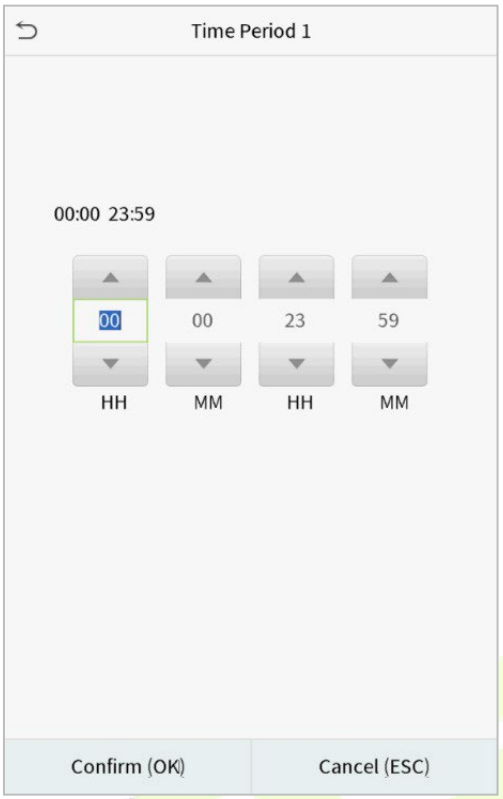
10.2 Configuração de regra de tempo

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

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

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

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



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

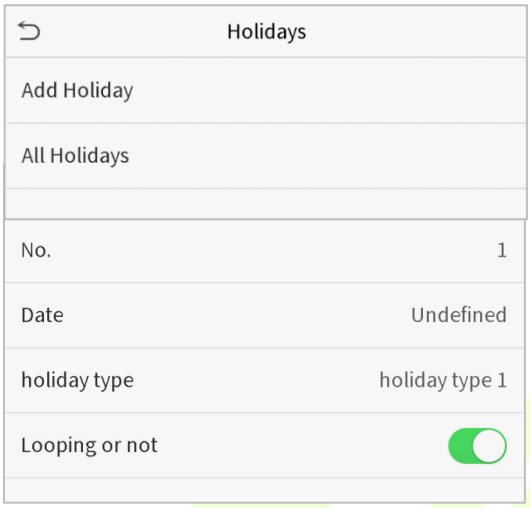
NOTA:

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.

10.3 Feriados

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

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



- **Adicionar um novo feriado**

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

- **Editar um feriado**

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

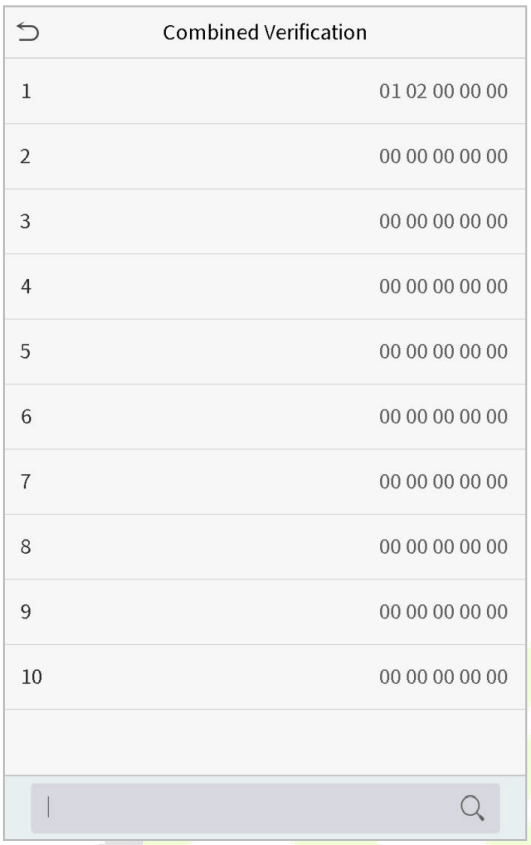
- **Excluir um feriado**

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

10.4 Acesso combinado

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

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



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

Por exemplo:

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

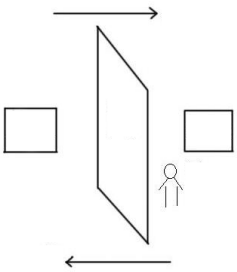
Excluir uma combinação de destravamento de porta

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

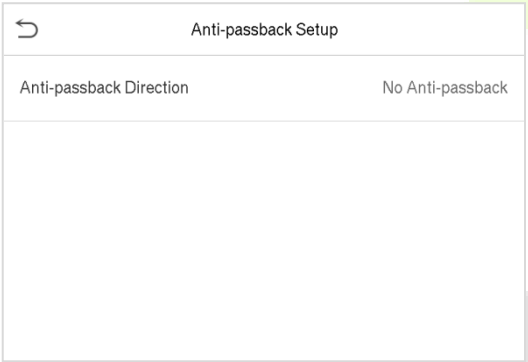
10.5 Anti-Passback

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

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



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

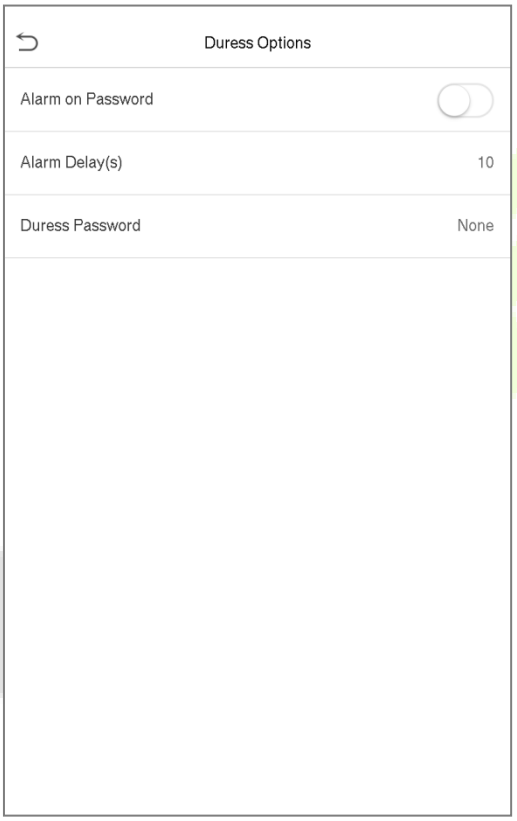


Menu	Descrição
Direção anti-passback	**Sem Anti-passback:** A função anti-passback está desativada, o que significa que a verificação bem-sucedida através do dispositivo mestre ou do dispositivo escravo pode desbloquear a porta. O status de entrada ou saída não é salvo nesta opção para o próximo desbloqueio.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

10.6 Opções de Coação

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

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

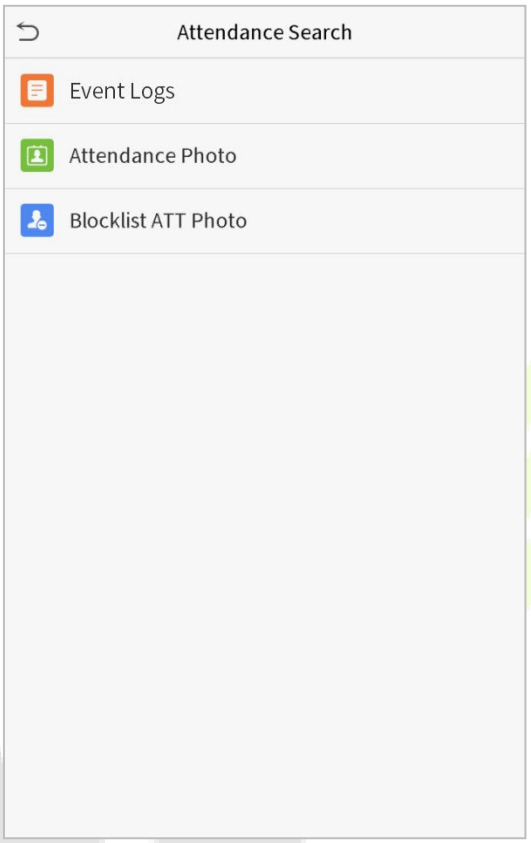


Nome da função	Descrição
Senha de alarme	Quando um usuário usa o método de verificação de senha, um sinal de alarme será gerado somente quando a verificação de senha for bem-sucedida, caso contrário não haverá sinal de alarme.
Atraso do Alarme (s)	O sinal de alarme não será transmitido até que o tempo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

11 Procurar registros

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

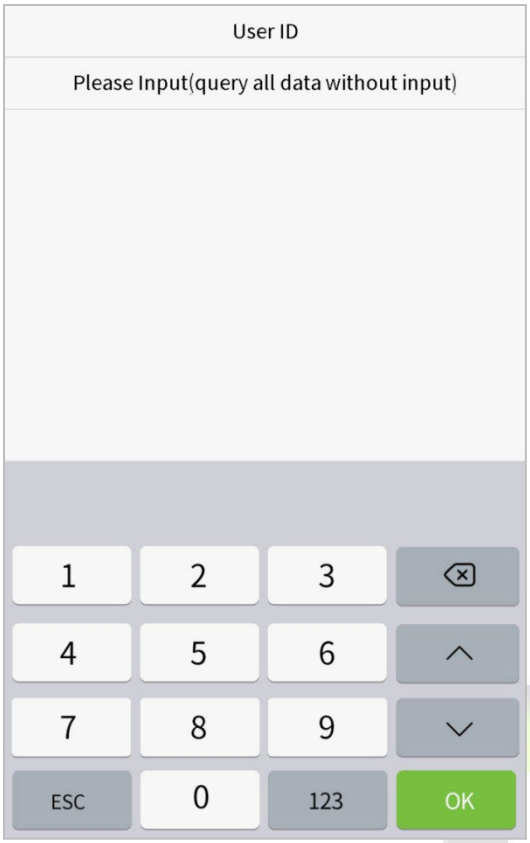
Clique em **Procurar registros** na interface do **Menu Principal** para pesquisar o registro de Acesso/Presença necessário.



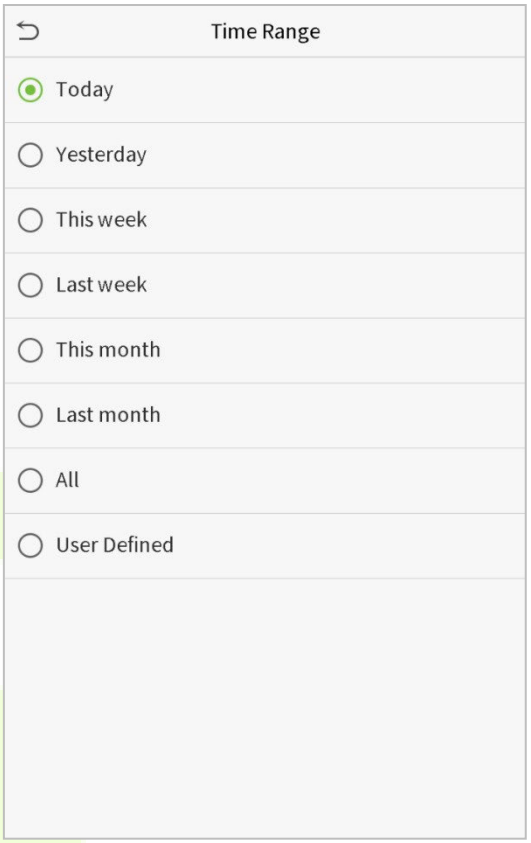
O processo de pesquisa de fotos de presença e lista de bloqueio é semelhante ao da pesquisa de logs de eventos. Veja a seguir um exemplo de pesquisa de logs de eventos.

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

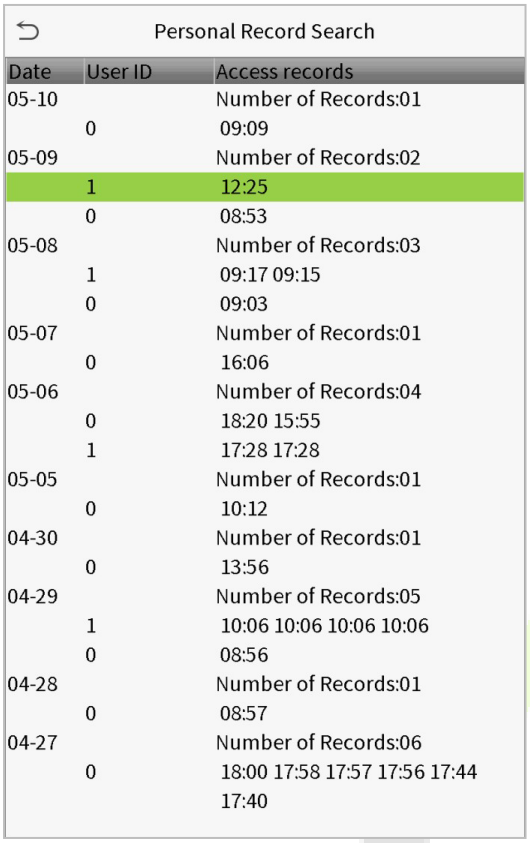
1. Insira o ID do usuário a ser pesquisado e clique em OK. Se desejar pesquisar logs de todos os usuários, clique em OK sem inserir nenhum ID de usuário.



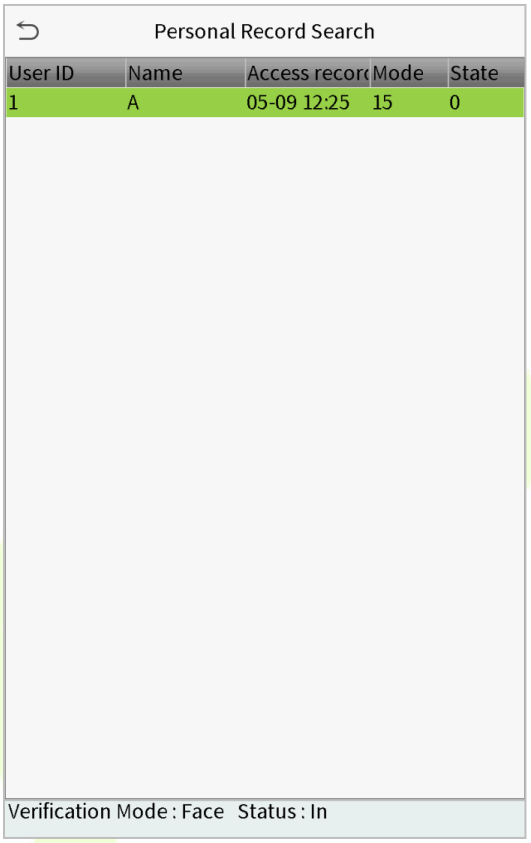
2. Selecione o intervalo de tempo em que os logs precisam ser pesquisados.



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



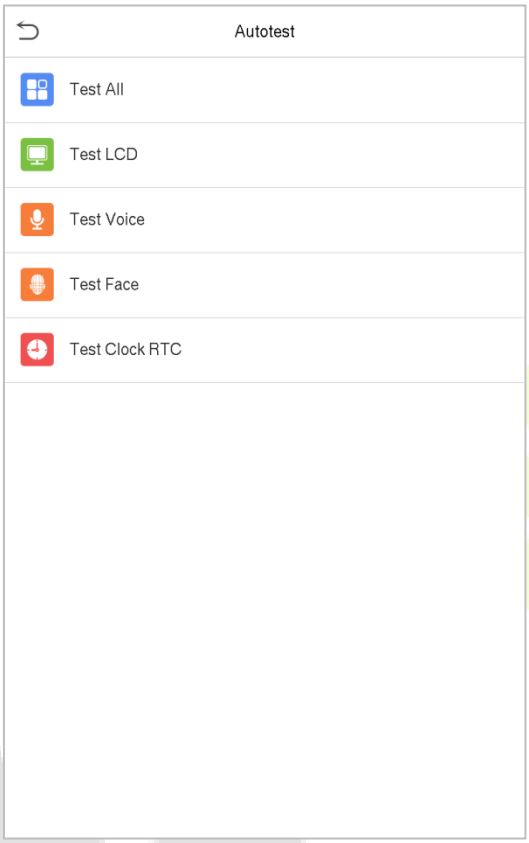
4. A figura abaixo mostra os detalhes do log selecionado.



12 Auto teste

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

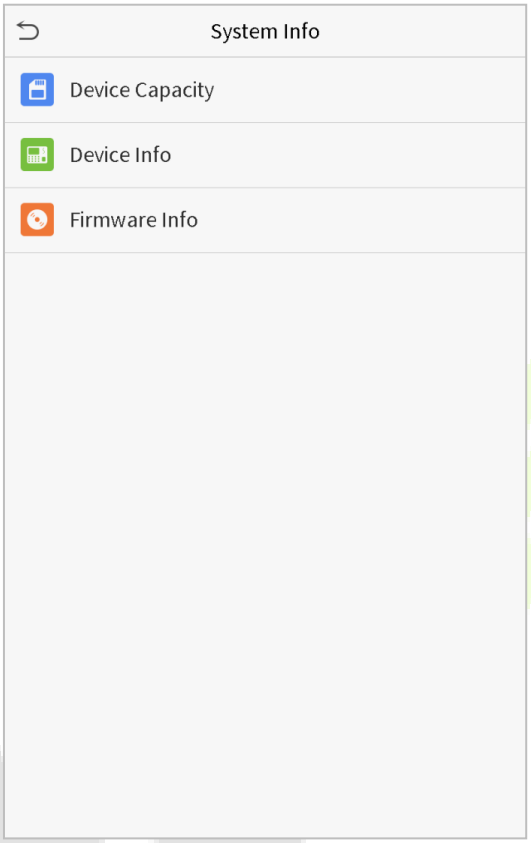
.



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 de câmera	Para testar se a câmera funciona corretamente, verificando as fotos tiradas estão claras o suficiente.
Teste relógio	Para testar o RTC. O dispositivo testa se o relógio funciona normalmente e com precisão com um cronômetro. Toque na tela para começar a contar e pressione-o novamente para parar de contar.

13 Informação do sistema

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



Nome da função	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.

14 Conecte-se ao software ZKBioAccess IVS

14.1 Defina o endereço de comunicação

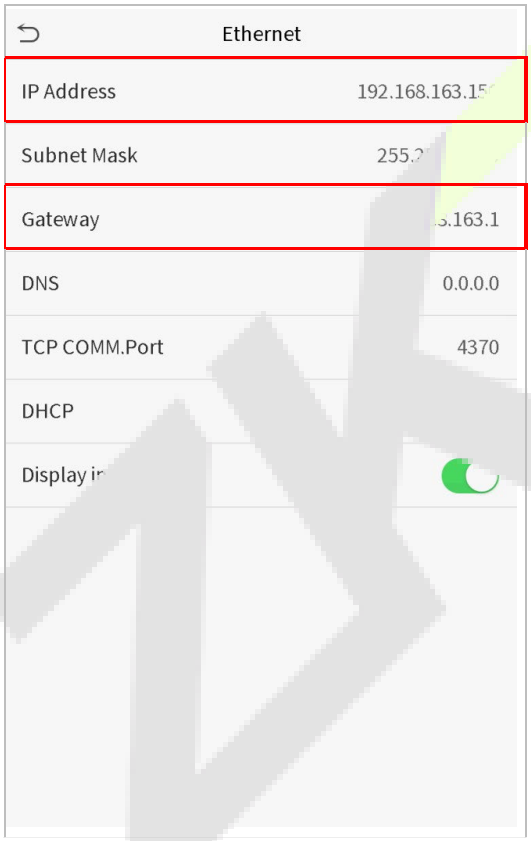
Lado do dispositivo

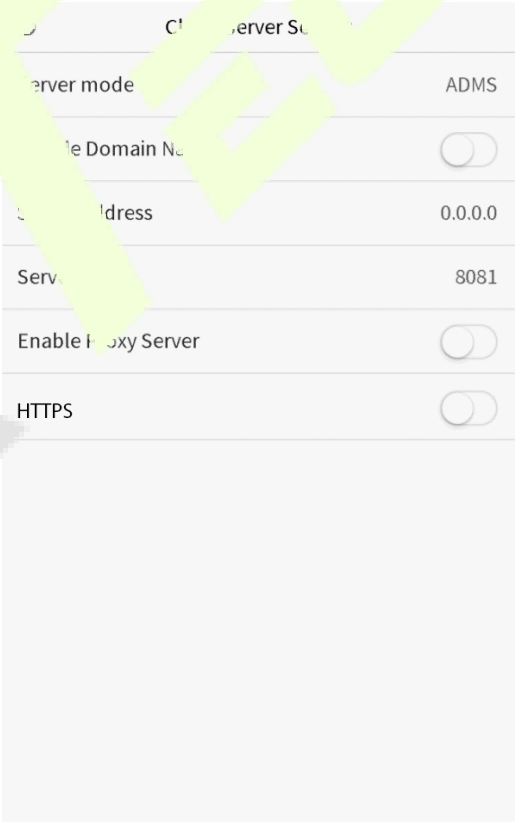
1. Toque em **Conf. com > TCP/IP** no menu principal para definir as configurações de rede.

(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. Com >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:

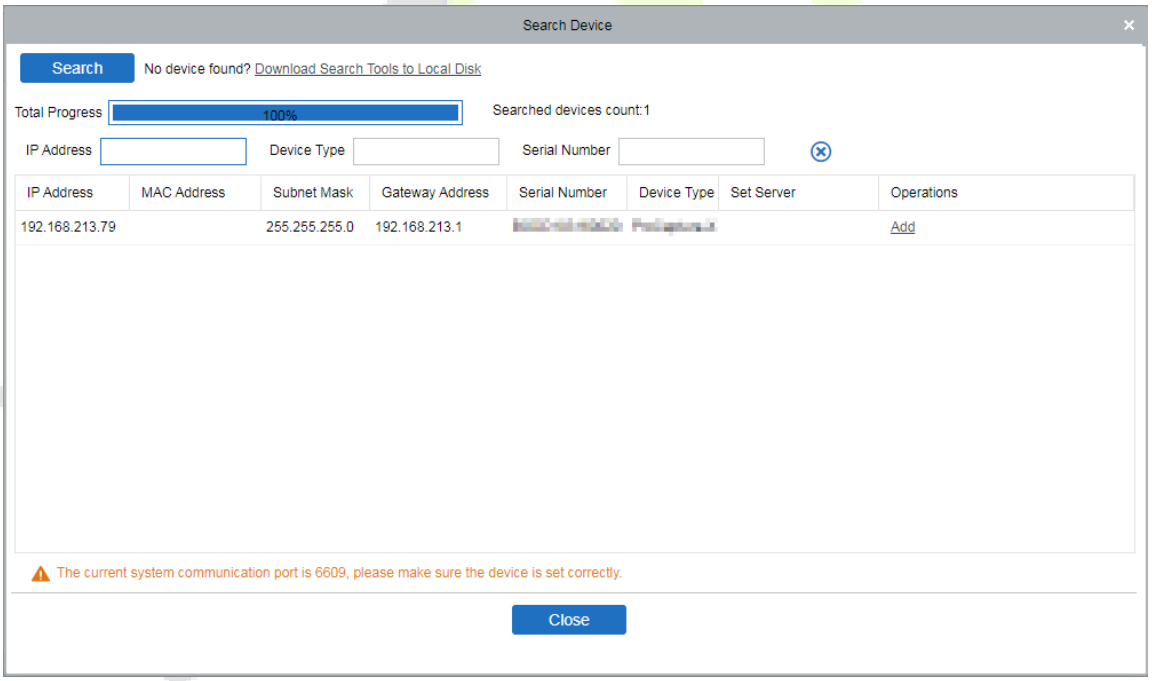
14.2 Adicionar dispositivo no software

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**……].

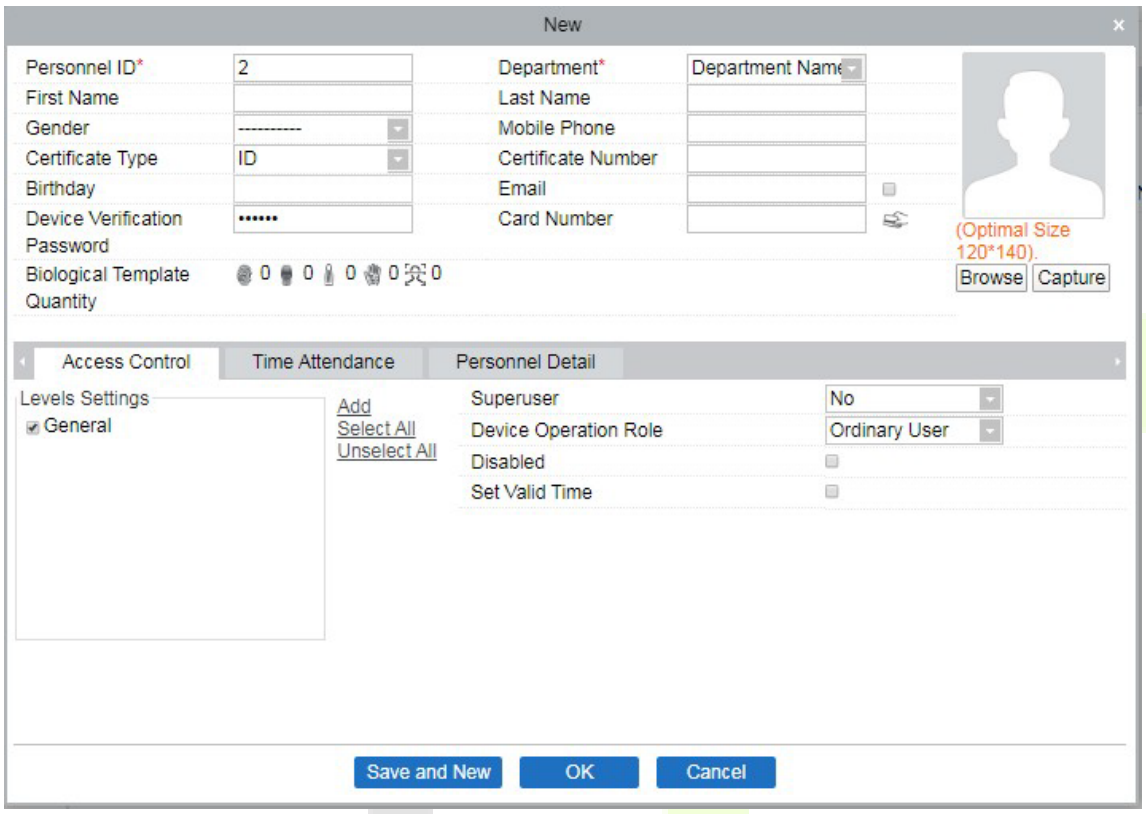
3) Após a pesquisa, a lista e o número total de equipamentos serão exibidas.



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.

14.3 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.

Apêndice 1

Requisitos para cadastro no equipamento 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 de pele e a cor de fundo.

4) Exponha face e a testa adequadamente e não cubra a face e as sobrancelhas com o cabelo.

5) Recomenda-se mostrar uma expressão facial simples. (Um sorriso simples é aceitável, mas não feche os olhos ou incline a cabeça para qualquer orientação).

6) Duas imagens são necessárias para uma pessoa com óculos, uma imagem com óculos e outra sem os óculos.

7) Não use acessórios como cachecol ou máscara que possam cobrir a boca ou o queixo durante o cadastro.

8) Posicione a face na área de captura, conforme mostrado na imagem abaixo.

9) Não inclua mais de um face na área de captura.

10) Recomenda-se uma distância de 50 cm a 80 cm para capturar a imagem. (a distância é ajustável, dependendo da altura do corpo).

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.

13.6.1 Distância dos olhos

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

13.6.2 Expressão Facial

Rosto neutro ou sorriso simples e olhos naturalmente abertos são recomendados.

13.6.3 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°.

13.6.4 Acessórios

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

13.6.5 Face

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

13.6.6 Formato de imagem

Deve estar em BMP, JPG ou JPEG.

13.6.7 Requisito de dados

Deve seguir os requisitos:

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

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 tóxica					
	Chumbo (Pb)	Mercury (Hg)	Cádmio (Cd)	Crómio hexavalente (Cr6+)	Bifenilos Polibromados (PBB)	Éteres Difenil Polibromados (PBDE)
Resistores	×	○	○	○	○	○
Capacitores	×	○	○	○	○	○
Indutores	×	○	○	○	○	○
Diodo	×	○	○	○	○	○
Componentes ESD	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adaptador	×	○	○	○	○	○
Parafusos	○	○	○	×	○	○

○ indica que a quantidade total de conteúdo tóxico em todos os materiais homogêneos está abaixo do limite, conforme especificado no SJ/T 11363—2006.
× indica que a quantidade total de conteúdo tóxico em todos os materiais homogêneos excede o limite, conforme especificado no SJ/T 11363—2006.

NOTA: 80% dos componentes deste produto são fabricados utilizando materiais que não são tóxicos e ecologicamente corretos. Os componentes que contêm toxinas ou elementos nocivos são incluídos devido às atuais limitações econômicas ou técnicas que impedem sua substituição por materiais não tóxicos.

Garantia

Este produto é garantido pela ZKTeco por um período de 3 meses (garantia legal), acrescidos de 9 meses de garantia adicional (garantia contratual), em um total de 1 ano, contra eventuais defeitos de material ou fabricação, desde que observadas as seguintes condições:

a) A garantia se aplica exclusivamente a produtos fornecidos pela ZKTeco do Brasil ou por Revenda Autorizada ZKTeco no Brasil.
b) O período de garantia será contado a partir da data de emissão da nota fiscal do produto.
c) Durante a garantia legal estão cobertos os custos de peças e serviços de reparo, que deverão ser realizados obrigatoriamente em Assistência Técnica ZKTeco ou na própria fábrica, conforme orientação da ZKTeco. Para o período de garantia contratual estão cobertos apenas os custos de peças que eventualmente necessitem substituição para reparo do produto, ficando excluídos os custos em relação aos serviços de manutenção (mão de obra), a remoção do produto (envio e retorno) e a visita/estadia de técnico especializado, se aplicável.
d) Detectado o defeito no produto, o usuário deverá entrar em contato com a ZKTeco nos canais de comunicação disponíveis em https://www.zkteco.com.br/suporte/, fornecendo informações sobre os produtos e problemas observados por meio do preenchimento e envio do formulário de Remessa de Material para Assistência Técnica (RMA) disponível em https://www.zkteco.com.br/manutencao/.
e) Recebidas as informações e o RMA, a ZKTeco analisará o caso e informará ao usuário sobre os próximos passos, bem como sobre a documentação que deve ser encaminhada em caso de envio do produto para a ZKTeco ou Assistência Técnica ZKTeco e/ou sobre opções para agendamento de visita técnica, quando aplicável.
f) Produtos enviados para a ZKTeco ou para Assistência Técnica ZKTeco sem notificação prévia e expressa autorização da ZKTeco não serão recebidos.
g) O produto e as peças substituídas serão garantidas pelo restante do prazo original, sendo que as peças retiradas dos produtos e/ou produtos eventualmente descartados serão de propriedade da ZKTeco.
h) Em caso de dúvidas o usuário deverá entrar em contato com a ZKTeco nos canais de comunicação disponíveis em https://www.zkteco.com.br/suporte/

Resultará nula e sem efeito esta garantia em caso de:

a) Produto que apresente lacres rompidos e/ou etiqueta de identificação violada.
b) Uso anormal do produto, inclusive em desconformidade com seu manual, especificações, desenhos, folhas de instruções ou quaisquer outros documentos relacionados, bem como em capacidade além de seus limites e taxas prescritas.
c) Uso indevido ou erro de instalação, operação, testes, armazenamento e/ou manuseio do produto.
d) Manutenção e/ou alteração no produto não aprovada previamente pela ZKTeco.
e) Defeitos e danos causados por agentes naturais (enchente, maresia e outros) ou exposição excessiva ao calor.
f) Defeitos e danos causados pelo uso de software e/ou hardware não compatíveis com especificações do produto.
g) Surtos e/ou picos de tensão na rede elétrica típicos de algumas regiões, para as quais deve-se utilizar dispositivos de proteção contra surtos elétricos.
h) Fatos ou eventos imprevisíveis ou de difícil previsão e de força maior.
i) Transporte do produto em embalagem ou de forma inadequada.
j) Furto ou roubo.
k) Desgaste natural do produto.
l) Danos exclusivamente causados pelo usuário ou por terceiros.

Em nenhum caso a ZKTeco será responsável por indenização superior ao preço da compra do produto, por qualquer perda de uso, perda de tempo, inconveniência, prejuízo comercial, perda de lucros ou economias ou outros danos diretos ou indiretos, decorrentes do uso ou impossibilidade de uso do produto.

A ZKTeco reserva-se o direito de alterar as condições e procedimentos aqui estabelecidos independente de aviso prévio, sendo de responsabilidade do usuário verificar periodicamente eventuais atualizações, que estarão disponíveis em https://www.zkteco.com.br/manutencao/. Nenhuma Revenda Credenciada ou Assistência Técnica ZKTeco

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

www.zkteco.com.br