Manual do Usuário

Elite Series

Modelos: Elite Pass, Elite Access

Versão: 1.1

Data: Outubro de 2023

Marca registrada

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

Responsabilidade

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

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

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

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

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

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

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

ZKTeco Filial Brasil

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

Telefone (31) 3055-3530

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

Sobre a Empresa

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

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

Sobre o Manual

Este manual apresenta as operações sobre a **Elite Series**.

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

Convenções do Documento

As convenções utilizadas neste manual estão listadas abaixo:

Convenções de Interface Gráfica do Usuário:

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

Símbolos

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

Índice

1 Instruções de Uso 7
1.1 Posição em Pé, Expressão Facial e Postura em Pé 7
1.2 Cadastro de face 8
1.3 Interface de Espera 9
1.4 Teclado Virtual 10
1.5 Modo de Autenticação 11
1.5.1 Autenticação por Senha 11
1.5.2 Verificação Facial 14
1.5.3 Verificação Combinada 17
2 Menu Principal 18
3 Gerenciamento de Usuários 19
3.1 Adicionar Usuários 19
3.2 Buscar Usuários 23
3.3 Editar Usuários 24
3.4 Excluir Usuários 24
4 Privilégio do Usuário 25
5 Configurações de Comunicação 27
5.1 Configurações de Rede 27
5.2 Conexão com o PC 29
5.3 Configuração do Servidor em Nuvem 30
5.4 Configuração de Wiegand 31
6 Configurações de Sistema 35
6.1 Data e Hora 35
6.2 Configuração de Registros de Acesso 36
6.3 Parâmetros de Face 38

6.4 Redefinição de Fábrica 40

6.5 Gerenciamento de Temperatura 41

7. Configurações de Personalização 42

7.1 Configurações da Exibição 42

7.2 Configurações de voz 43

7.3 Horários 44

8. Gerenciamento de Dados 45

8.1 Excluir dados 46

9. Controle de acesso 48

9.1 Opções de Controle de Acesso 49

9.2 Regras de Tempo 51

9.3 Configurações de Feriado 53

9.4 Configurações de Verificação Combinada 54

9.5 Configuração Anti-passback 55

9.6 Opções de Coação 56

10. Procurar registros 57

11. Auto teste 60

12. Informações do Sistema 61

13. Conexão com o Software ZKBioSecurity 62

13.1 Configurar o Endereço de Comunicação 62

13.2 Adicionar um Dispositivo no Software 63

13.3 Adicionar Pessoal no Software 63

Declaração sobre o Direito à Privacidade 65

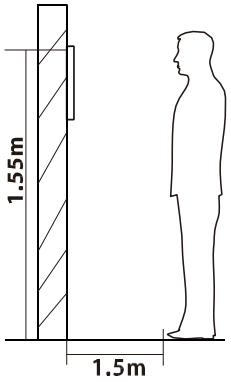
Operação Ecologicamente Correta 66

Garantia 67

1 Instruções de Uso

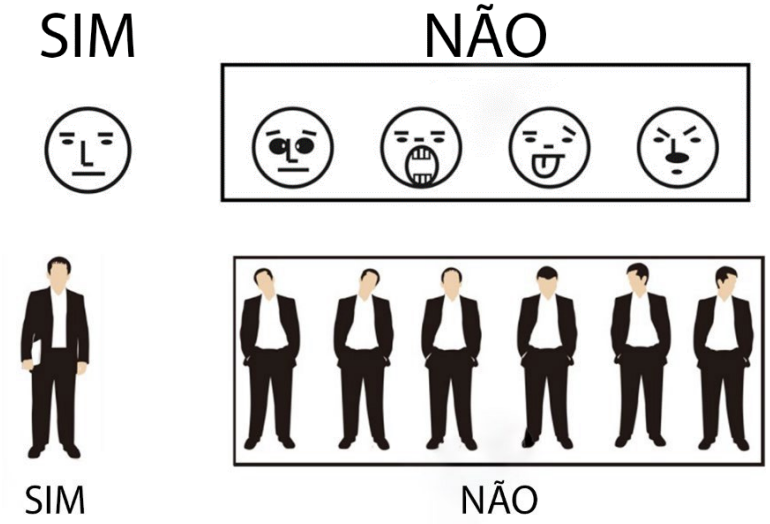
1.1 Posição em Pé, Expressão Facial e Postura em Pé

- **A distância recomendada**



A distância entre o dispositivo e um usuário com altura entre 1,55m e 1,85m é recomendada para ser de 1,5m. Os usuários podem se mover ligeiramente para frente e para trás para melhorar a qualidade das imagens faciais capturadas.

- **Expressão facial e postura em pé**



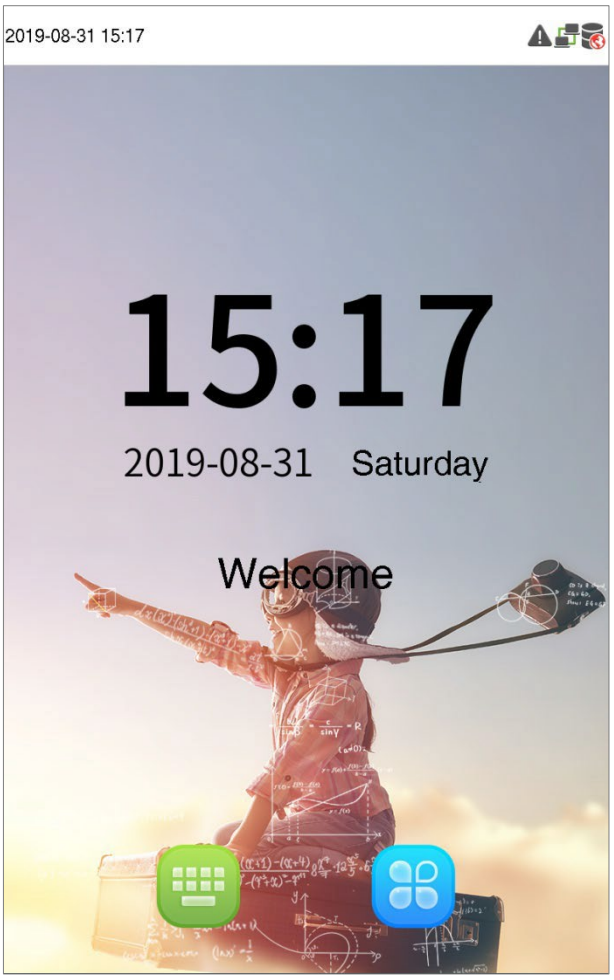
Observação: Durante o cadastro e a autenticação, por favor, mantenha uma expressão facial natural e uma postura em pé.

1.2 Cadastro de face

Tente manter o rosto no centro da tela durante o registro. Por favor, olhe diretamente para a câmera e mantenha-se parado durante o registro facial, conforme mostrado abaixo.

1.3 Interface de Espera

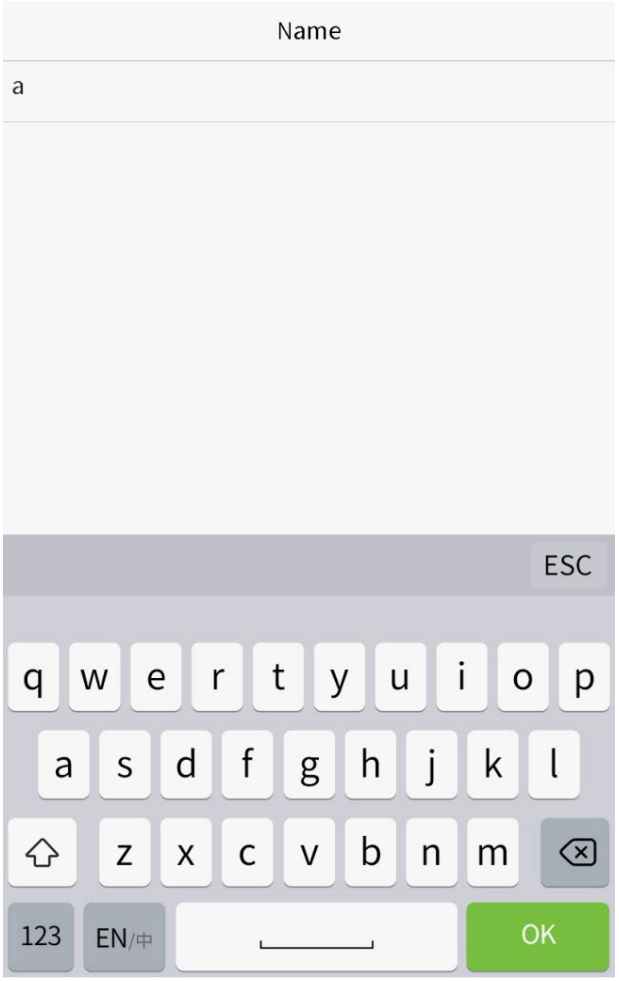
Após conectar à fonte de alimentação, você terá acesso à seguinte interface de espera:



1. Clique para acessar a interface de entrada do ID do usuário.

2. Quando não houver um super administrador definido no dispositivo, clique para acessar o menu e configurar um. Após configurar a conta de super administrador, o usuário deve autenticar sua identidade de super administrador antes de acessar o menu. Por motivos de segurança, é recomendado registrar uma conta de super administrador pela primeira vez usando o dispositivo.

1.4 Teclado Virtual



Observação: O dispositivo suporta entrada de chinês, inglês, números e símbolos. Clique em [EN] para alternar para o teclado em inglês. Pressione [123] para alternar para o teclado numérico e de símbolos e clique em [ABC] para voltar ao teclado alfabético. Clique na caixa de entrada e o teclado virtual aparecerá. Clique em [ESC] para sair.

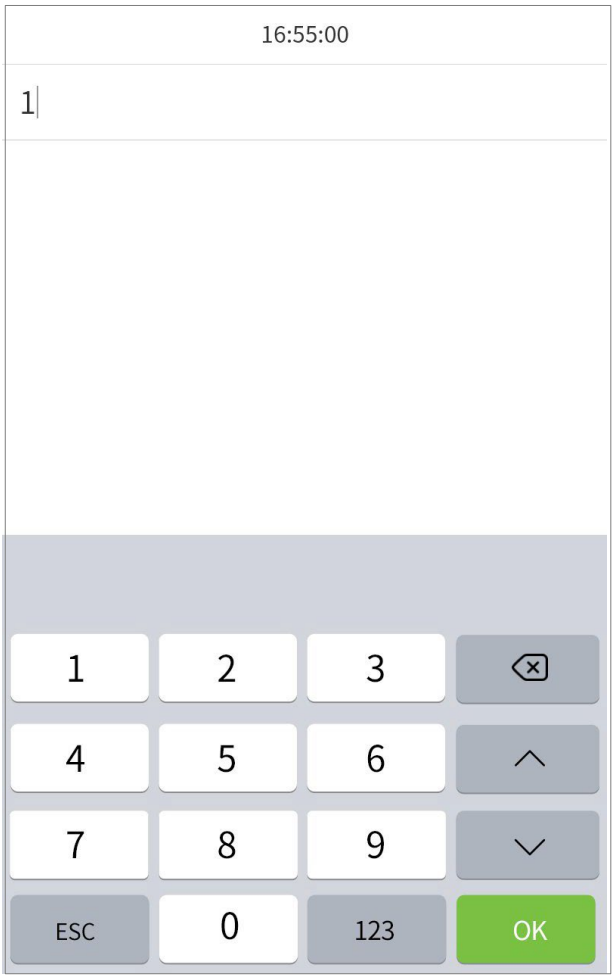
1.5 Modo de Autenticação

1.5.1 Autenticação por Senha

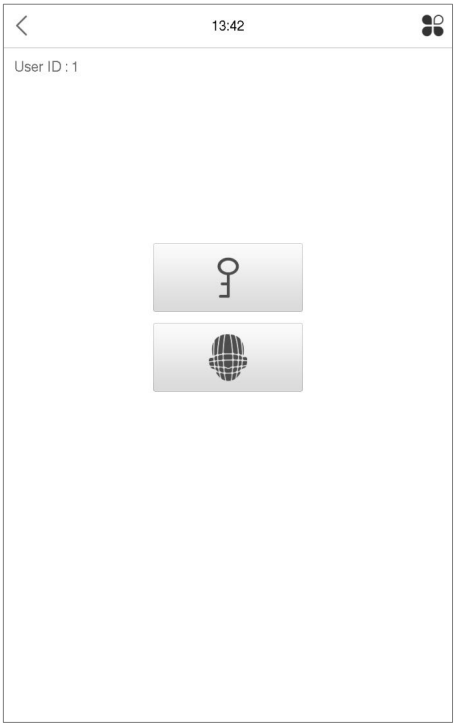
Compara a senha inserida com o ID de usuário e a senha registrados.

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

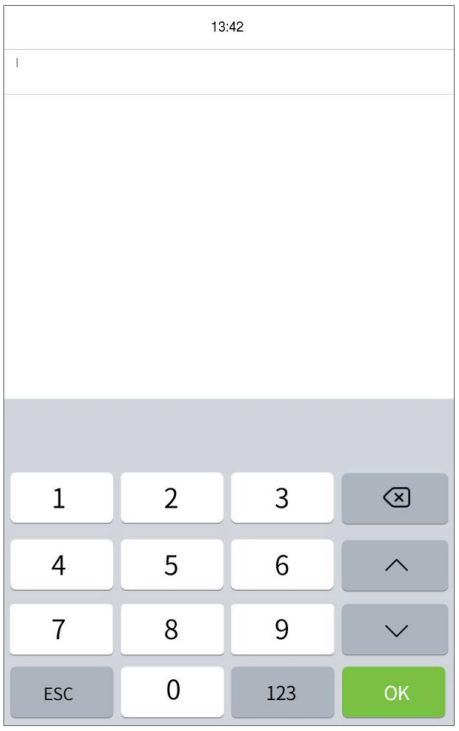
1. Insira o ID do usuário e pressione [**OK**].



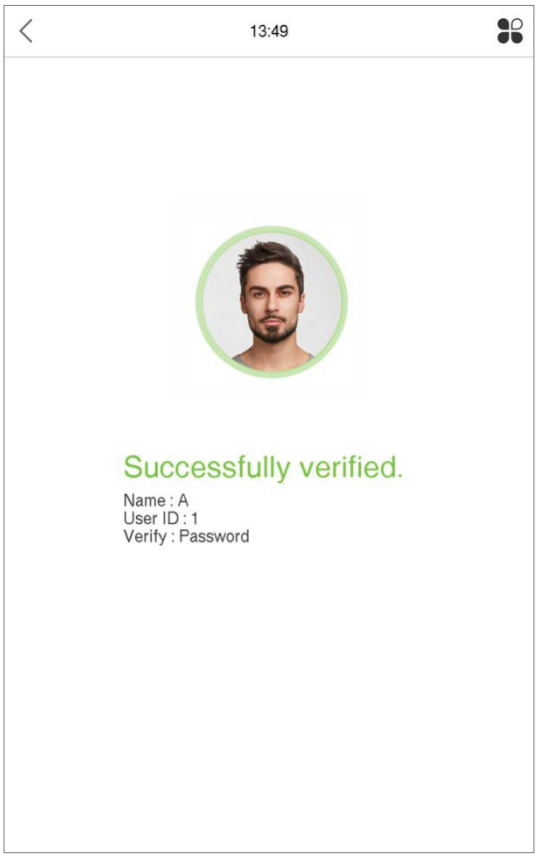
Se o usuário tiver cadastrado um modelo facial e definido uma senha para verificação, a seguinte tela aparecerá. Selecione o ícone para entrar no modo de verificação por senha.



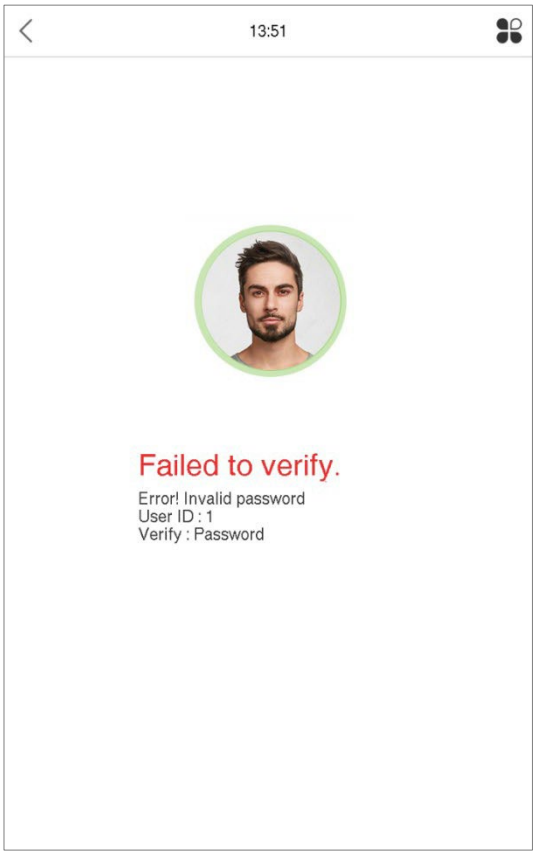
2. Insira a senha e pressione [**OK**].



A autenticação foi bem-sucedida.



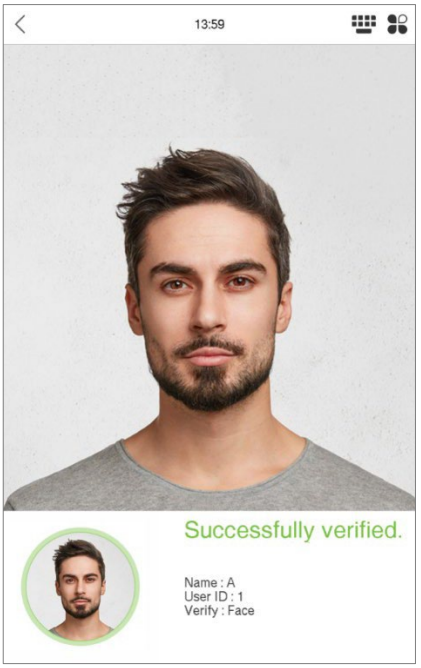
A autenticação falhou.



1.5.2 Verificação Facial

- **Verificação Facial 1:N**

Compara as imagens faciais adquiridas com todos os dados faciais registrados no dispositivo. A seguir está a mensagem pop-up sobre o resultado da comparação.

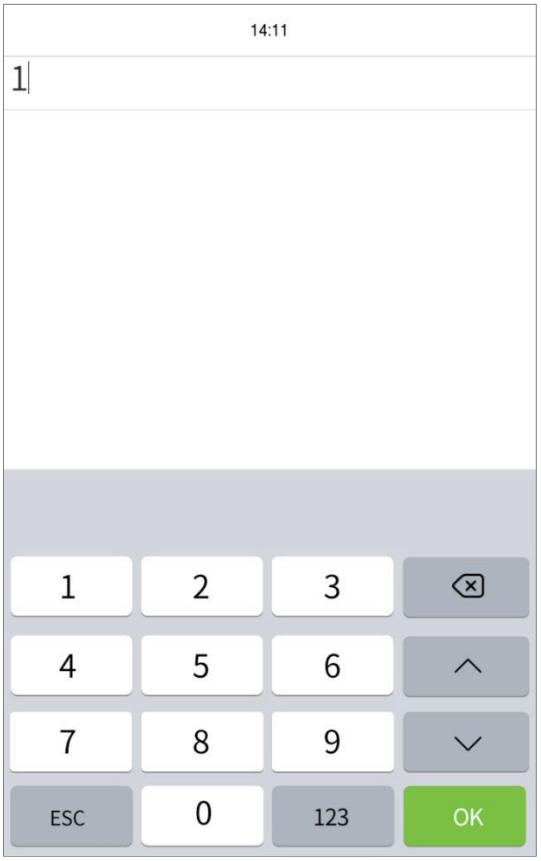


- **Verificação Facial 1:1**

Comparar o rosto capturado pela câmera com o modelo facial relacionado ao ID do usuário inserido.

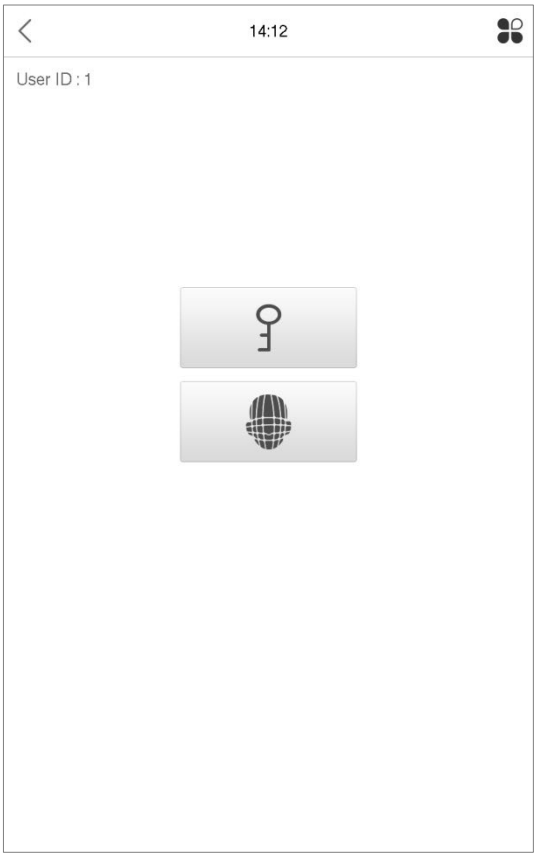
Pressione na interface principal e entre no modo de verificação facial 1:1.

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

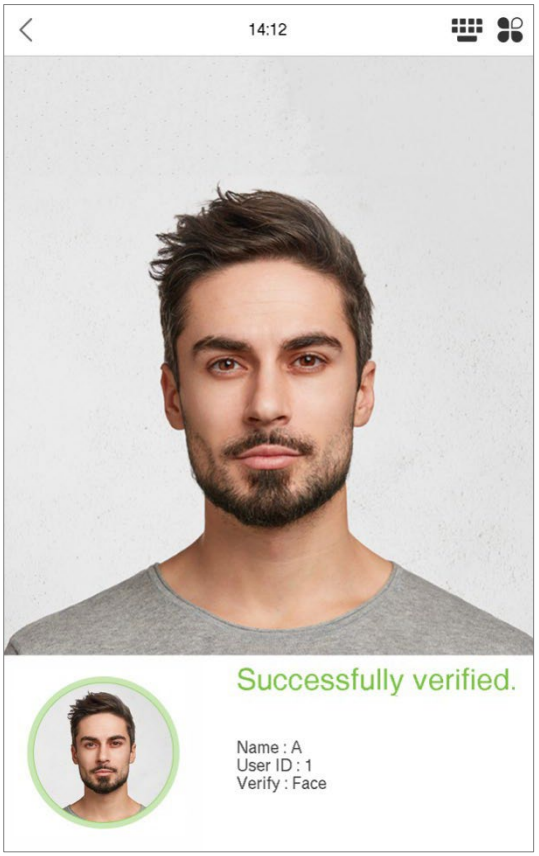


Se o usuário tiver definido uma senha e cadastrado um modelo facial para verificação, a seguinte tela aparecerá.

Selecione o ícone para entrar no modo de verificação facial.



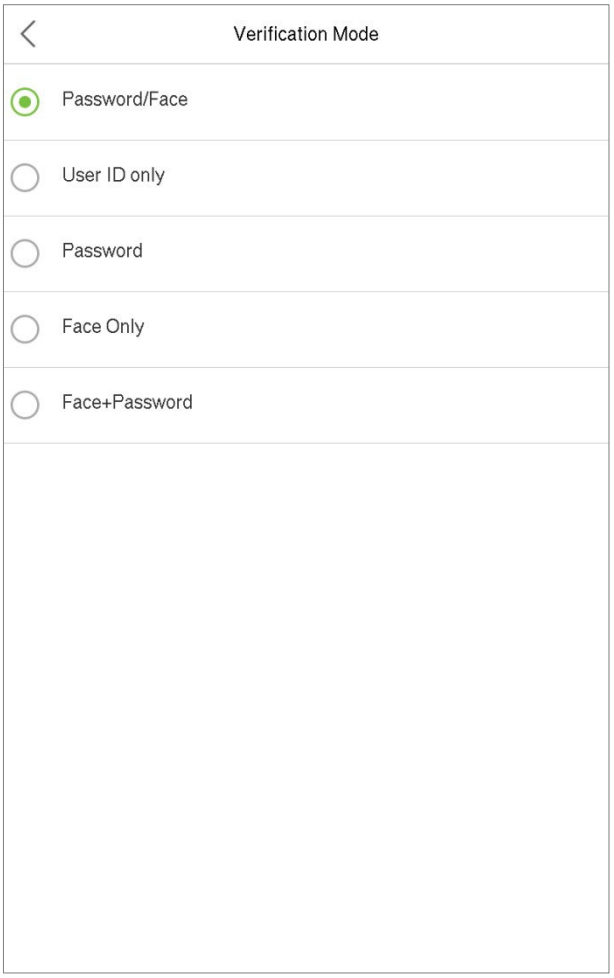
Após a verificação bem-sucedida, o sistema exibirá a seguinte mensagem:



Se a verificação falhar, será exibida a seguinte mensagem: "Ajuste sua posição, por favor!".

1.5.3 Verificação Combinada

Para aumentar o nível de segurança, este dispositivo oferece opções de múltiplas formas de métodos de verificação. Um total de 5 combinações diferentes de verificação podem ser usadas, conforme mostrado abaixo:



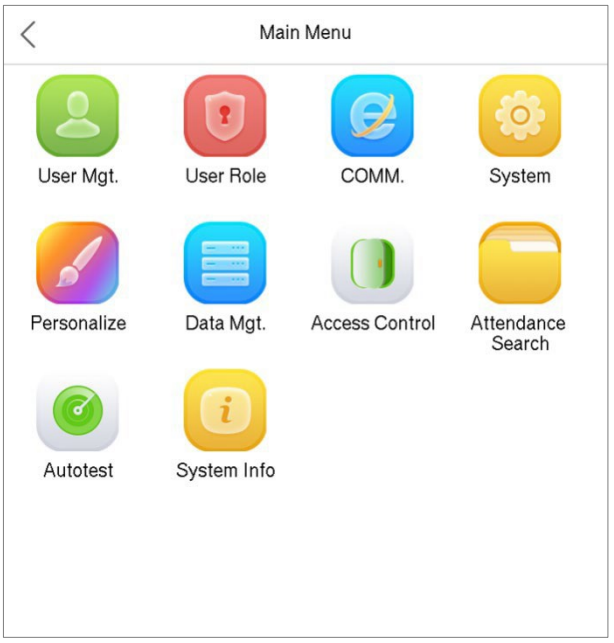
Observação:

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

2) Você deve registrar as informações de verificação necessárias antes da combinação de verificação; caso contrário, a verificação poderá falhar. Por exemplo, se um usuário que apenas registrou um modelo facial escolher "Rosto + Senha" como modo de verificação, esse usuário nunca passará na verificação.

2 Menu Principal

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



Item	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 configurar os parâmetros relevantes de rede, conexão com PC, servidor em nuvem e Wiegand.
Sistema	Para configurar os parâmetros relacionados ao sistema, incluindo data e hora, registros de acesso, modelos faciais, redefinição para configurações de fábrica e gerenciamento de temperatura.
Personalização	Isso inclui configurações de Interface do Usuário, Voz e Alarme.
Ger. Dados	Para excluir todos os dados relevantes no dispositivo.
Controle Acesso	Para configurar os parâmetros da fechadura e do dispositivo de controle de acesso relacionado.
Proc. Registros	Consultar o registro de acesso especificado, verificar fotos de registro de presença e fotos da lista de bloqueios.
Autoteste	Testar automaticamente se cada módulo funciona corretamente, incluindo a tela, o áudio, a câmera e o relógio em tempo real.
Informação de sistema	Visualizar capacidade de dados, informações do dispositivo e firmware do dispositivo atual.

3 Gerenciamento de Usuários

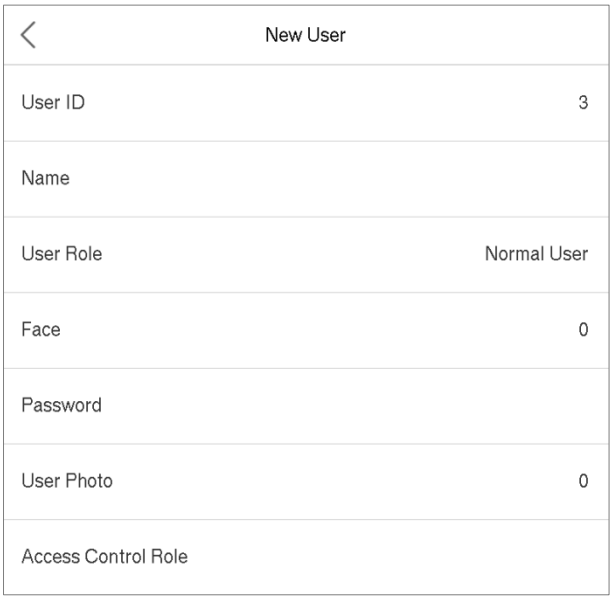
3.1 Adicionar Usuários

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

Clique em **Novo Usuário**.

- **Registre com um ID de Usuário e Nome.**

Digite o ID de usuário e o nome.



Observações:

1) Um nome de usuário pode conter até 17 caracteres.

2) O ID de usuário pode conter de 1 a 9 dígitos por padrão.

3) Durante o registro inicial, você pode modificar seu ID, mas após o registro não poderá ser alterado.

4) Se uma mensagem "O ID já existe" aparecer, você deve escolher outro ID.

- **Definindo a Função do Usuário.**

Existem dois tipos de contas de usuário: **usuário normal** e **super administrador**. Se já houver um administrador registrado, os usuários normais não têm direitos para gerenciar o sistema e só podem acessar autenticações. O administrador possui todos os privilégios de gerenciamento. Se um papel personalizado for definido, você também pode selecionar **privilégios customizados** para o usuário.

Clique em **Função do Usuário** para selecionar Usuário Normal ou Super Administrador.

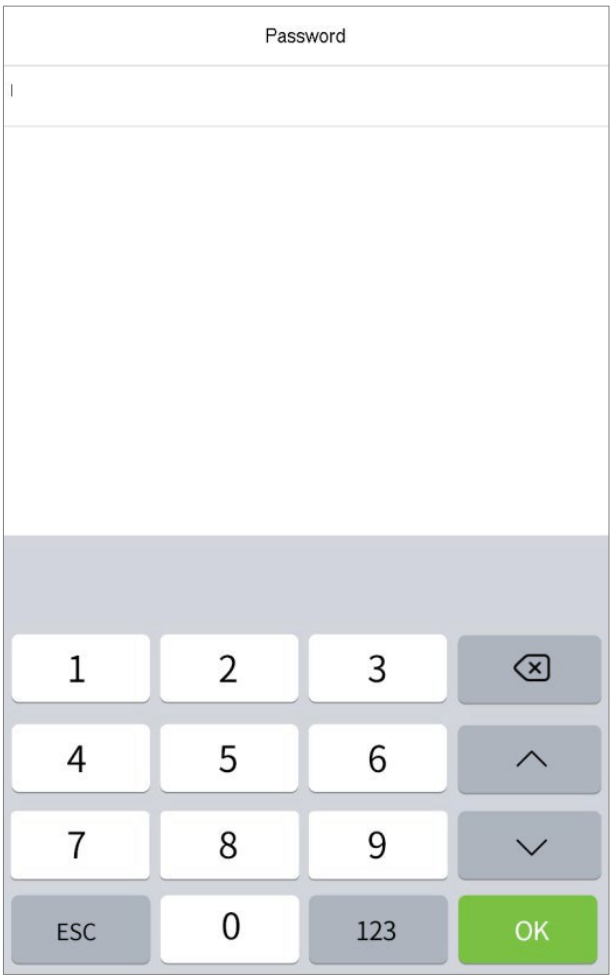
Observação: Se a função de usuário selecionada for Super Admin, o usuário deve passar pela autenticação de identidade para acessar o menu principal. A autenticação é baseada no(s) método(s) de autenticação que o super administrador registrou. Consulte a seção 1.5 Modo de Autenticação para obter mais informações.

- **Cadastrar uma face**

Clique em **Face** para acessar a interface de cadastro facial. Por favor, olhe diretamente para a câmera e mantenha-se imóvel durante o registro facial. A interface de cadastro é a seguinte:

- **Cadastrar uma senha**

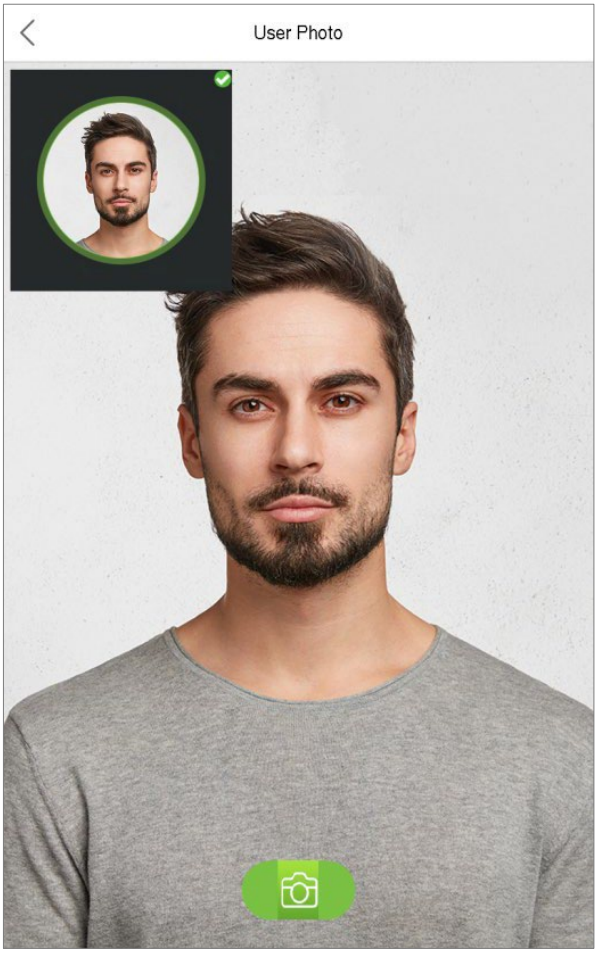
Clique em **Senha** para acessar a página de registro de senha. Digite uma senha e digite-a novamente. Clique em **OK**. Se as duas senhas digitadas forem diferentes, aparecerá a mensagem "Senha não corresponde".



Observação: Por padrão, a senha pode conter de um a oito dígitos.

- **Cadastrar uma foto de usuário**

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



Clique em **Foto do Usuário**, em seguida, clique no ícone da câmera para tirar uma foto. O sistema retornará à interface de Novo Usuário após tirar a foto.

Observação: Durante o registro da face, o sistema capturará automaticamente uma foto como foto do usuário. Se você não deseja registrar uma foto do usuário, o sistema definirá automaticamente a foto capturada como a foto padrão.

- **Função de Controle de Acesso**

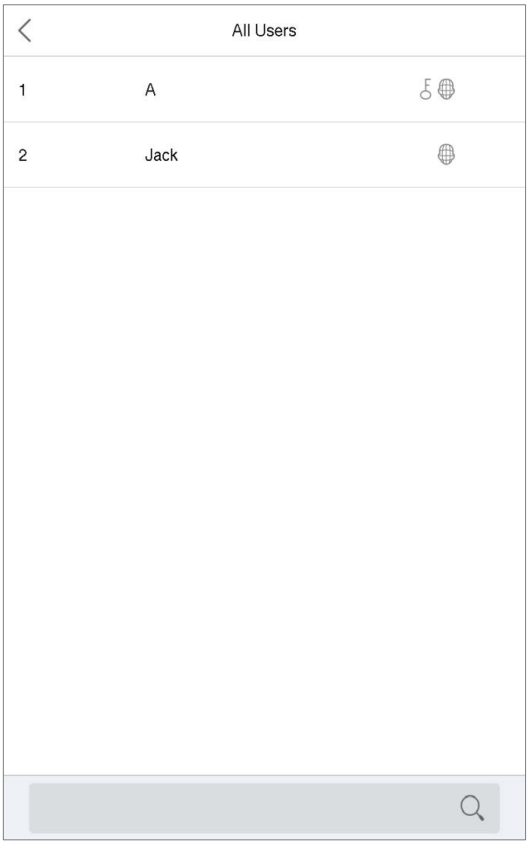
O controle de acesso do usuário define os direitos de desbloqueio de porta de cada pessoa, incluindo o grupo e o período de tempo ao qual o usuário pertence.

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

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

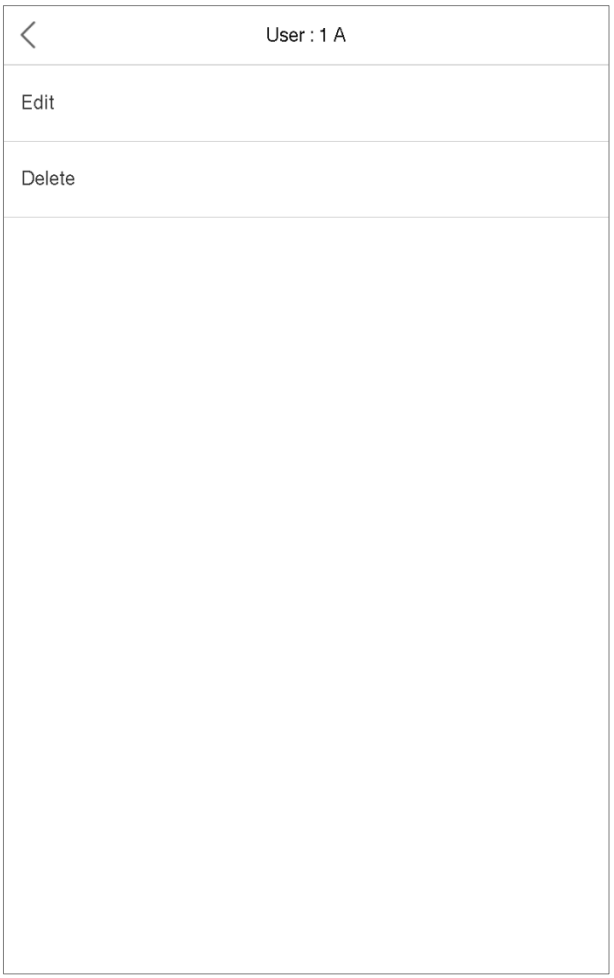
3.2 Buscar Usuários

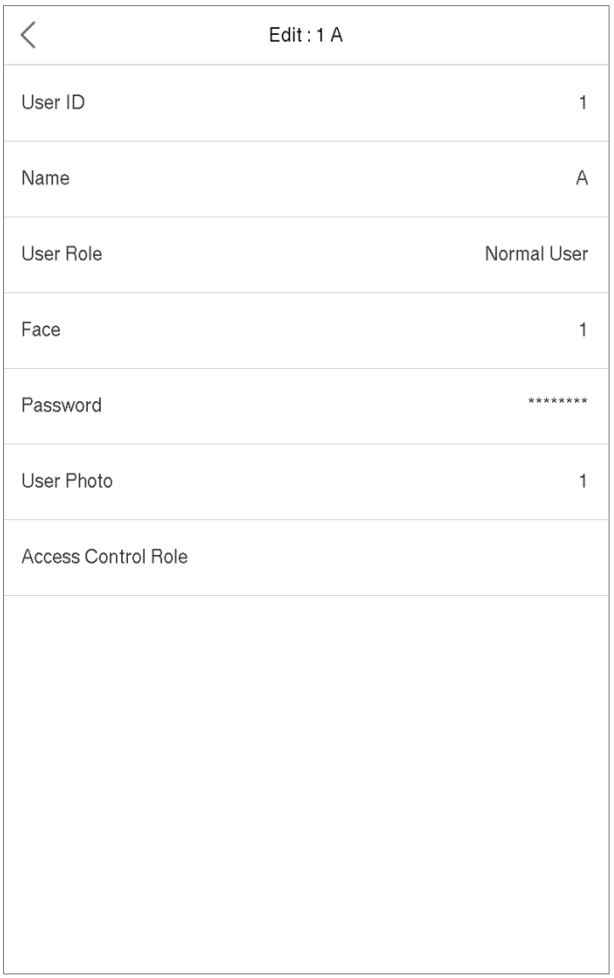
Clique na barra de pesquisa na lista de usuários e digite a palavra-chave de busca; a palavra-chave pode ser um ID, sobrenome ou nome completo. O sistema irá procurar pelos usuários relacionados à informação.



3.3 Editar Usuários

Escolha um usuário da lista e clique em "Editar" para entrar na interface de edição do usuário:





Observação: A operação de edição de um usuário é a mesma que a de adicionar um usuário, exceto que o ID do usuário não pode ser modificado ao editar um usuário. O método de operação refere-se a "3.1 Novos Usuários".

3.4 Excluir Usuários

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

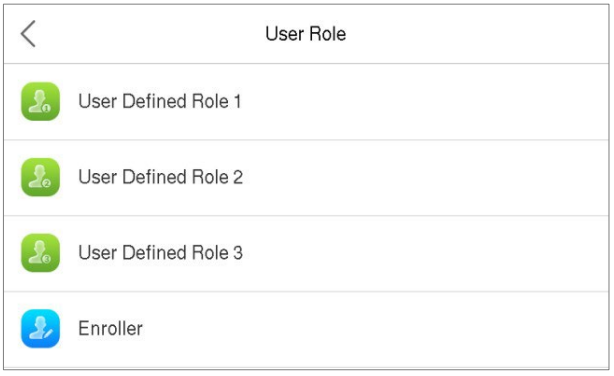
Observação: Se você selecionar **Excluir Usuário,** todas as informações do usuário serão apagadas..

4 Privilégio do Usuário

Se você precisa atribuir permissões específicas a determinados usuários, você pode editar o "Privilégio Definido pelo Usuário" no menu de **Privilégio do Usuário**.

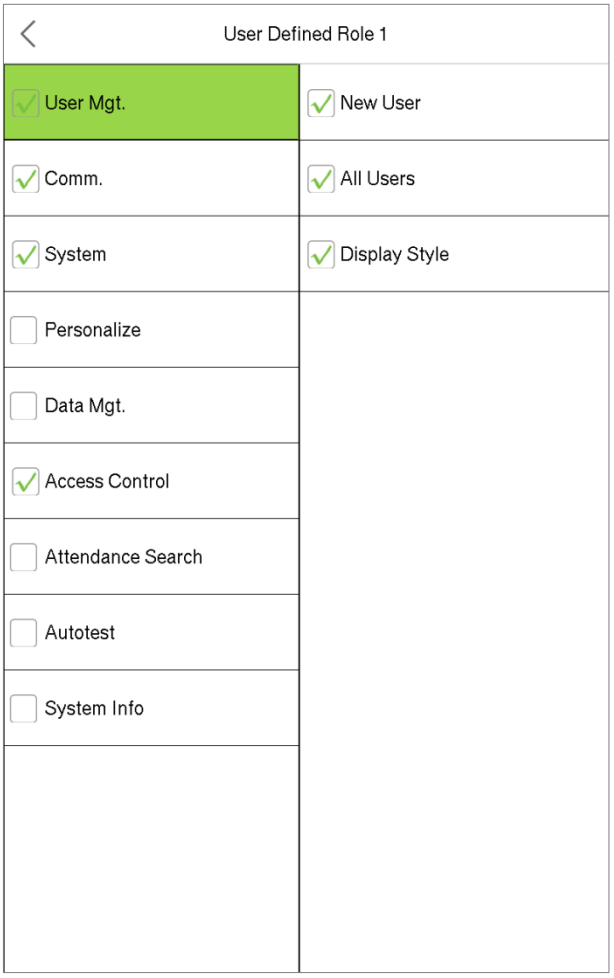
Você pode definir o escopo de permissão da função personalizada (até 3 funções) e do cadastrador, ou seja, o escopo de permissão do menu de operações.

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

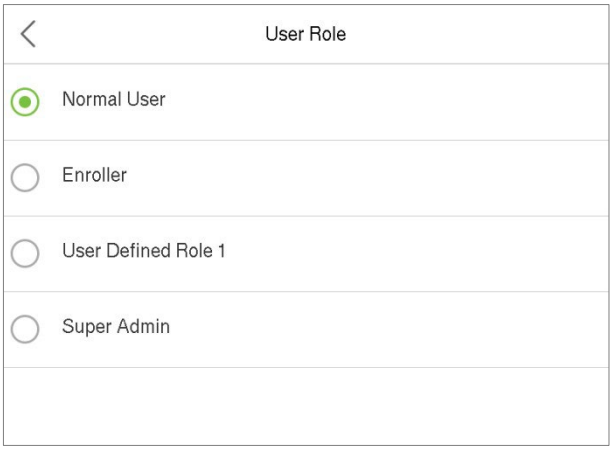


Clique em qualquer item para definir uma função específica. Clique na linha **Habilitar Função Definida** para ativar essa função definida. Clique em **Nome** e digite o nome da função.

Clique em **Definir Priv. Usuário** para atribuir os privilégios à função. Quando a atribuição de privilégios estiver concluída, clique em **Retornar**.



Observação: Durante a atribuição de privilégios, o menu principal está à esquerda e seus submenus estão à direita. Você só precisa selecionar as funcionalidades mostradas nos submenus. Se o dispositivo tiver uma função habilitada, você pode atribuir as funções que definiu aos usuários clicando em "Usuário Adm." > "Novo Usuário" > "Priv. Usuário".

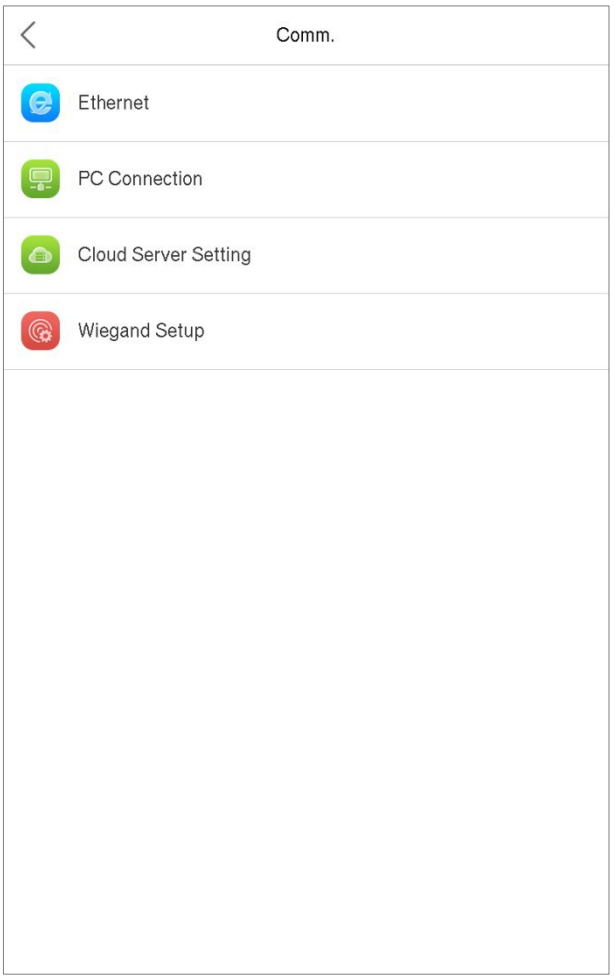


Se nenhum super administrador estiver registrado, o dispositivo exibirá a mensagem "Por favor, registre primeiro um usuário super administrador!" após clicar na barra de habilitação.

5 Configurações de Comunicação

Defina os parâmetros de rede, conexão com PC, servidor em nuvem e Wiegand.

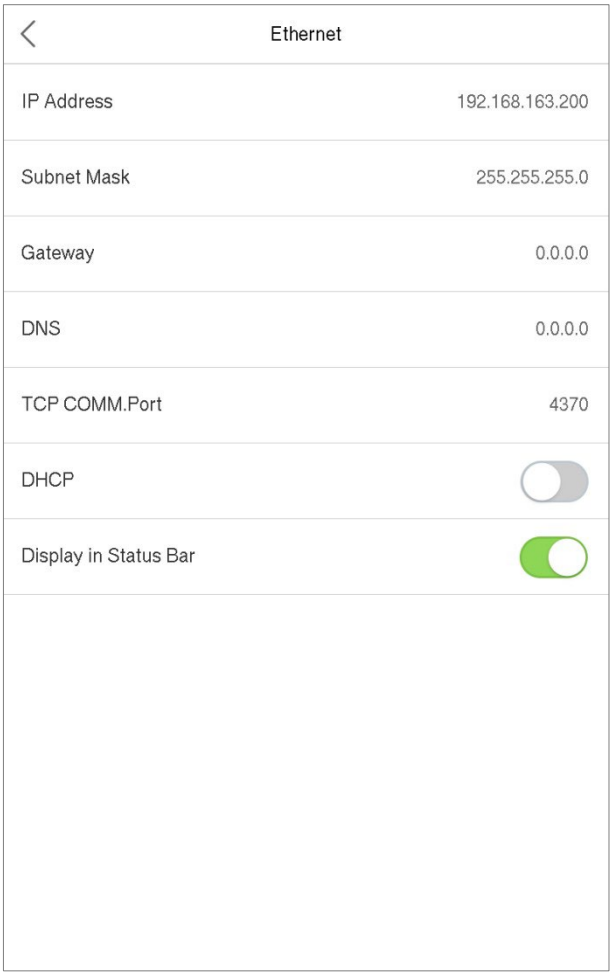
Toque em **Conf. Com.** no menu principal.



5.1 Configurações de Rede

Quando o dispositivo precisa se comunicar com um PC por meio da Ethernet, você precisa configurar as configurações de rede e garantir que o dispositivo e o PC estejam conectados ao mesmo segmento de rede.

Clique em **TCP/IP** na interface de Configurações de Comunicação.

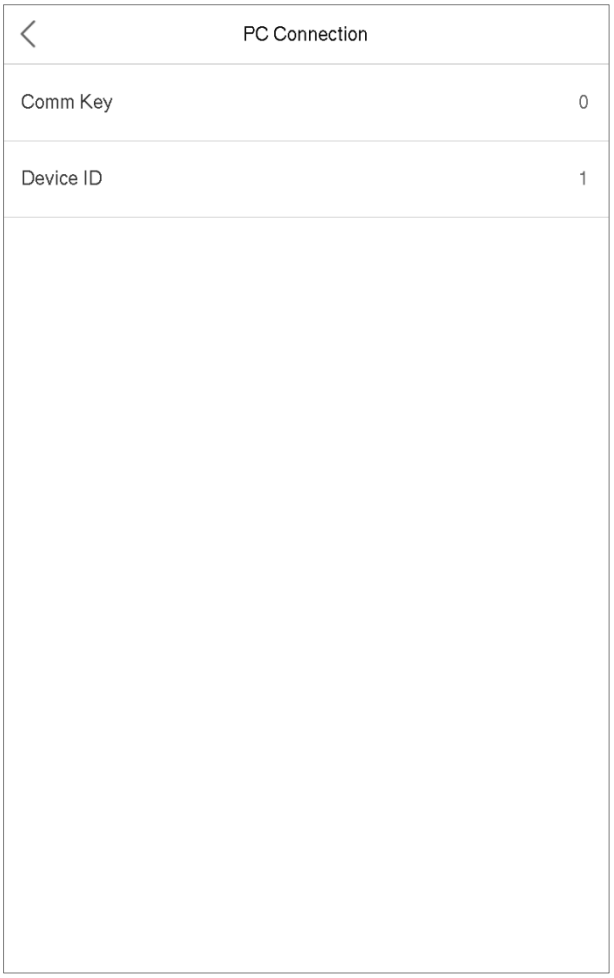


Item	Descrição
TCP/IP	O valor padrão de fábrica é 192.168.1.201. Por favor, ajuste de acordo com a situação de rede real.
Máscara de Rede	O valor padrão de fábrica é 255.255.255.0. Por favor, ajuste de acordo com a situação de rede real.
Gateway	O endereço padrão de fábrica é 0.0.0.0. Por favor, ajuste de acordo com a situação de rede real.
DNS	O endereço padrão de fábrica é 0.0.0.0. Por favor, ajuste de acordo com a situação de rede real.
Porta de Com. TCP	O valor padrão de fábrica é 4370. Por favor, ajuste de acordo com a situação de rede real.
DHCP	Dynamic Host Configuration Protocol (DHCP) é um protocolo utilizado para a alocação dinâmica de endereços IP para clientes por meio de um servidor.
Mostrar na barra status	Para definir se o ícone de rede será exibido na barra de status da tela incial.

5.2 Conexão com o PC

Para aumentar a segurança dos dados, por favor defina uma Chave de Comunicação para a comunicação entre o dispositivo e o PC. Se uma Chave de Comunicação for definida, essa senha de conexão deverá ser inserida antes de conectar o dispositivo ao software do PC.

Clique em **Conexão PC** na interface de Configurações de Comunicação.

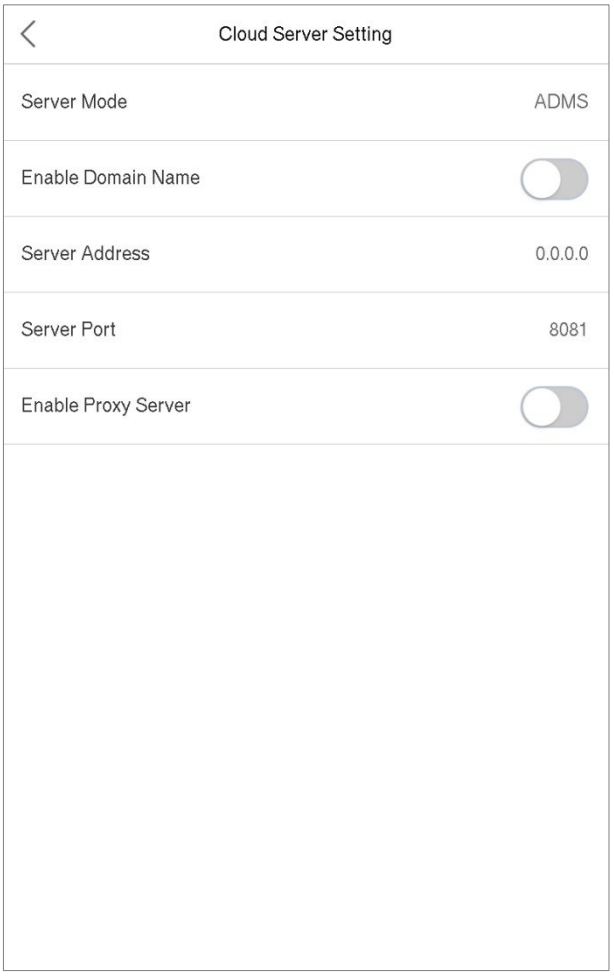


Item	Descriptions
Senha de Comunicação	A senha padrão é 0, que pode ser alterada. A senha de comunicação pode conter de 1 a 6 dígitos.
ID do aparelho	Número de identificação do dispositivo na rede serial, que varia entre 1 e 254. Se o método de comunicação for RS232/RS485, você precisa inserir este ID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

5.3 Configuração do Servidor em Nuvem

Isso representa as configurações usadas para conectar com o servidor ADMS.

Clique em **Configuração do Servidor de Nuvem** na interface de Configurações de Comunicação.

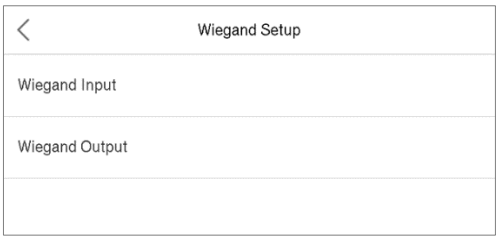


Item		Descrição
Ativar nome de domínio	**Endereço do servidor**	Quando essa função está ativada, o modo de nome de domínio "http://..." será utilizado, como por exemplo http://www.XYZ.com, sendo que "XYZ" representa o nome de domínio quando esse modo está ativado.
Desativar nome de domínio	**Endereço do servidor**	O endereço IP do servidor ADMS.
	Porta do servidor	Port used by the ADMS server.
Ativar servidor proxy		Ao optar por habilitar o proxy, você precisa definir o endereço IP e o número da porta do servidor proxy

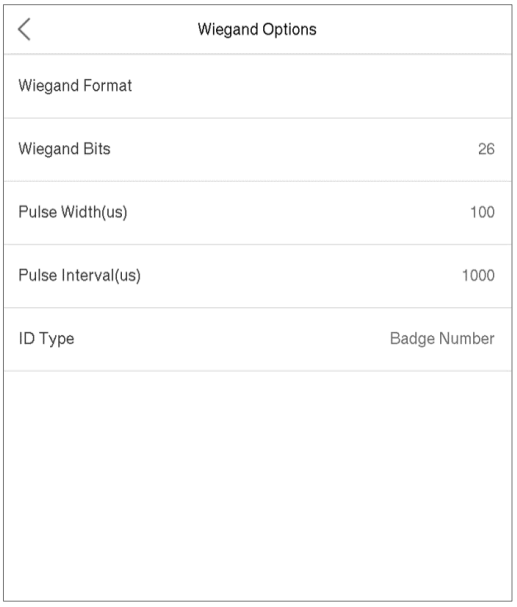
5.4 Configuração de Wiegand

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**



Item	Descrição
Formato Wiegand	Disponíveis: 26 bits, 34 bits, 36 bits, 37 bits e 50 bits.
Bits Wiegand	Número de bits dos dados Wiegand.
Largura de pulso(us)	O valor da largura de pulso enviada pelo Wiegand é de 100 microssegundos por padrão, podendo ser ajustado dentro da faixa de 20 a 100 microssegundos.
Intervalo de pulso (us)	O valor padrão é de 1000 microssegundos, podendo ser ajustado dentro da faixa de 200 a 20000 microssegundos.
Tipo de ID	Selecione entre ID do usuário e número do cartão.

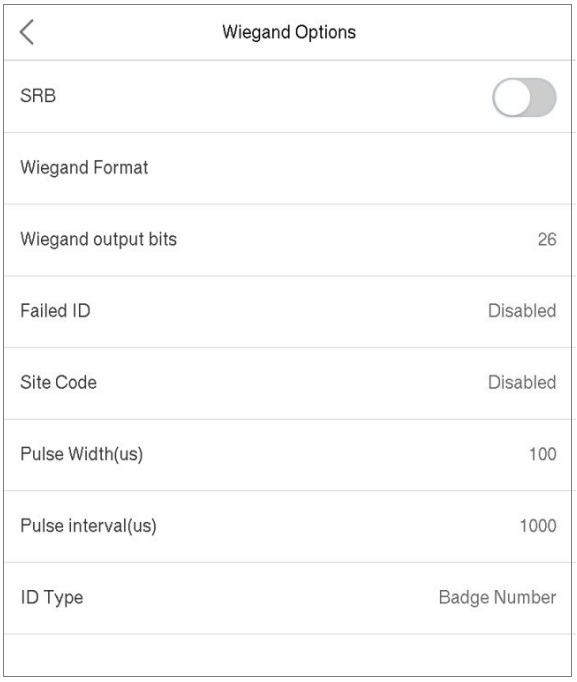
Definições de diferentes formatos comuns de Wiegand:

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	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE Consiste em 37 bits de código binário. O 1º bit é o bit de paridade ímpar do 2º ao 18º bits, enquanto o 37º bit é o bit de paridade par do 19º ao 36º bits. O 2º ao 4º bits são os códigos do fabricante. O 5º ao 16º bits são os site code e os 21º ao 36º bits são os números do cartão.

Wiegand37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Consiste em 37 bits de código binário. O 1º bit é o bit de paridade par do 2º ao 18º bits, enquanto o 37º bit é o bit de paridade ímpar do 19º ao 36º bits. O 2º ao 4º bits são os códigos do fabricante. O 5º ao 14º bits são os códigos do dispositivo, e o 15º ao 20º bits são os site code e os 21º ao 36º bits são os números do cartão.
Wiegand50	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; and "**S**" Site code.

➢ Saída Wiegand

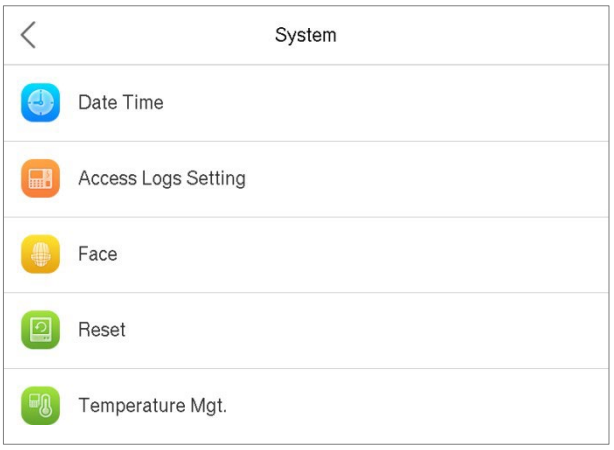


Item	Descrição
SRB	Quando o dispositivo estiver conectado ao SRB, selecione Habilitar. Nesse momento, os parâmetros de saída Wiegand não podem ser configurados.
Formato Wiegand	26 bits, 34 bits, 36 bits, 37 bits, and 50 bits available.
Bits de saída Wiegand	Após escolher o formato Wiegand, você pode selecionar um dos dígitos de saída correspondentes no formato Wiegand.
Código com Falha	Se a verificação falhar, o sistema enviará o ID falhado para o dispositivo e substituirá o número do cartão ou ID do pessoal pelos novos.
Site Code	É semelhante ao ID do dispositivo. A diferença é que um código de local pode ser configurado manualmente e pode ser repetido em um dispositivo diferente. O valor válido varia de 0 a 256 por padrão.
Largura do pulso (us)	A largura do tempo representa as mudanças da quantidade de carga elétrica com capacitância de alta frequência de forma regular dentro de um tempo especificado.
Intervalo de pulso (us)	O intervalo de tempo entre pulsos.
Tipo de ID	Selecione entre ID do usuário e número do crachá.

6 Configurações de Sistema

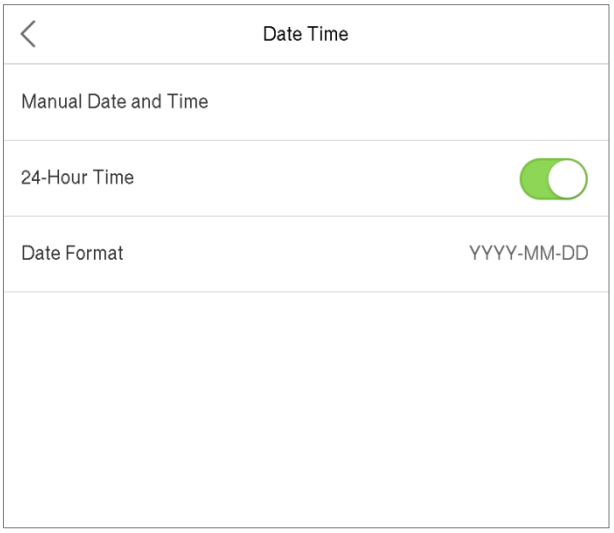
Configure os parâmetros do sistema relacionados para otimizar o desempenho do dispositivo.

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



6.1 Data e Hora

Toque em **Data e Hora** na interface do Sistema.



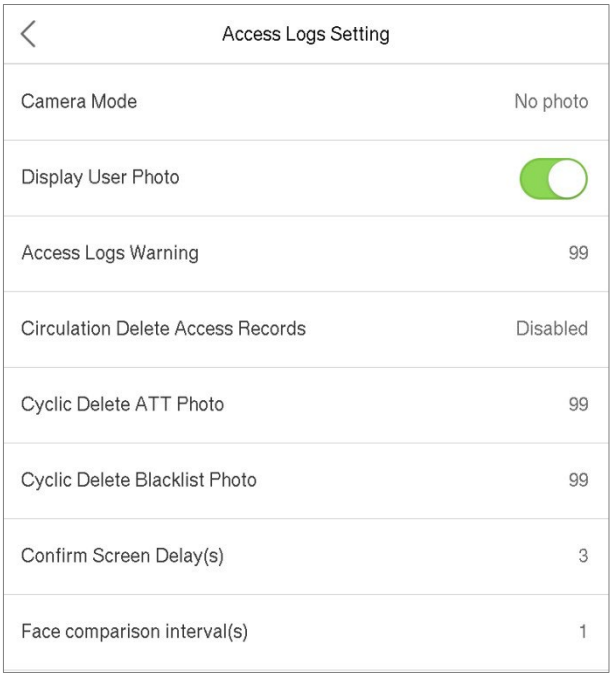
1. Você pode configurar manualmente a data e a hora e clicar em Confirmar para salvar.
2. Clique em Horário de 24 horas para habilitar ou desabilitar esse formato e selecione o formato de data.

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

Observação: Por exemplo, se o usuário configurar o horário do dispositivo para 18h35 do dia 15 de março de 2019 e, em seguida, restaurar as configurações de fábrica, o horário do equipamento permanecerá como 18h30 do dia 1º de janeiro de 2020.

6.2 Configuração de Registros de Acesso

Clique em **Conf. reg. de acesso** na interface do sistema.

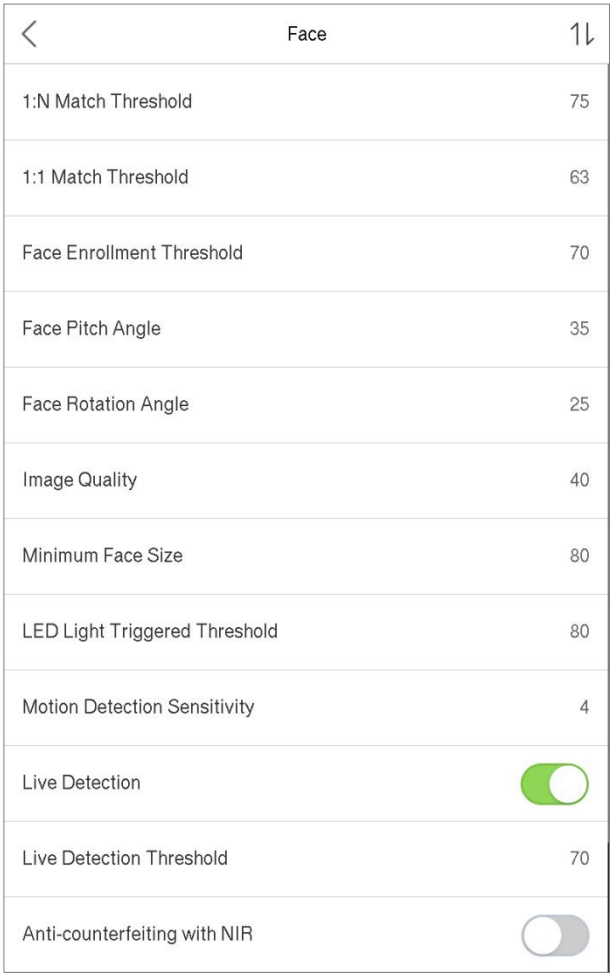


Item	Descrição
Modo de câmera	Se deseja capturar e salvar a imagem instantânea durante a verificação. Existem 5 modos: **Sem Foto:** Nenhuma foto é tirada durante a verificação do usuário. **Tirar foto, não salvar:** Uma foto é tirada, mas não é salva durante a verificação. **Tirar foto e salvar:** Uma foto é tirada e salva durante a verificação. **Salvar em verificação bem-sucedida:** Uma foto é tirada e salva para cada verificação bem-sucedida. **Salvar em verificação falha:** Uma foto é tirada e salva durante cada verificação falha.
Exibir foto do usuário	Se deseja exibir a foto do usuário quando ele passa pela verificação.
Aviso de logs de acesso	Quando o espaço de registro restante atingir um valor definido, o dispositivo exibirá automaticamente um aviso de memória de registro restante. Os usuários podem desativar a função ou definir um valor válido entre 1 e 9999.
Exclusão cíclica dos registros de acesso	Quando os registros de acesso atingem a capacidade máxima, o dispositivo automaticamente deletará um valor definido de registros antigos de acesso. Os usuários podem desativar a função ou definir um valor válido entre 1 e 999.

Exclusão cíclica de fotos de ponto	Quando as fotos de registro de presença atingem a capacidade máxima, o dispositivo automaticamente deletará um valor definido de fotos antigas de registro de presença. Os usuários podem desativar a função ou definir um valor válido entre 1 e 99.
Exclusão cíclica de fotos da lista de bloqueios	Quando as fotos da lista de bloqueios atingirem a capacidade máxima, o dispositivo excluirá automaticamente um conjunto de fotos antigas da lista. Os usuários podem desativar a função ou definir um valor válido entre 1 e 99.
Atraso de tela (s)	O tempo em que a mensagem de autenticação bem-sucedida é exibida. Valor válido: 1 a 9 segundos.
Intervalo de comparação facial (s)	Definir o intervalo de tempo para correspondência de modelo facial conforme necessário. Valor válido: 0 a 9 segundos.

6.3 Parâmetros de Face

Clique em **Face** na interface do sistema.



FRR	FAR	Limiares de correspondência recomendados	
		1:N	1:1
Alto	Baixo	85	80
Médio	Médio	82	75
Baixo	Alto	80	70

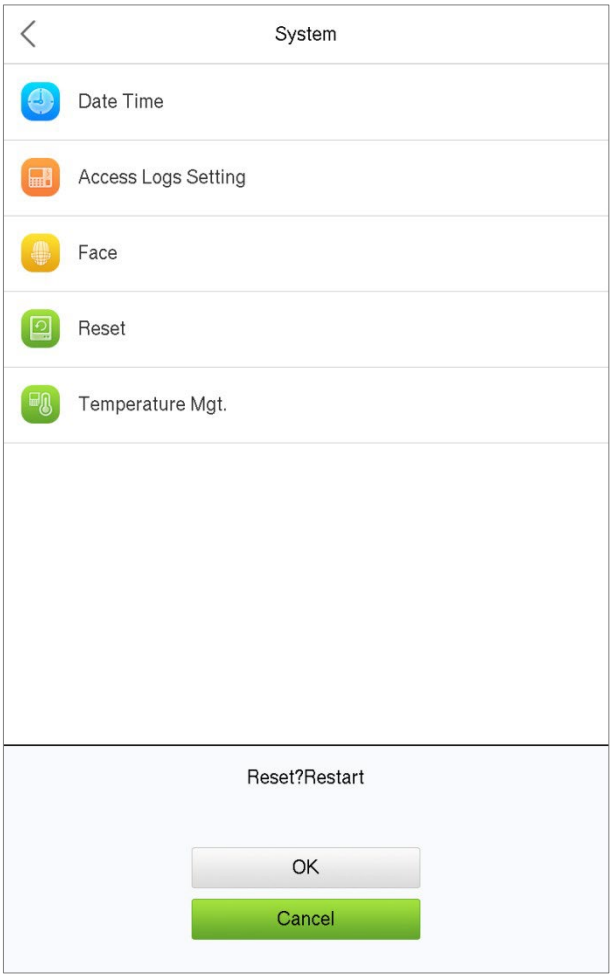
Item	Descrição
Limiar 1:N	No modo de verificação 1:N, a verificação será bem-sucedida somente quando a similaridade entre a imagem facial adquirida e todos os modelos faciais registrados for maior que o valor definido. O valor válido varia de 65 a 120. Quanto mais alto for o limiar definido, menor será a taxa de erro de julgamento e maior será a taxa de rejeição, e vice-versa.
Limiar 1:1	No modo de verificação 1:1, a verificação será bem-sucedida somente quando a similaridade entre a imagem facial adquirida e os modelos faciais registrados no dispositivo for maior que o valor definido. O valor válido varia de 55 a 120. Quanto mais alto for o limiar definido, menor será a taxa de erro de julgamento e maior será a taxa de rejeição, e vice-versa.

Limiar de registro facial	Durante o registro facial, é utilizada a verificação 1:N para determinar se o usuário já está registrado. O rosto atual é registrado quando a similaridade entre a imagem facial adquirida e todos os modelos faciais registrados é maior que o valor definido.
Ângulo de inclinação da face	Para limitar o ângulo de inclinação da face na autenticação facial, o valor recomendado é de 20.
Ângulo de rotação da face	Para limitar o ângulo de rotação da face na autenticação facial, o valor recomendado é de 20.
Qualidade da Imagem	Para obter o limite de qualidade das imagens faciais. Quando o valor da qualidade da imagem é maior que o valor definido, o dispositivo aceitará as imagens faciais e iniciará o processamento do algoritmo; caso contrário, o dispositivo filtrará as imagens faciais.
Tamanho Mínimo da Face	Para limitar o tamanho de detecção da face em pixels na autenticação facial, o limite recomendado é de 80.
Limiar para acionamento da luz LED	Detectar a intensidade da luz ambiente. Quando o brilho do ambiente é menor que o limite, a luz de preenchimento é ligada; quando o brilho do ambiente é maior que esse limite, a luz de preenchimento não é ligada. O valor padrão é 80.
Sensibilidade de detecção de movimento	Durante a autenticação facial, as imagens faciais em movimento coletadas ao longo do tempo são comparadas com todas as imagens faciais armazenadas no dispositivo pelo algoritmo correspondente. Se o valor for maior ou igual ao valor definido, significa que a verificação é bem-sucedida; caso contrário, significa que a verificação falhou.
Detecção de face viva	Se ativado, ele irá detectar automaticamente se há uma pessoa em movimento em frente ao dispositivo.
Limiar de Detecção em Tempo Real	Detectar se há uma pessoa em movimento em frente ao dispositivo para determinar se a autenticação facial está ativada. O valor padrão é 100. O valor válido varia de 0 a 100.
Antifalsificação por infravermelho	Se ativado, a imagem será capturada pela câmera preto e branco para determinar se o rosto pertence a uma pessoa real.
WDR	Ampla Faixa Dinâmica
Modo Antioscilação	Configurar para evitar o piscar da tela.
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 Redefinição de Fábrica

Restaurar o dispositivo, como as configurações de comunicação e configurações do sistema, para as configurações de fábrica sem apagar os dados de usuário registrados.

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

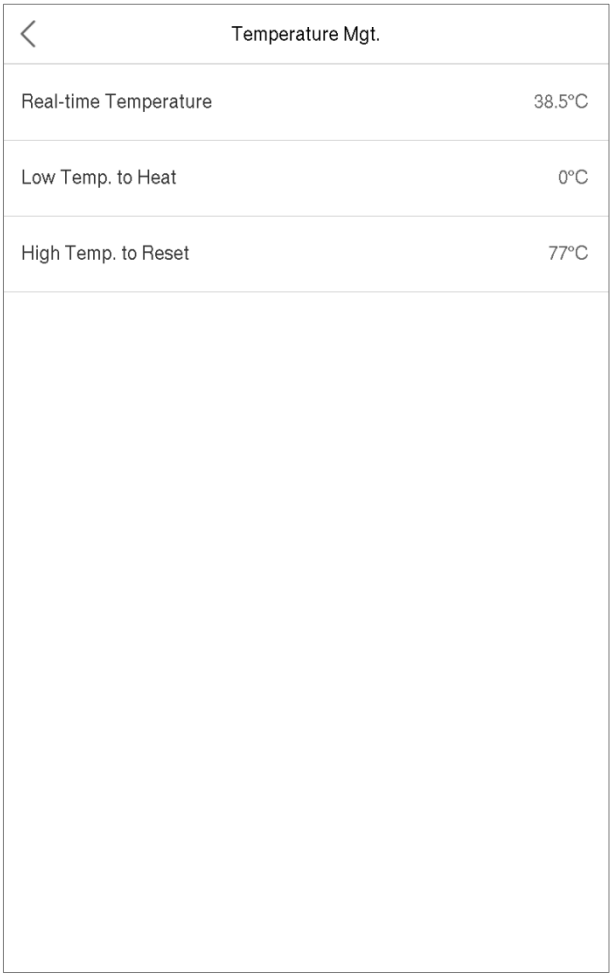


Clique em **OK** para confirmar a redefinição.

6.5 Gerenciamento de Temperatura

O terminal possui um sensor de temperatura incorporado. Quando a temperatura está muito baixa ou muito alta, ele ativará o aquecimento automático ou desligará.

Clique em **Gerenciamento de Temperatura** na interface do Sistema.



Item	Descrição
Temperatura em Tempo Real	Esta coluna exibe a temperatura interna em tempo real do terminal.
Temperatura Muito Baixa	Quando a temperatura do terminal está abaixo do valor definido, ele iniciará o aquecimento automático. A faixa de valor definida é de 0 a 10ºC.
Temperatura Muito Alta	Quando a temperatura do terminal é maior que o valor definido, ele desligará automaticamente para proteger o hardware. A faixa de valor definida é de 60 a 80ºC.

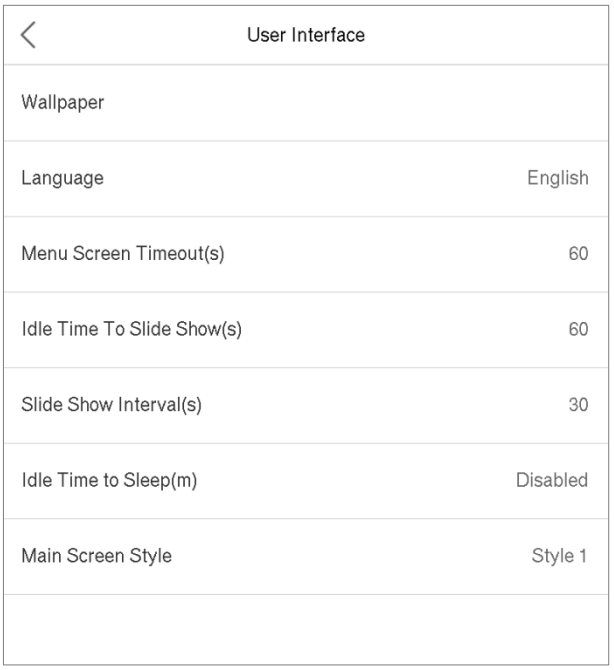
7 Configurações de Personalização

Você pode personalizar as configurações da interface, áudio e campainha. Clique em **Personalizar** no menu principal.

7.1 Configurações da Exibição

Você pode personalizar o estilo de exibição da interface principal.

Clique em **Interface do Usuário** no menu Personalizar.

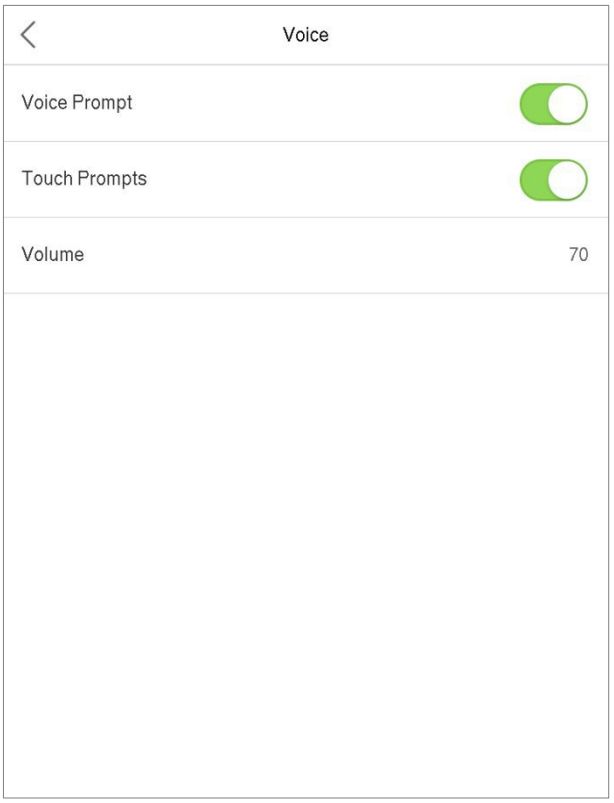


Item	Descrição
Papel de parede	Permite selecionar o papel de parede da tela principal.
Idioma	Permite selecionar o idioma do dispositivo.
Tempo limite da tela do menu (s)	Quando não há utilização e o tempo excede o valor definido, o dispositivo retornará automaticamente à tela inicial. A função pode 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

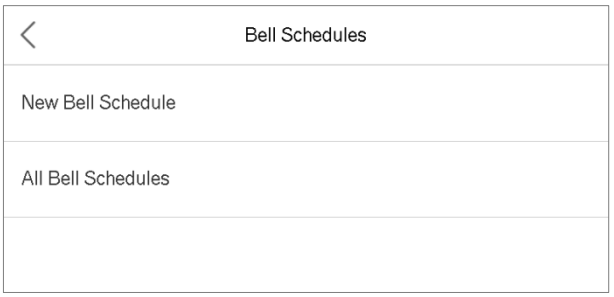
Toque em **Opções de Voz** na interface Personalização para definir as configurações de voz.



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

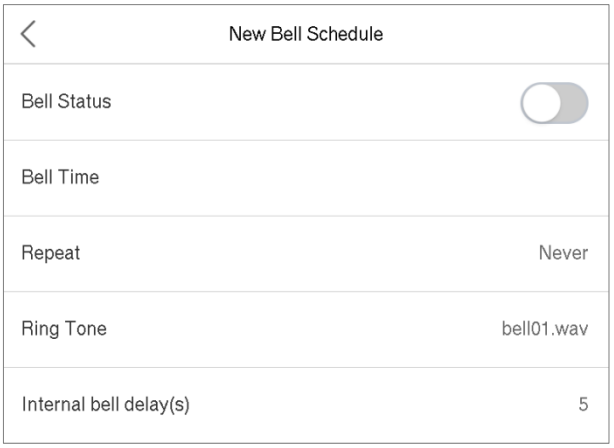
7.3 Horários

Toque em **Horários** na interface Personalização.



- **Novo Alarme**

1. Clique em **Novo Alarme** para acessar a interface de adição:



Item	Descrição
Status da Campainha	Defina se deseja habilitar o status da campainha.
Horário da Campainha	Neste momento do dia, o dispositivo toca a campainha automaticamente.
Repetir	Configure o ciclo de repetição da campainha.
Toque	Selecione um toque de campainha.
Intervalo campainha (s)	Defina a duração da campainha interna. Os valores válidos variam de 1 a 999 segundos.

2. De volta à interface de Horários, clique em Todos os Horários para visualizar a campainha recém-adicionada.

- **Editar uma campainha**

Na interface de Todos os Horários, toque na campainha que deseja editar.

Clique em **Editar**, o método de edição é o mesmo que as operações de adição de uma campainha.

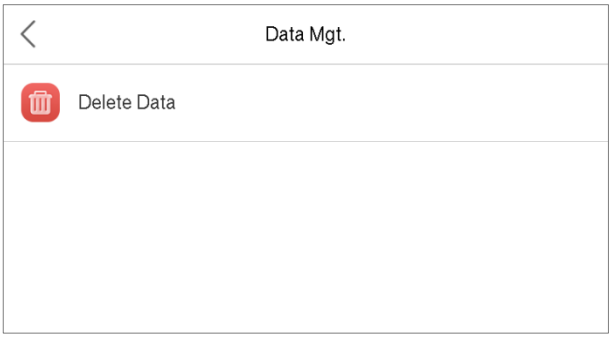
- **Excluir uma campainha**

Na interface de **Todos os Horários**, toque na campainha que deseja excluir. Toque em **Excluir** e selecione [**Sim**] para excluir a campainha.

8 Gerenciamento de Dados

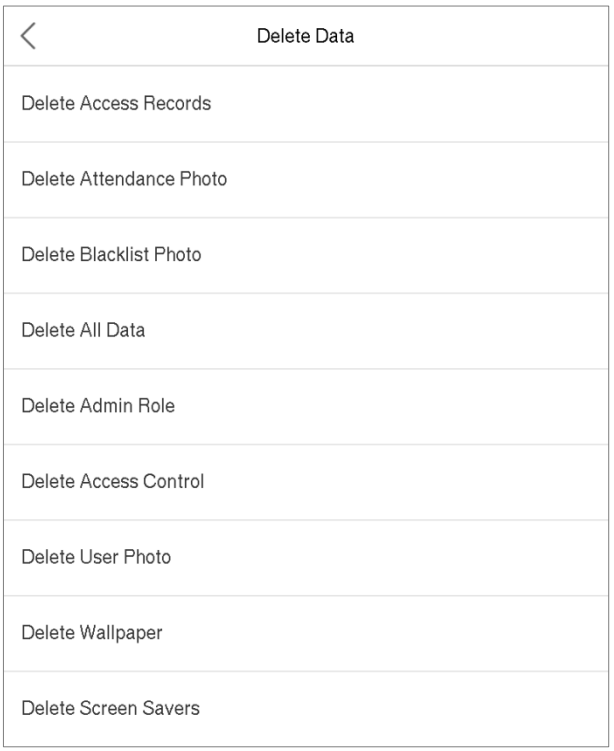
Para excluir os dados relevantes no dispositivo.

Clique em **Ger. Dados** no menu principal.



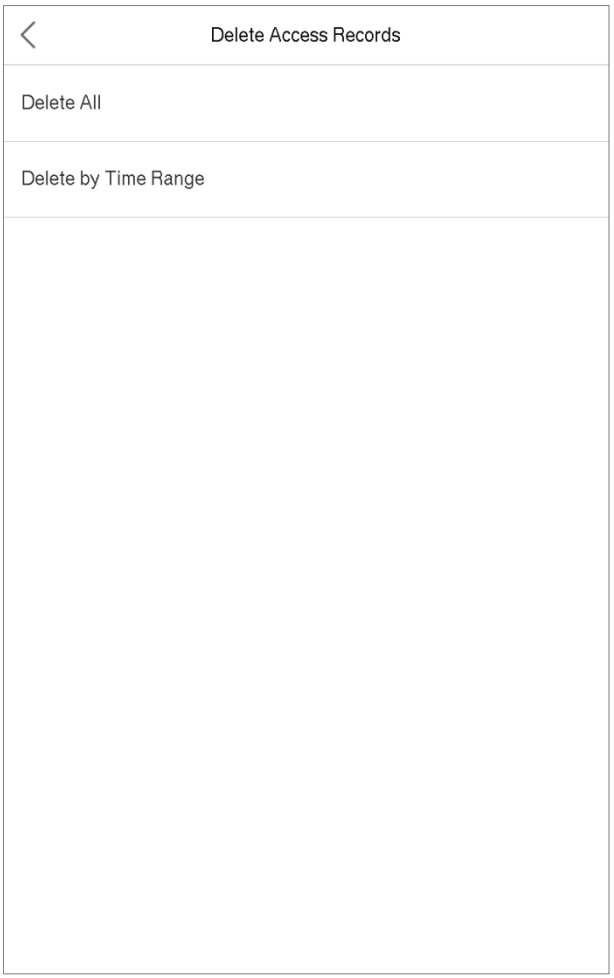
8.1 Excluir dados

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

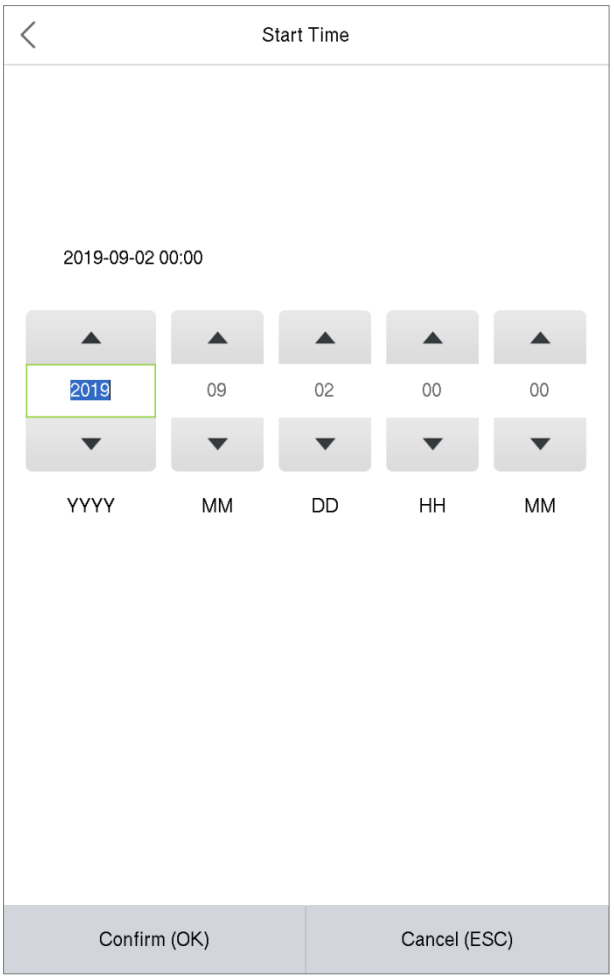


Item	Descrição
Apagar reg. de acesso	Para apagar registros de acesso
Apagar foto ponto	Para apagar fotos de ponto registradas.
Apagar foto lista bloqueio	Para apagar as fotos tiradas durante verificações com falha
Apagar todos os dados	Para apagar informações e registros de todos os usuários registrados.
Apagar privilégios de administrador	Para remover todos os privilégios de administrador.
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

Observação: Ao excluir os registros de acesso, fotos de presença ou fotos da lista de bloqueios, você pode selecionar Excluir Tudo ou Excluir por Intervalo de Tempo. Ao escolher Excluir por Intervalo de Tempo, é necessário definir um período de tempo específico para excluir todos os dados dentro desse período.



Selecione Excluir por Intervalo de Tempo.

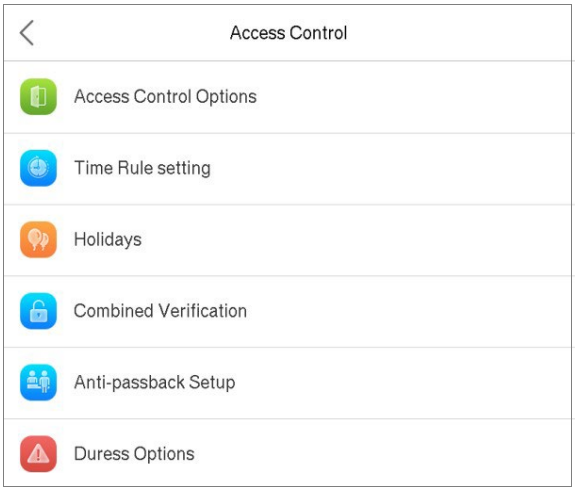


Defina o intervalo de tempo e clique em OK.

9 Controle de acesso

O Controle de Acesso é usado para definir o cronograma de abertura de portas, controle de fechaduras e outras configurações de parâmetros relacionados ao controle de acesso.

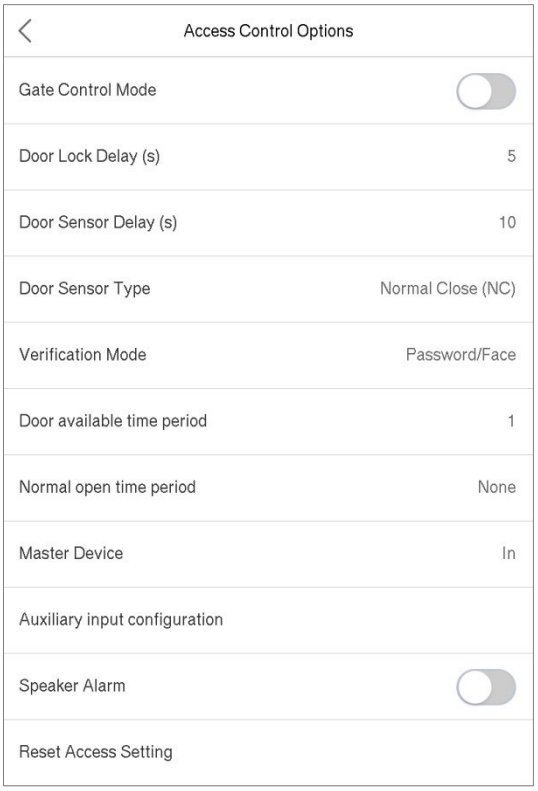
Clique em **Controle de Acesso** no menu principal.

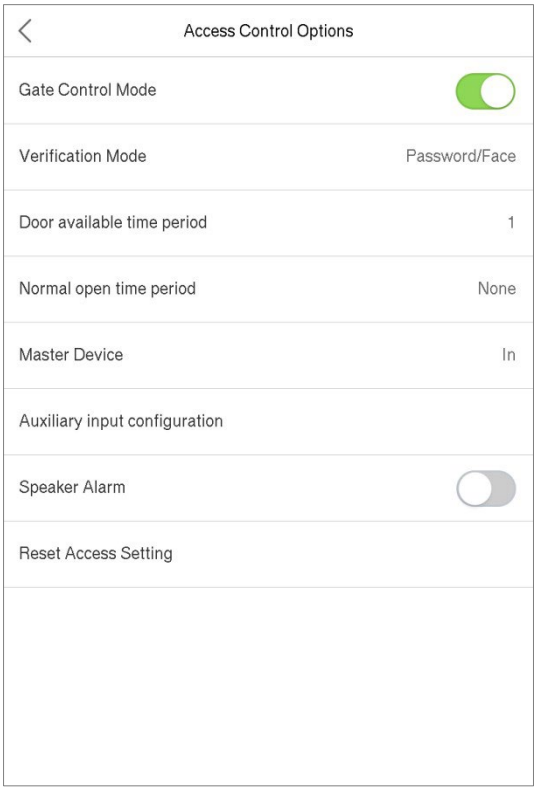


9.1 Opções de Controle de Acesso

Para definir os parâmetros do controle da fechadura do terminal e do equipamento relacionado.

Clique em **Opções de Controle de Acesso** na interface de Controle de Acesso.





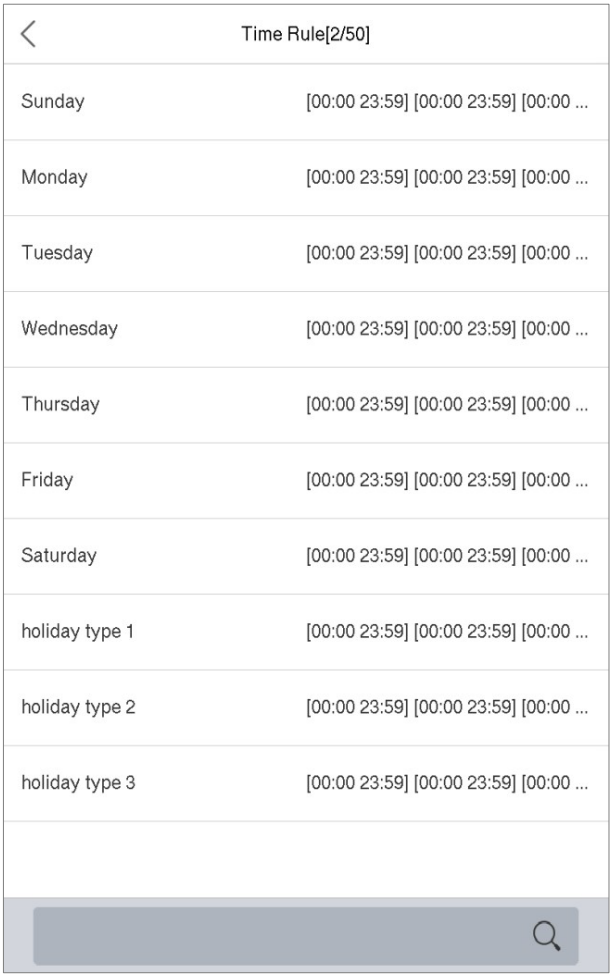
Item	Descrição
Modo de Controle de Porta	Selecione se deseja habilitar o Modo de Controle de Porta. Quando estiver habilitado, o Relé de Fechadura da Porta, o Relé do Sensor da Porta e o Tipo de Sensor da Porta não serão exibidos.
Tempo de trava (s)	Tempo de acionamento do relé após uma autenticação válida. Valor válido: 1~10 segundos; 0 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 tipos: Nenhum, Normalmente Aberto e Normalmente Fechado. Nenhum significa que o sensor da porta não está em uso; Normalmente Aberto significa que a porta está sempre aberta quando a eletricidade está ligada; Normalmente Fechado significa que a porta está sempre fechada quando a eletricidade está ligada.
Modo de verificação	Os modos de verificação suportados incluem face, ID do usuário, senha, senha/face e face + senha.
Período de Disponibilidade da Porta	O período de tempo em que o usuário pode abrir a porta, pode ser configurado em uma das 50 regras de tempo.
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 como entrada ou saída. **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	Defina o período de tempo de desbloqueio da porta e o tipo de saída auxiliar do dispositivo do terminal auxiliar. Os tipos de saída auxiliar incluem Nenhum, Acionar Abertura da Porta, Acionar Alarme, Acionar Abertura da Porta e Alarme.
Alarme de Alto-Falante	Para transmitir um alarme sonoro ou alarme de desmontagem localmente. Quando a porta está fechada ou a verificação é bem-sucedida, o sistema cancelará o alarme localmente.
Redefinir Configuração de Acesso	Os parâmetros de controle de acesso restaurados incluem atraso da fechadura da porta, atraso do sensor da porta, tipo de sensor da porta, modo de verificação, período de disponibilidade da porta, período de abertura normal, dispositivo mestre e alarme. No entanto, não inclui os dados de controle de acesso excluídos no Gerenciamento de Dados.

9.2 Regras de Tempo

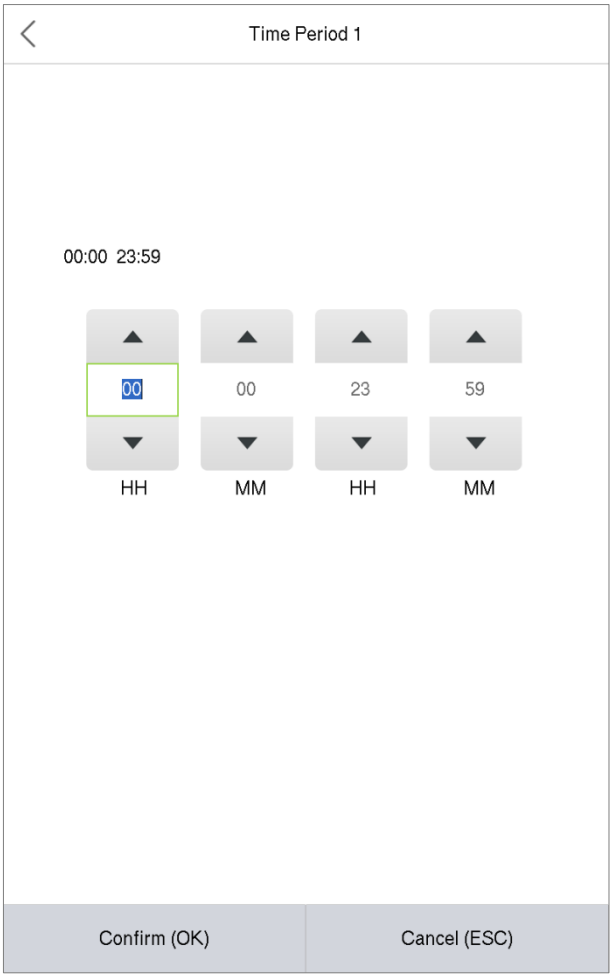
O dispositivo pode definir até 50 regras de tempo. Cada regra de tempo representa dez fusos horários, ou seja, uma semana e 3 feriados, e cada fuso horário é um período de tempo válido dentro de 24 horas por dia. Você pode definir no máximo 3 períodos de tempo para cada fuso horário. A relação entre esses períodos de tempo é "ou". Quando o tempo de verificação está em qualquer um desses períodos de tempo, a verificação é válida. O formato de cada período de tempo do fuso horário é: HH MM-HH MM, com precisão em minutos de acordo com o relógio de 24 horas.

Clique em **Configuração de Regra de Tempo** na interface de Controle de Acesso.

1. Clique na caixa cinza para inserir uma regra de tempo para buscar. Insira o número de regras de tempo (máximo: 50 regras).



2. Clique na data para a qual as configurações do fuso horário são necessárias. Insira a hora de início e de término e, em seguida, pressione OK.



Observações:

1. Quando a hora de término é anterior à hora de início, como 23:57~23:56, indica que o acesso é proibido durante todo o dia. Quando a hora de término é posterior à hora de início, como 00:00~23:59, o intervalo é válido.

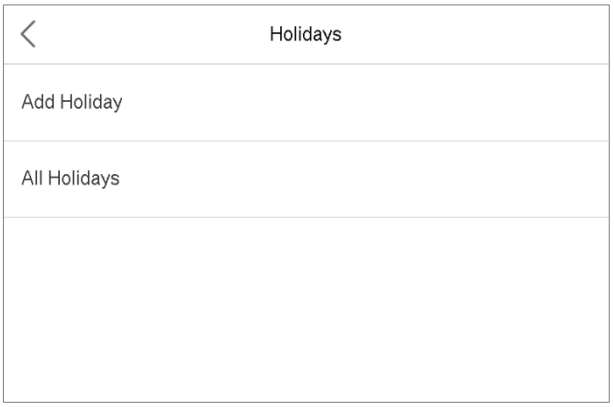
2. O período de tempo efetivo para desbloquear a porta: aberto o dia todo (00:00~23:59) ou sempre que a hora de término for posterior à hora de início, como 08:00~23:59.

3. A regra de tempo padrão 1 indica que a porta está aberta o dia inteiro.

9.3 Configurações de Feriado

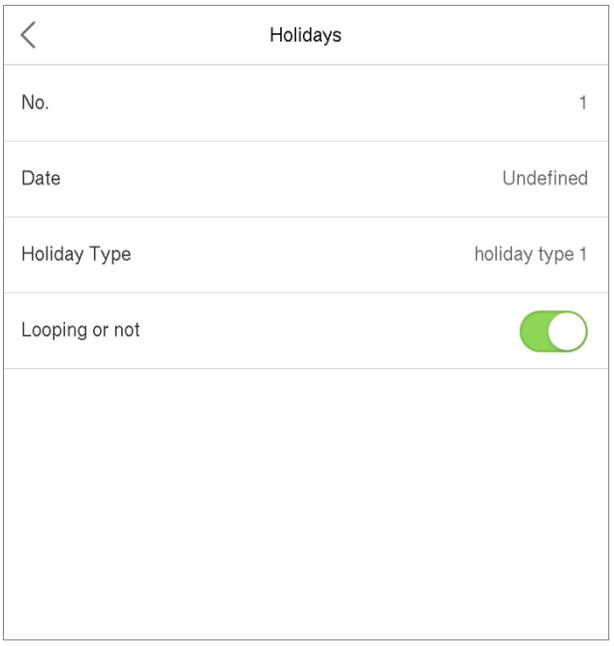
Sempre que houver um feriado, você pode precisar de um horário de acesso especial. No entanto, alterar o horário de acesso de cada pessoa individualmente é extremamente trabalhoso. Portanto, você pode configurar um horário de acesso para feriados que seja aplicável a todos os funcionários, e os usuários poderão abrir a porta durante os feriados.

Clique em **Feriados** na interface de Controle de Acesso.



- **Adicionar um Novo Feriado**

Clique em Adicionar Feriado na interface de Feriados e configure os parâmetros do feriado.



- **Editar um Feriado**

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

- **Excluir um Feriado**

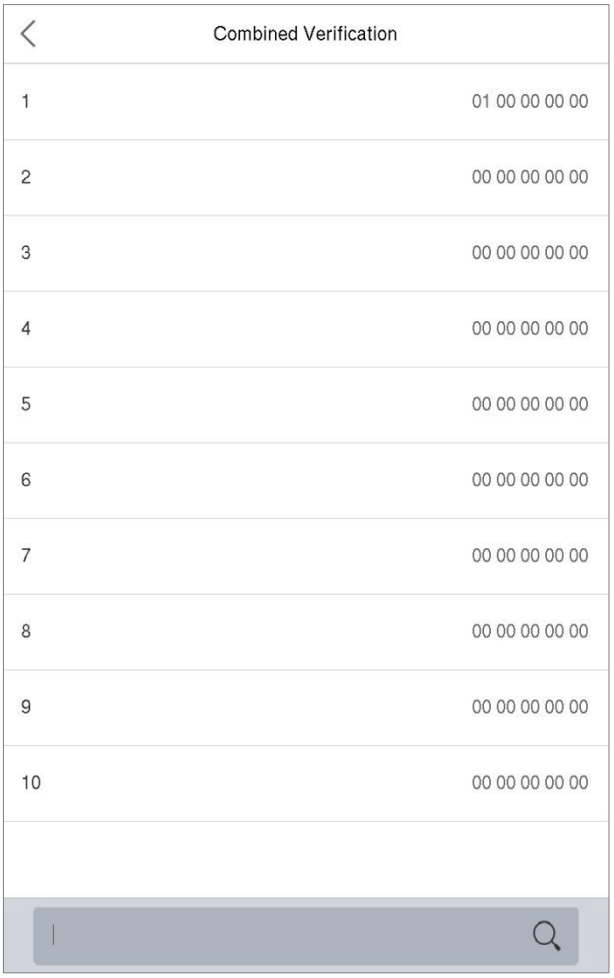
Na interface de Feriados, selecione um item de feriado a ser excluído e clique em **Excluir**. Clique em **OK** para confirmar a exclusão. Após a exclusão, este feriado não será mais exibido na interface de Todos os Feriados.

9.4 Configurações de Verificação Combinada

Grupos de controle de acesso são organizados em diferentes combinações de desbloqueio de portas para realizar várias verificações e fortalecer a segurança.

Em uma combinação de desbloqueio de portas, o número da combinação varia de 0 a 5, e os membros da combinação podem pertencer a um único grupo de controle de acesso ou a até cinco grupos de controle de acesso diferentes.

Clique em **Verificação Combinada** na interface de Controle de Acesso.



Clique na combinação de desbloqueio de portas a ser configurada. Clique nas setas para cima e para baixo para inserir o número da combinação e, em seguida, pressione OK.

Exemplos:

A combinação de desbloqueio de portas 1 é definida como (01 03 05 06 08), o que indica que a combinação de desbloqueio 1 consiste em 5 pessoas, e as 5 pessoas pertencem a 5 grupos diferentes de controle de acesso, a saber, Grupo de Controle de Acesso 1, Grupo de Controle de Acesso 3, Grupo de Controle de Acesso 5, Grupo de Controle de Acesso 6 e Grupo de Controle de Acesso 8, respectivamente.

A combinação de desbloqueio de portas 2 é configurada como (02 02 04 04 07), o que indica que a combinação de desbloqueio 2 consiste em 5 pessoas; as duas primeiras pertencem ao Grupo de Controle de Acesso 2, as duas seguintes pertencem ao Grupo de Controle de Acesso 4 e a última pessoa pertence ao Grupo de Controle de Acesso 7.

A combinação de desbloqueio de portas 3 é definida como (09 09 09 09 09), o que indica que há 5 pessoas nessa combinação; todas elas pertencem ao Grupo de Controle de Acesso 9.

A combinação de desbloqueio de portas 4 é configurada como (03 05 08 00 00), o que indica que a combinação de desbloqueio 4 consiste em três pessoas. A primeira pessoa pertence ao Grupo de Controle de Acesso 3, a segunda pessoa pertence ao Grupo de Controle de Acesso 5 e a terceira pessoa pertence ao Grupo de Controle de Acesso 8.

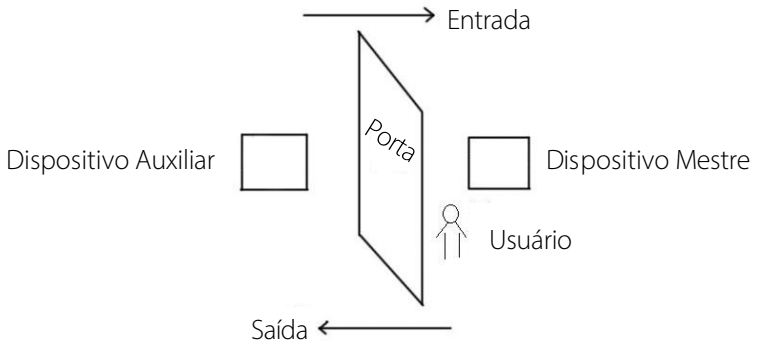
Excluir uma combinação de desbloqueio de portas

Defina todos os números de grupo como 0 se desejar excluir combinações de desbloqueio de portas.

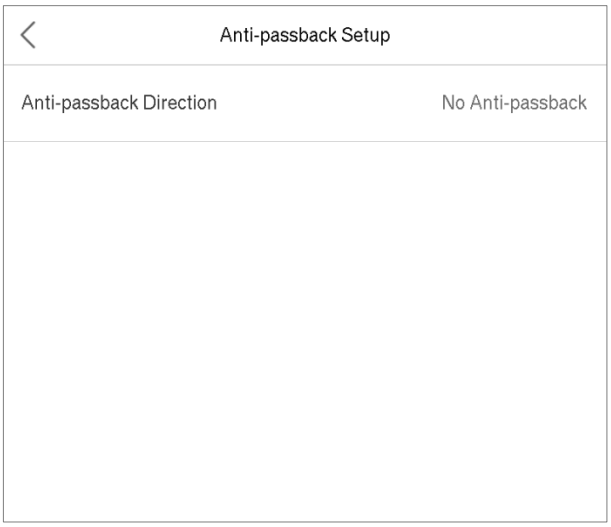
9.5 Configuração Anti-passback

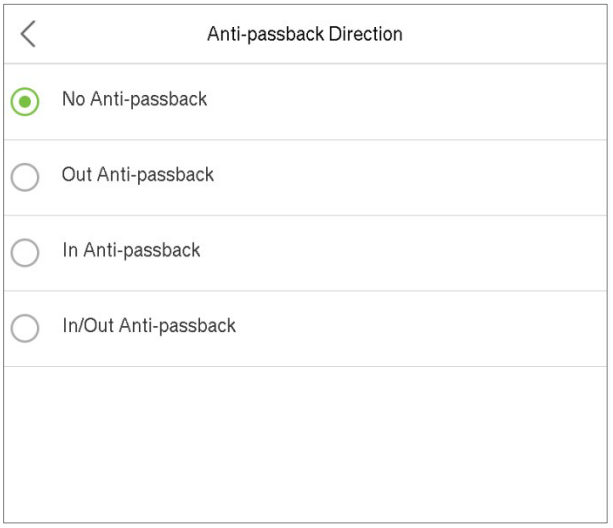
Para evitar que algumas pessoas sigam os usuários e entrem na porta sem verificação, o que resulta em problemas de segurança, os usuários podem ativar a função anti-retorno. O registro de entrada deve corresponder ao registro de saída para abrir a porta.

Essa função requer que dois dispositivos trabalhem juntos: um é instalado dentro da porta (dispositivo mestre) e o outro é instalado fora da porta (dispositivo auxiliar). Os dois dispositivos se comunicam por meio do sinal Wiegand. O formato Wiegand e o tipo de saída (ID do usuário / Número de crachá) adotados pelo dispositivo mestre e pelo dispositivo escravo devem ser consistentes.



Clique em **Configuração Anti-passback** na interface de Controle de Acesso.



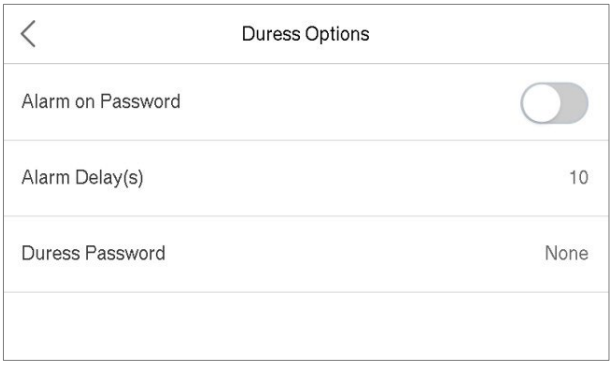


Item	Descrição
Sem Anti-passback	A função Anti-passback está desativada, o que significa que passar pela autenticação no dispositivo mestre ou no dispositivo auxiliar pode desbloquear a porta. O estado de presença não é reservado.
Anti-passback na Saída	Após um usuário efetuar o registro de saída, somente se o último registro for um registro de entrada, o usuário pode fazer o registro de saída novamente; caso contrário, o alarme será acionado. No entanto, o usuário pode fazer o registro de entrada livremente.
Anti-passback na Entrada	Após um usuário efetuar o registro de entrada, somente se o último registro for um registro de saída, o usuário pode fazer o registro de entrada novamente; caso contrário, o alarme será acionado. No entanto, o usuário pode fazer o registro de saída livremente.
Anti-passback na Entrada e na Saída	Após um usuário efetuar o registro de entrada/saída, somente se o último registro for um registro de saída, o usuário pode fazer o registro de entrada novamente, ou se for um registro de entrada, o usuário pode fazer o registro de saída novamente; caso contrário, o alarme será acionado.

9. 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.

Clique em **Opções de Coação** na interface de Controle de Acesso.

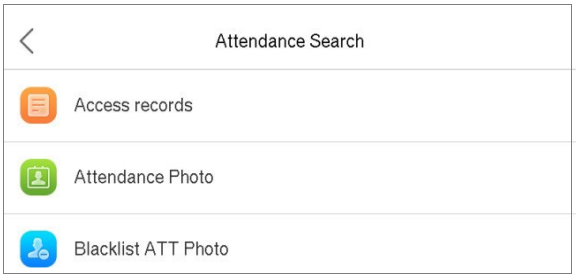


Item	Descrição
Alarme na Senha	Quando um usuário utiliza o método de verificação de senha, um sinal de alarme será gerado; caso contrário, não haverá sinal de alarme.
Atraso do Alarme (s)	O sinal de alarme não será transmitido até que o tempo de atraso do alarme tenha passado. O valor varia de 1 a 999 segundos.
Buscar Registros	Quando a identidade de um usuário é verificada, o registro é salvo no dispositivo. Essa função permite aos usuários verificar seus registros de acesso.

10 Procurar registros

O processo de busca por registros de presença e fotos de lista de bloqueios é semelhante ao da busca por registros de acesso. O seguinte é um exemplo de busca por registros de acesso.

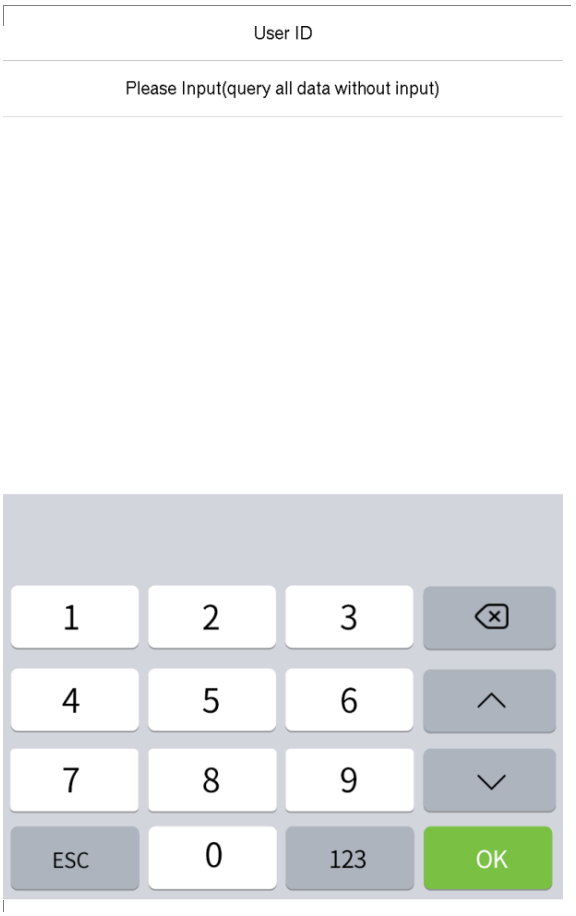
Clique em **Procurar Registros** na interface do **Menu Principal** para pesquisar o registro de Acesso/Presença necessário.



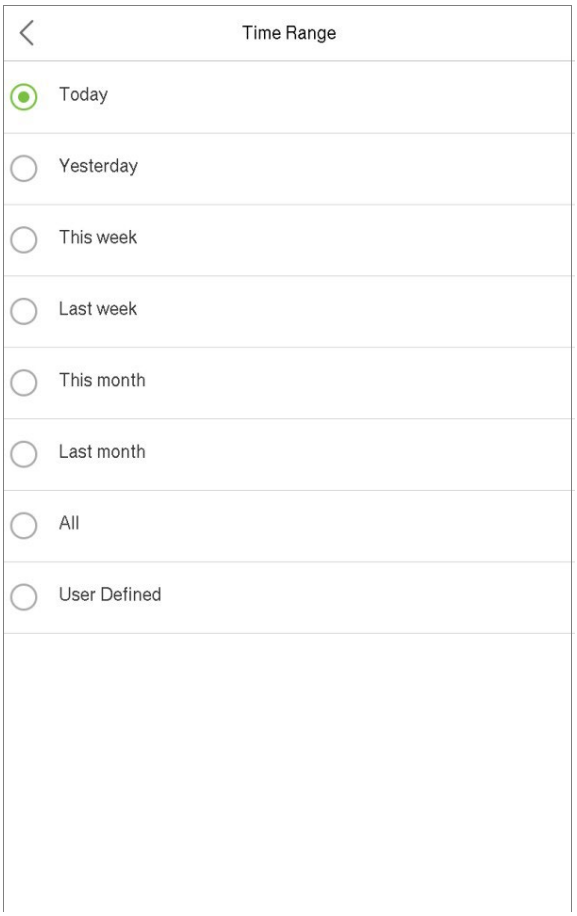
O processo de busca por registros de acesso e fotos de lista de bloqueios é semelhante ao da busca por registros de acesso. O seguinte é um exemplo de busca por registros de acesso.

Na interface de Buscar Presenças, clique em **Registros de Acesso**.

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

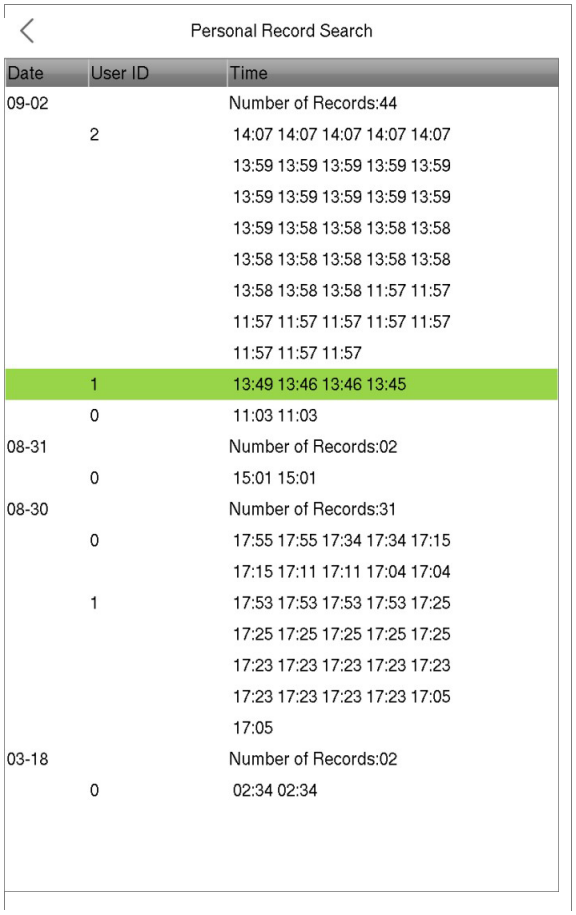


2. Selecione o intervalo de tempo no qual deseja pesquisar os registros.

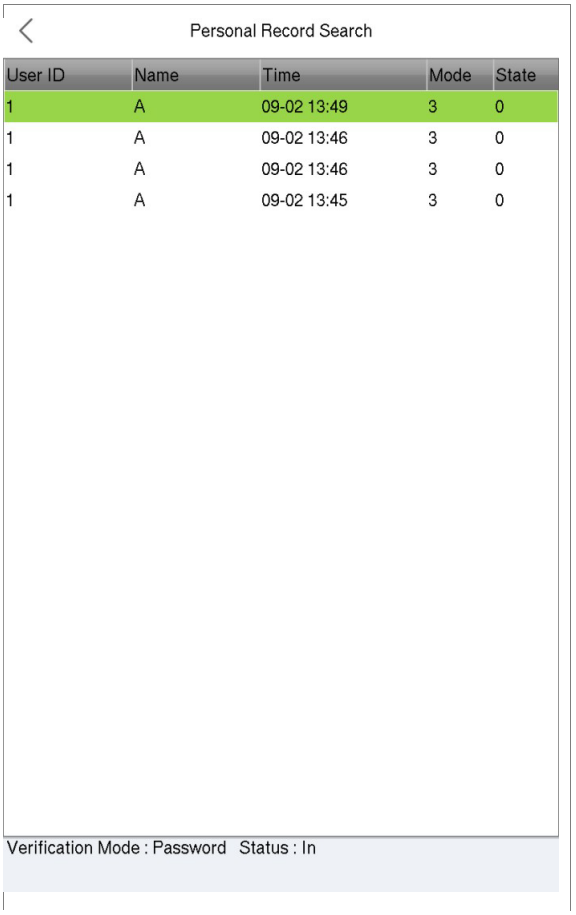


3. A pesquisa de registros é bem-sucedida.

Clique no registro em verde para ver seus detalhes.



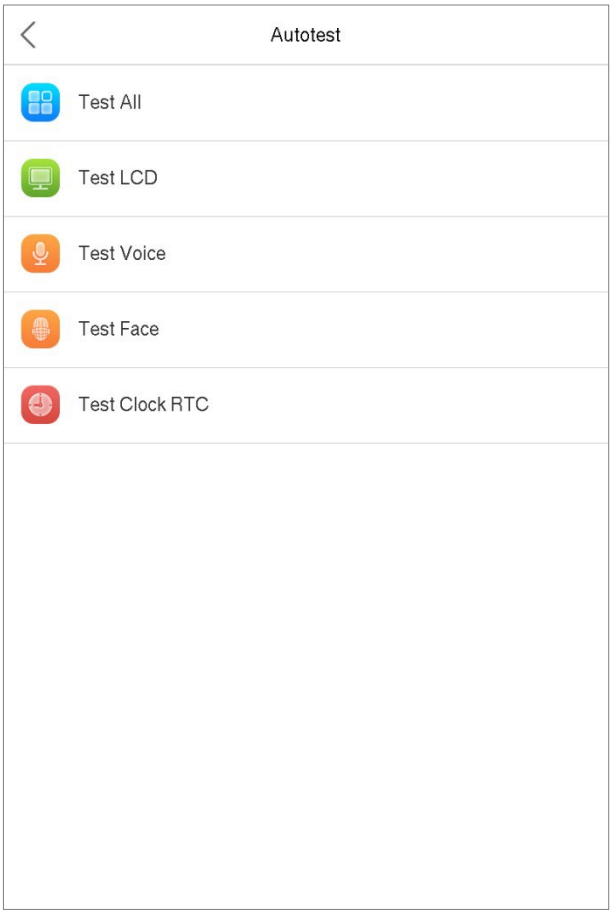
4. A figura abaixo mostra os detalhes do registro selecionado.



11 Auto teste

Para testar automaticamente se todos os módulos no dispositivo funcionam corretamente, o que inclui o LCD, áudio, câmera e relógio em tempo real (RTC).

Clique em **Auto teste** no menu principal.

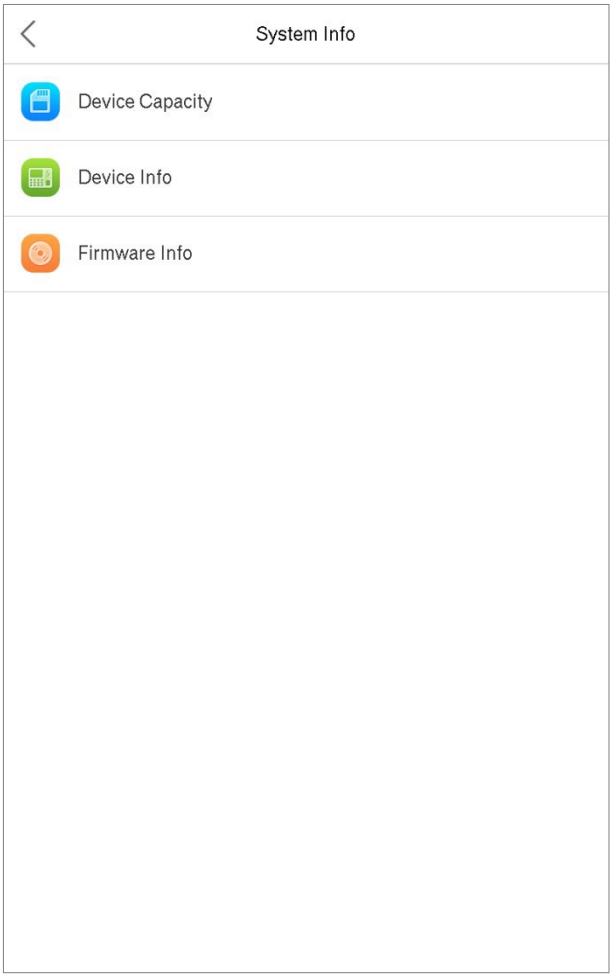


Item	Descrição
Testar Todos	Para testar automaticamente se o LCD, áudio, câmera e RTC estão normais.
Testar LCD	Para testar automaticamente o efeito de exibição da tela LCD, exibindo cores completas, branco puro e preto puro para verificar se a tela exibe cores normalmente.
Testar Voz	Para testar automaticamente se os arquivos de áudio armazenados no dispositivo estão completos e a qualidade do som é boa.
Testar Face	Para testar se a câmera funciona corretamente, verificando se as fotos tiradas estão suficientemente claras.
Testar Relógio RTC	Para testar o RTC. O dispositivo testa se o relógio funciona normalmente e com precisão usando um cronômetro. Toque na tela para iniciar a contagem e toque novamente para parar a contagem.

12 Informações do Sistema

Aqui você pode visualizar o status de armazenamento, as informações de versão do dispositivo, e assim por diante.

Clique em **Informações do Sistema** no menu principal.



Item	Descrição
Capacidade do Dispositivo	Exibe o armazenamento atual de usuários do dispositivo, armazenamento de senhas e reconhecimento facial, administradores, registros de acesso, fotos de presenças e fotos de lista de bloqueios, e fotos de usuários.
Informações do Dispositivo	Exibe o nome do dispositivo, número de série, endereço MAC, versão do algoritmo facial, informações da plataforma e fabricante.
Informações de Firmware	Exibe a versão do firmware e outras informações de versão do dispositivo.

13 Conexão com o Software ZKBioSecurity

13.1 Configurar o Endereço de Comunicação

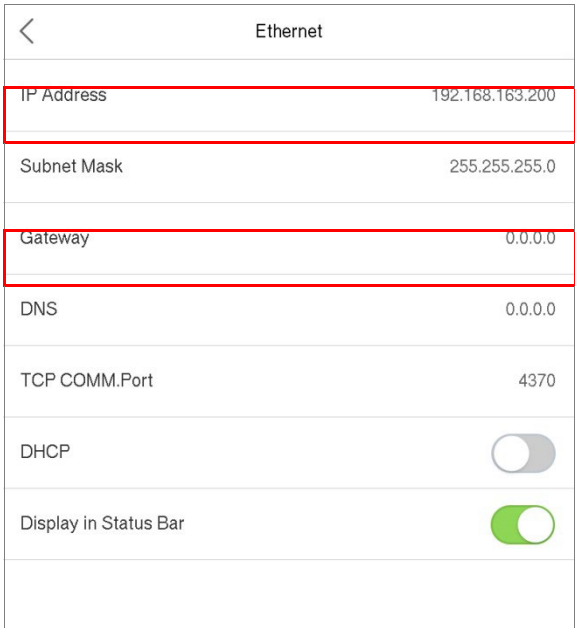
➢ **Device**

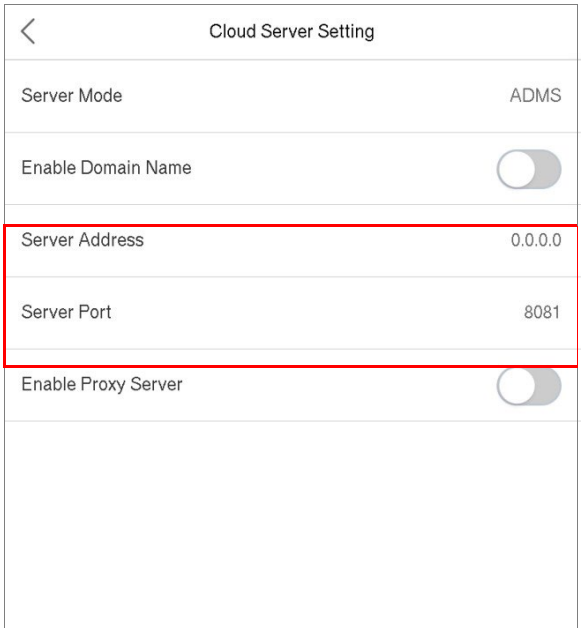
1. Clique em **Config. Com.** > **TCP/IP** no menu principal para configurar o endereço IP e gateway do dispositivo. (**Observação:** O endereço IP deve ser capaz de se comunicar com o servidor ZKBioSecurity, preferencialmente na mesma segmentação de rede do endereço do servidor.)

2. No menu principal, clique em **Config. Com.** > **Configuração do Servidor na Nuvem** para definir o endereço do servidor e a porta do servidor.

Endereço do servidor: Configure o endereço IP do servidor ZKBioSecurity.

Porta do servidor: Configure a porta de serviço do ZKBioSecurity (o padrão é 8088).





➢ **Software**

Faça login no software ZKBioSecurity, clique em **Sistema > Comunicação > Dispositivo de Comunicação** para configurar a porta de serviço adms, conforme mostrado abaixo:

13.2 Adicionar um Dispositivo no Software

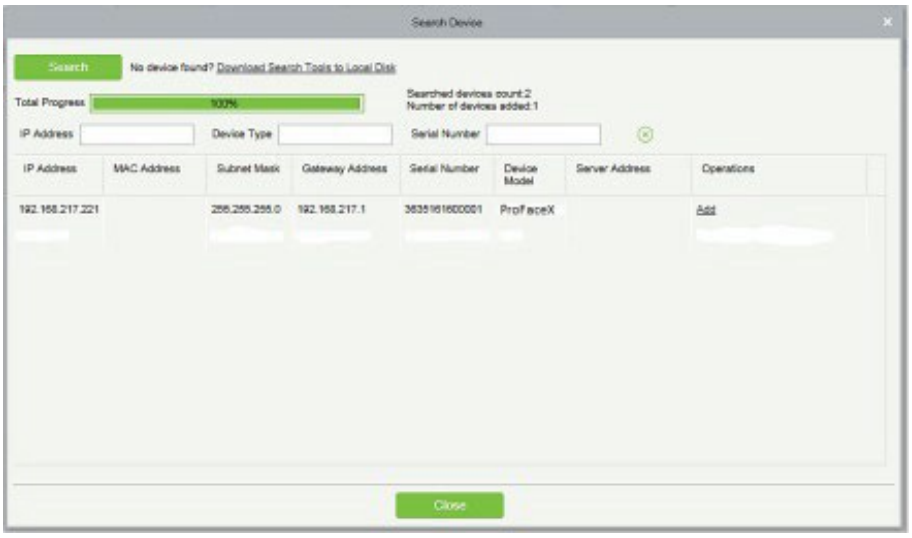
Adicione dispositivos por meio de uma pesquisa. O processo é o seguinte:

1. Clique em **Controle de Acesso** > **Dispositivo** > **Pesquisar Dispositivo**, para abrir a interface de Pesquisa

2. Clique em **Pesquisar**, e o sistema mostrará [Pesquisando...].

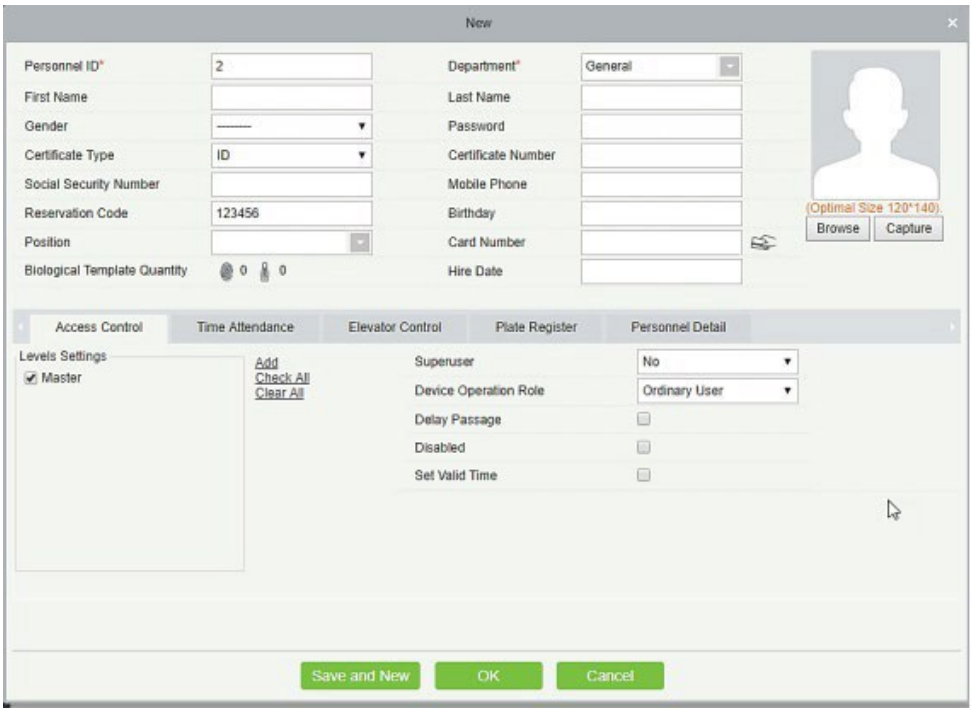
3. Após a pesquisa, a lista e o número total de controladores de acesso serão exibidos.

4. Selecione o dispositivo e clique em **Adicionar.**



13.3 Adicionar Pessoal no Software

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



2. Após configurar todos os parâmetros, clique em **OK**.

Observação: *Para outras operações específicas, consulte o Manual do Usuário do ZKBioSecurity.*

Declaração sobre o Direito à Privacidade

Prezados Clientes:

Agradecemos por escolher este produto híbrido de reconhecimento biométrico, que foi projetado e fabricado pela ZKTeco. Como um fornecedor mundialmente reconhecido de tecnologias de reconhecimento biométrico, estamos constantemente desenvolvendo e pesquisando novos produtos e nos esforçamos para seguir as leis de privacidade de cada país onde nossos produtos são vendidos.

Declaramos o seguinte:

1. Todos os nossos dispositivos civis de reconhecimento de impressões digitais capturam apenas características, não imagens de impressões digitais, e não envolvem proteção de privacidade.
2. Nenhuma das características de impressões digitais que capturamos pode ser usada para reconstruir uma imagem da impressão digital original e não envolvem proteção de privacidade.
3. Como fornecedor deste dispositivo, não assumiremos responsabilidade direta ou indireta por quaisquer consequências que possam resultar do uso deste dispositivo.
4. Se você desejar contestar questões de direitos humanos ou privacidade relacionadas ao uso de nosso produto, entre em contato diretamente com seu revendedor.

Nossos outros dispositivos de impressões digitais para aplicação na área de segurança pública ou ferramentas de desenvolvimento podem capturar imagens originais das impressões digitais dos cidadãos. Quanto a se isso constitui uma violação de seus direitos, entre em contato com o Governo ou o fornecedor final do dispositivo. Como fabricante do dispositivo, não assumiremos responsabilidade legal.

Observação:

A lei chinesa inclui as seguintes disposições sobre a liberdade pessoal de seus cidadãos:

1. Não deve haver prisão ilegal, detenção, busca ou violação de pessoas;
2. A dignidade pessoal está relacionada à liberdade pessoal e não deve ser infringida;
3. A casa de um cidadão não pode ser violada;
4. O direito de comunicação de um cidadão e a confidencialidade dessa comunicação são protegidos por lei

Por fim, gostaríamos de enfatizar que o reconhecimento biométrico é uma tecnologia avançada que certamente será usada no comércio eletrônico, bancos, seguros, judiciário e em outros setores no futuro. Todos os anos, o mundo sofre grandes perdas devido à natureza insegura das senhas. Os produtos biométricos servem para proteger sua identidade em ambientes de alta segurança.

Operação Ecologicamente Correta

O "período de operação ecologicamente correto" do produto refere-se ao tempo durante o qual este produto não liberará nenhuma substância tóxica ou perigosa quando usado de acordo com os pré-requisitos deste manual. O período de operação ecologicamente correto especificado para este produto não inclui baterias ou outros componentes que se desgastam facilmente e devem ser substituídos periodicamente. O período operacional ecologicamente correto da bateria é de 5 anos.

Substâncias tóxicas ou perigosas e suas quantidades

Nome do Componente	Substância/Elemento Perigoso/Tóxico					
	Chumbo (Pb)	Mercúrio (Hg)	Cádmio (Cd)	Crómio hexavalente (Cr6+)	Bifenilas Polibromadas (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.

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

Garantia

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

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

Resultará nula e sem efeito esta garantia em caso de:

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

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

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

Telefone: (31) 3055-3530

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

www.zkteco.com.br