



Manual de Referência de Instalação

Índice

1.	Apresentação	6
1.1	Aparências do dispositivo	7
1.1.1	Vista Frontal	7
1.1.2	Vista Lateral	7
1.2	Interface Principal	8
1.3	Modos de Verificação	9
1.3.1	Verificação da Impressão	9
1.3.2	Verificação de Face	11
1.3.3	Verificação de Senha	13
1.3.4	Verificação do Cartão de Identificação	14
1.3.5	Combinação para Verificação	15
2.	Menu Principal	17
2.1	Adicionar Usuário	19
2.2	Digitando ID do Usuário	19
2.3	Digitando um Nome	20
2.4	Registrando uma Impressão Digital	21
2.5	Registrando uma Senha	22
2.6	Registrando um Cartão de Identificação	22

2.7	Registrando uma Face	23
2.8	Digitando No. de Grupo	24
2.9	Modificando os Direitos de Usuário	24
2.10	Registrar Foto.....	25
2.11	Configurações de Acesso do Usuário.....	26
2.11.1	Verificar Tipo (verTipo)	26
2.11.2	Período.....	27
2.11.3	Estresse da impressão digital.....	27
3.	Gerenciamento de Usuários	28
3.1	Editar um Usuário	29
3.2	Deletar um Usuário.....	29
3.3	Pesquisar um Usuário	30
4.	Configurações de Comunicação.....	30
4.1	Configurações de Conexão	31
5.	Configurações do Sistema.....	32
5.1	Parâmetros Gerais	32
5.2	Display.....	33
5.3	Parâmetros da Impressão Digital.....	33
5.4	Parâmetros da Face	34
5.5	Presença.....	35

5.6	Definições de Atalho.....	36
5.7	Opções de Acesso	38
5.7.1	Opções de Hora.....	38
5.7.2	Opções de férias	39
5.7.3	Configuração da Zona de Tempo do Grupo.....	40
5.7.4	Configuração da Combinação de Destravamento	42
5.7.5	Parâmetro de controle de acesso	43
5.7.6	Parâmetros do Alarme de Coação	44
5.7.7	Configuração de Anti-passagem de retorno.....	45
5.8	Atualização.....	46
6.	Configuração Data/Hora	46
6.1	Configurar Data/Hora	46
6.2	Configuração da Campainha	47
6.3	Horário de Verão (DLST)	49
7.	AutoTeste.....	50
8.	Gerenciamento do USB.....	52
8.1	USB.....	53
9.	Informações do Sistema	54
10.	Apêndice	54
10.1	Apêndice 1 Introdução a Wiegand	54

10.2	Sinais digitais.....	55
10.3	Apêndice 2 Função ID de Foto	56
10.4	Apêndice 3 Modo de Autenticação de Multi-combinação	57
10.5	Apêndice 4 Anti-Passagem de Retorno	60

Apresentação

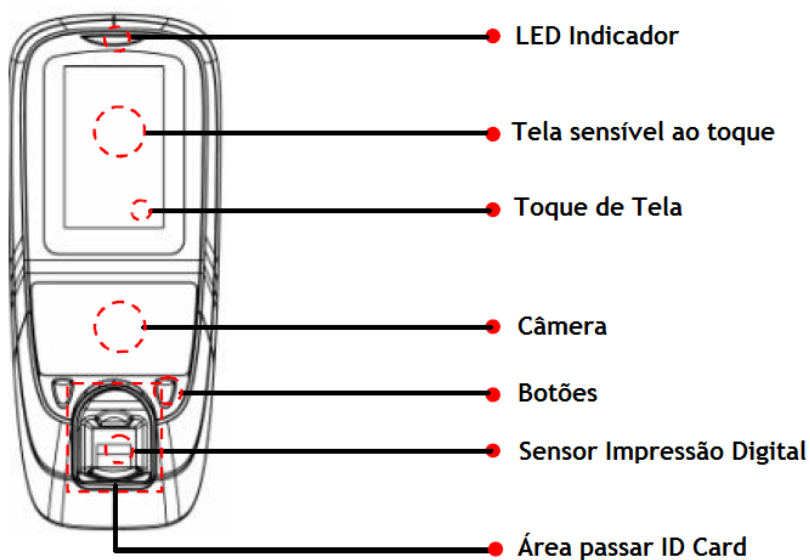
O **MULTIBIO 700** da CS é um avançado equipamento de múltipla identificação biométrica, integrando os padrões faciais, impressões digitais, senhas e RFID. O algoritmo de identificação facial capta a posição relativa, tamanho e formato dos olhos do usuário, nariz, maçãs do rosto e características da mandíbula. Dessa forma gerando precisão e confiabilidade nas leituras. Podem ser criadas diversas combinações para liberação do acesso. O **MULTIBIO 700** pode armazenar 500 faces, 2.000 impressões digitais, 10.000 cartões RFID e 100.000 logs.



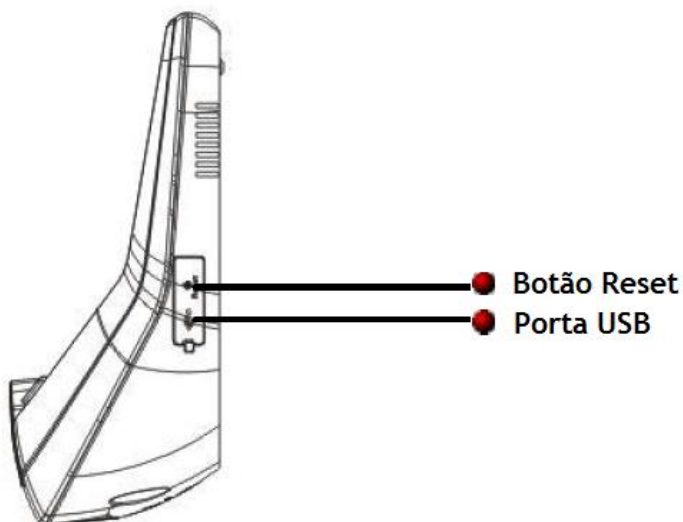
Instruções de Uso

1.1 Aparências do dispositivo

1.1.1 Vista Frontal



1.1.2 Vista Lateral



1.2 Interface Principal



① **Data:** A data atual é exibida.

② **Teclas de Atalho da Tela:** Pressione as teclas de atalho para exibir o status de frequência. Os usuários podem personalizar a função de cada tecla de atalho.

③ **Hora:** A hora atual é exibida. Pode-se ajustar para sistema 12 ou 24 horas.

④ **Status de Frequência:** O status atual de presença é exibido.

⑤ **1:1 Tecla Interruptor:** Ao pressionar esta tecla, você pode mudar para os modos de verificação 1:1, e entrar na interface de entrada digital.

⑥ **Menu:** Você pode entrar no menu principal pressionando esta tecla.

Nota:

1. Registro de Impressão Digital, Acesso do Usuário, Botão Campainha da Porta e 1:1 Botão Interruptor são funções opcionais.

1.3 Modos de Verificação

1.3.1 Verificação da Impressão *

1) Verificação de Impressão Digital 1:N

O terminal compara a impressão digital coletada atualmente pelo leitor de impressão digital com todos os dados de impressão digital que o terminal possui.

(1) Para entrar no modo verificação de impressão digital. O dispositivo automaticamente distingue a face e faz a verificação da impressão digital, apenas pressionando o dedo no coletor. Para verificação deve-se estar no modo de autenticação de impressão digital.

(2) Pressionar o dedo no sensor de impressão digital posicionando o dedo de forma adequada.

(3) Se a verificação for bem-sucedida, o dispositivo indicará “Verified” (Verificado).

(4) Se a verificação não for bem-sucedida, o dispositivo indicará “Please try again” (Favor, tentar novamente).



2) Verificação de impressão digital 1:1

No modo de verificação 1:1 de impressão digital, o dispositivo compara a impressão digital atual coletada pelo sensor de impressão digital em relação à ID de usuário digitada através do teclado. Adotar este modo apenas quando for difícil reconhecer a impressão digital.

(1) Pressione [1:1] no botão da tela para entrar no modo verificação de impressão digital 1:1.

(2) Digitar ID do Usuário ou No. de Grupo, depois pressione o ícone “Impressão digital” para entrar no modo reconhecimento de impressão digital 1:1. Se a mensagem “Unregistered user!” (Usuário não registrado) for exibida, a ID do Usuário não existe.

(3) Pressionar o dedo no sensor de impressão adotando a colocação de dedo apropriada.

(4) Se a verificação for bem-sucedida, o dispositivo indicará “Verified”, (Verificado). Caso contrário, o dispositivo indicará “Please try again” (Favor, tentar novamente).



1.3.2 Verificação de Face

1) Verificação de Face 1:N

O terminal compara a imagem atual da face coletada pela câmera com todos os dados de face que o terminal possui.

(1) O dispositivo automaticamente distingue a face e a verificação de impressão digital.

(2) Comparar a face de uma maneira adequada. A tela de comparação exibe a imagem atual coletada pela câmera. Uma tela como é exibida na Figura (a) abaixo será apresentada.

(3) Se a verificação for bem-sucedida, uma tela como mostra a Figura (b) será exibida.



Figura (a)



Figura (b)

2) Verificação de face 1:1

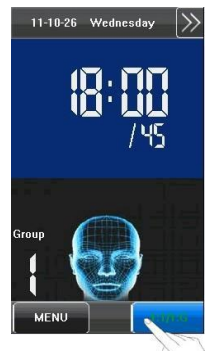
No modo de verificação de face 1:1, o dispositivo compara a face atual coletada pelo sensor de reconhecimento facial em relação à ID de usuário digitada através do teclado. Adote este modo apenas quando houver dificuldade em reconhecer a face.

(1) Pressione o botão [1:1] na tela para entrar no modo de reconhecimento de face.

(2) Digitar ID do Usuário, posteriormente pressione o ícone "1:1 Face" para entrar no modo de reconhecimento de face 1:1. Se a mensagem "Unregistered user!" (Usuário não registrado) for exibida, a ID do Usuário não existe.

(3) Comparar a face de uma maneira adequada.

(4) Se a verificação for bem-sucedida, o dispositivo indicará "Verified" (Verificado). O sistema retornará à tela principal se a verificação não for realizada dentro de 20 segundos.



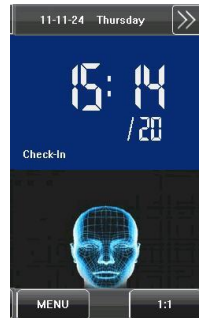


3) Verificação de Face 1:G

Quando você abre a Função de Verificação 1:G, depois você pode realizar a Verificação de Face 1:G.

No. de grupo atual (Número de grupo válido é 1-5) é exibido na tela de reconhecimento de face. Os usuários do grupo atual podem

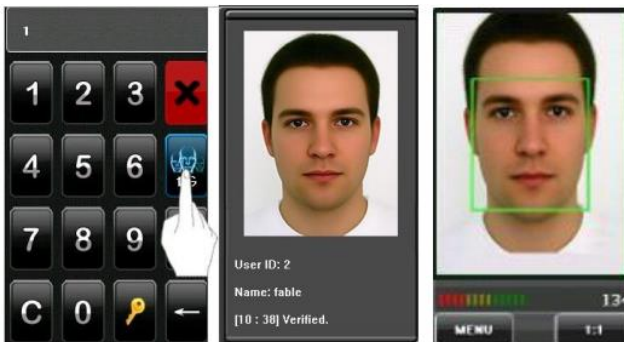
executar a comparação facial diretamente. Os usuários de outro grupo podem executar comparação de face somente após digitar o No. de grupo ou selecionando usando a tecla de atalho. O sistema definirá o grupo digitado ou selecionado por usuários para ser o grupo atual instantaneamente.



(1) Pressione [1:1/1:G] na tela para entrar no modo de reconhecimento de 1:G.

(2) Digite o N. de Grupo de usuário e depois pressione o ícone “1:G”: (exibido na figura 1) para entrar no modo de reconhecimento facial 1:G.

(3) Comparar a face de maneira adequada. O No. De Grupo atual é exibido na interface de comparação, como mostrado nas figuras a seguir.



Nota: Verifique se você está no grupo atual. Se não, retorne ao Passo 1.

(4) Se a verificação for bem-sucedida, ocorrerá como ilustrado na figura seguinte.

Nota: O grupo de face G 1 é uma função opcional. Algumas máquinas possuem esta função, porém outras não. A função de grupo de face não é modificada, procede com padrão de fábrica. Os usuários podem configurar em → System -- Log Settings -- 1: Verificar G para abrir esta função.

1.3.3 Verificação de Senha

No modo de verificação de senha, o dispositivo compara a senha digitada com aquela em relação à ID do usuário.

1. Pressionar [1:1] na tela ou botão [1:1] para entrar no modo de verificação de senha.

2. Digitar ID de usuário, e depois pressionar o ícone “chave” para entrar no modo verificação de senha. Se a mensagem “*Não registrado*” for exibida, a ID do Usuário não existe.

3. Digitar a senha e pressionar o ícone “OK” para começar a comparação da senha.

4. Se a verificação for bem-sucedida, o dispositivo indicará “*Verificado*”, caso contrário o dispositivo indicará “*Verify fail*” (Falha de verificação) e retornará à interface de entrada de senha.



1.3.4 Verificação do Cartão de Identificação*

Apenas os produtos com um módulo de cartão de identificação integrado suporta a verificação do cartão de identificação. Os produtos com um módulo de cartão de identificação integrado suportam os seguintes dois modos de verificação:



- Somente Cartão de Identificação: Os usuários apenas precisam passar seus cartões de identificação para verificação.
- ID + Verificação Facial: Depois de passar na verificação de cartão de identificação, você também deve executar a verificação de face.
 1. Somente Cartão de Identificação
 - 1) Deslize seu cartão de identificação na área de deslize do cartão, de maneira adequada.
 - 2) Se a verificação for bem-sucedida, o dispositivo indicará “Verified” (Verificado).
 - 3) Se a verificação não for bem sucedida, o dispositivo indicará “Not Enrolled” (Não registrado).

Nota:

- (1) As máquinas que possuem a função de interface com identificação com foto, aparece verificação bem sucedida conforme a figura 1 acima.
- (2) As máquinas que não possuem a função de identificação com foto, a verificação é exibida conforme a figura 2 acima.

2. ID + Verificação de Face

(1) Passar seu cartão de identificação adequadamente na área de deslize para digitar o modo de verificação de face 1:1.

(2) Comparar a face de uma maneira adequada.

(3) Se a verificação for bem-sucedida, uma interface mostrada como na figura abaixo será exibida. O sistema retornará à interface principal se a verificação não for efetuada dentro de 20 segundos.



1.3.5 Combinação para Verificação

O dispositivo suporta até 20 modos de verificação, incluindo FACE&PIN/FP/RF/PW, F P&PW, F P&RF, F ACE&FP, F ACE&PW, F ACE&RF, FP, PW, RF, FACE&PIN, FP/RF, PW/RF, FP/PW, PW&RF, PIN&FP, FP&PW&RF, PIN&FP&PW, FP&RF/PIN, FACE&FP&RF, FACE&FP&PW etc.

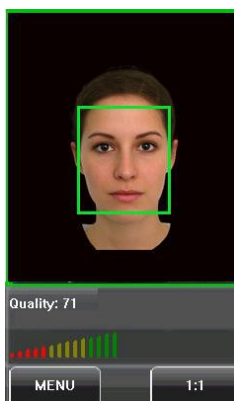
Nota: RF significa verificação de identificação do cartão. Apenas os produtos construídos no módulo de identificação do cartão suportam a verificação do cartão de identificação.



Aqui está a operação de verificação de combinação; usaremos a verificação FACE&FP como exemplo.

Se você verificar a impressão digital primeiro e depois a face, o usuário deverá seguir as seguintes operações:

1. A interface principal é a tela do modo de verificação de impressão digital, ver a figura abaixo.
2. Pressionar o dedo no sensor de impressão digital adotando a colocação de dedo apropriada.
3. Se a verificação for bem-sucedida, o dispositivo entrará no modo de reconhecimento de face 1:1. Comparar a face de uma maneira adequada.
4. Se a verificação for bem-sucedida, o dispositivo indicará *“Verified”* (Verificado). O sistema retornará à interface principal se a verificação não for efetuada dentro de 20 segundos.



Caso contrário, a verificação da combinação FACE&FP pode executar tal como FACE (1: N) + FP, PIN + FACE (1:1) + FP, PIN + FP (1:1) + FACE etc. A operação é semelhante ao procedimento apresentado antes.

2.Menu Principal

Há dois tipos de direitos respectivamente concedidos a dois tipos de usuários: os usuários comuns e os administradores. Os usuários comuns só recebem os direitos de face, impressão digital, senha ou verificação de cartão, enquanto os administradores recebem acesso ao menu principal para várias operações à parte de ter todos os privilégios concedidos aos usuários comuns.

Pressione [**Menu**] na interface inicial para acessar o menu principal, como é ilustrado na figura seguinte:



O menu principal inclui nove submenus:

Add User (Adi Usu): Por este submenu, você pode adicionar um novo usuário e digitar as informações no dispositivo, inclusive a ID do usuário, nome, impressão digital, face, cartão, senha, direitos, No. de grupo e acesso de usuário.

User Mgt. (Ger.Usuar): Através deste submenu, você pode procurar as informações do usuário armazenadas no dispositivo, incluindo o ID de usuário, nome, impressão digital, face, cartão, senha, direitos, No. grupo e acesso do usuário. Aqui você também pode adicionar, alterar ou apagar as informações de um usuário.

COMM. (Conexão): Por este submenu, você pode configurar os parâmetros relacionados para comunicação entre o dispositivo e o PC, inclusive o endereço de IP, entrada, máscara de subnet, taxa de transmissão, No. de dispositivo e senha de comunicação.

System (Sistema): Por este submenu, você pode configurar os parâmetros relacionados ao sistema, inclusive os parâmetros básicos, parâmetros de interface, impressão digital, face e parâmetros de frequência, definições de teclado, configurações de acesso, atualização de firmware, etc. para habilitar o dispositivo e atender os requisitos do usuário plenamente em termos de funcionalidade e exibição.

Data Mgt.(Dado): Por este submenu, você pode executar o gerenciamento de dados armazenados no dispositivo. Por exemplo: deletar os registros de frequência, todos os dados, apagando o administrador, restaurando as configurações de fábrica e os registros de pesquisa.

Date/Time (Data/Hora): Por este submenu, você pode configurar a hora e a duração do alarme ou configurar a Campanha.

Auto Test (AutoTeste): Este submenu habilita o sistema automaticamente para testar se as funções de vários módulos são normais, inclusive tela, sensor, voz, face, teclado, testes de relógio e calibração de tela.

Dn/Upload (USB): Por este submenu, você pode baixar informações do usuário e dados de frequência armazenados no dispositivo através de um disco USB para software relacionado ou outro equipamento de reconhecimento de impressão digital.

Sys Info. (InfoSis): Por este submenu, você pode navegar nos registros e informações do dispositivo.

Qualquer usuário pode acessar o menu principal pressionando a tecla [Menu] se o sistema não tiver um administrador. Depois que os administradores estiverem configurados no dispositivo, será necessário uma verificação da identidade dos administradores antes de conceder-lhes acesso ao menu principal. Para assegurar a segurança do dispositivo, é recomendado definir um administrador ao usar o terminal inicialmente. Para operações detalhadas, ver 3.8 Modificando os Direitos do Usuário.

2.1 Adicionar Usuário

Pressionar **[Adi Usu]** do menu principal para exibir a interface **[Add User]**.

User ID (ID do Usuário): Digitar uma ID do usuário. As IDs de usuário com 1 a 9 dígitos são suportadas por padrão.

Nome: Digitar um nome de usuário. Nomes de usuários com 14 caracteres são suportados por padrão.

Fp (Impressão Digital): Registrar a impressão digital de um usuário e o dispositivo exibe o número de impressões digitais registradas. Um usuário pode registrar no máximo 10 (dez) impressões digitais.

Senha: Registrar a senha de um usuário. O dispositivo suporta senhas de 1-8 dígitos por padrão.

Face: Registrar a face de um usuário.

No.de.Grp(No. de grupo): Configurar o grupo de usuários.

Configuração do usuário no grupo.

Função: Definir os direitos de um usuário. Um usuário é definido como usuário comum por padrão e também pode ser definido como administrador.

Os usuários comuns só recebem os direitos de face, impressão digital ou verificação de senha, enquanto os administradores recebem acesso ao menu principal para várias operações à parte de ter todos os privilégios concedidos aos usuários comuns.

Foto: Registrar uma foto de usuário. Se a verificação de usuário for bem-sucedida; a foto do usuário é exibida na tela.

Acesso Usr (Acesso do usuário): Configurar o controle de travamento e os parâmetros de controle de acesso.



2.2 Digitando ID do Usuário

O dispositivo automaticamente aloca uma ID, começando de 1 (um) para cada usuário em sequência. Se você usar a ID alocada pelo dispositivo, você pode pular esta seção.

1. Pressionar **[ID.Nr:]** na interface **[Adi Usu]** para exibir a interface para gerenciamento de ID de usuário.

Dica: A ID de usuário pode ser modificada durante o registro inicial, mas uma vez registrada, não pode ser modificada.

2. Na interface do teclado, digite um ID de usuário e



pressionar **[OK]**. Se a mensagem “No.ID exist!” for exibida, digitar outra ID.

Dica: O dispositivo suporta IDs de usuário de 1-9 dígitos por padrão. Se você precisar ampliar a extensão de números atuais para ID de usuário, favor consultar nossos representantes comerciais ou técnicos de pré-vendas.

3. Depois que a ID de usuário for digitada, pressionar **[Salv]** para salvar as informações atuais e retornar à interface anterior. Pressionar **[Volta]** para retornar à interface anterior sem salvar as informações atuais.



2.3 Digitando um Nome

Usar o método de entrada T9 para digitar o nome de usuário pelo teclado.

1. Pressione **[Nome]** na interface **[Add User]** para exibir a interface para entrada de nome.

2. Na interface de teclado exibida, digite o nome de um usuário e pressione **[Enter]** e depois pressione **[x]**.

3. Depois que o nome de usuário for digitado, pressione **[Salv]** para salvar as informações atuais e retornar à interface anterior. Pressione **[Volta]** para retornar à interface anterior sem salvar as informações atuais.



Dica: O dispositivo suporta nomes de 1 a 12 caracteres por padrão.

2.4 Registrando uma Impressão Digital

1. Pressione **[Fp]** na interface **[Add User]** para exibir a interface **[Cadast. FP(3-0)]**.

2. No display da interface **[Cadast. FP(3-0)]**, posicione seu dedo no sensor de impressão digital adequadamente de acordo com a mensagem do sistema.

3. Coloque o mesmo dedo no sensor de impressão digital por três vezes consecutivas corretamente. Se o registro for bem-sucedido, o sistema exibirá uma mensagem e automaticamente retornará à interface **[Add User]**. Se o registro falhar, o sistema exibirá uma mensagem e retornará à interface **[Cadast. FP(3-0)]**. Neste caso, você deve repetir as operações do passo 2.

4. Você pode registrar a impressão digital de segurança pressionando **[Fp]** outra vez. Um usuário pode registrar 10 impressões digitais no máximo.

5. Pressione **[Save]** para salvar as informações atuais e retornar à tela anterior. Pressione **[Volta]** para retornar à interface anterior sem salvar as informações atuais.



2.5 Registrando uma Senha

1. Pressione [senha] na interface [Add User] para exibir a interface de gerenciamento de senhas.

2. Na interface de teclado, digite uma senha e pressione [OK]. Re-digite a senha de acordo com a mensagem do sistema e em seguida pressione [OK].

Dica: O dispositivo suporta senhas de 1-8 dígitos por padrão.

3. Depois que uma senha for digitada, uma interface é exibida como mostrado abaixo. Pressione [Salv] para salvar as informações atuais e retorne à interface anterior. Pressione [Volta] para retornar à interface anterior sem salvar as informações atuais.



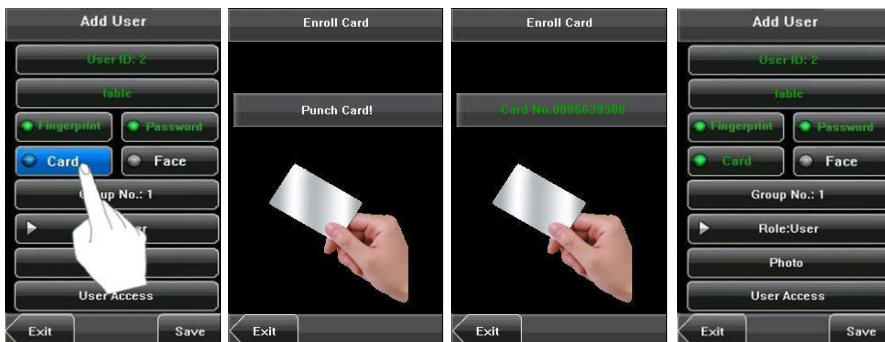
2.6 Registrando um Cartão de Identificação*

1. Pressione [Cartão] na interface [Add User] para exibir a interface [Enroll Card].

2. A interface [Punch Card!] (Cartão de Ponto) aparece como ilustrado na Figura abaixo. Passe seu cartão de identificação adequadamente na área de leitura.

3. Se o cartão passar na verificação, o dispositivo exibirá uma mensagem "Read Successfully! (Leitura Bem-sucedida) No. do Cartão: *****", e retornará à interface [Add User].

4. Pressione [Save] para salvar as informações atuais e retornar à interface anterior. Pressione [Exit] para retornar à interface anterior sem salvar as informações atuais.



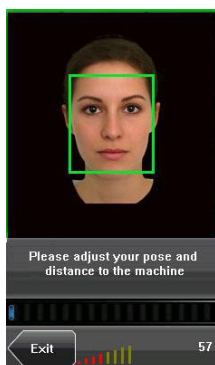
2.7 Registrando uma Face

1. Pressione o botão [Face] na janela [Add User] para exibir a tela de registro de face.

2. Na tela de registro de face, movimente a cabeça um pouco para a esquerda e para a direita, levante e abaixe a cabeça de acordo com as mensagens de voz, de forma a registrar diferentes partes da sua face no sistema para garantir uma verificação precisa.

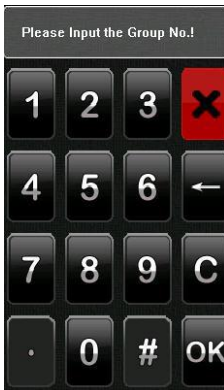
3. Se a imagem da sua face for registrada com êxito, o sistema exibirá uma mensagem e automaticamente retornará à janela [Add User].

4. Pressione [Save] para salvar as informações atuais e retornar à tela anterior. Pressione [Volta] para retornar à interface anterior sem salvar as informações atuais.



2.8 Digitando No. de Grupo

1. Pressione **[No.de Grp:]** na janela **[Add User]** para exibir a interface de gerenciamento do No. de grupo.
2. Na interface de teclado, digitar seu No. de grupo e pressione **[OK]**.
3. Depois que o No. de grupo for digitado, uma interface é exibida como mostrado abaixo. Pressione **[Save]** para salvar as informações atuais e retornar à tela anterior. Pressione **[Volta]** para retornar à tela anterior sem salvar as informações atuais.



2.9 Modificando os Direitos de Usuário

Nota: Há dois tipos de direitos respectivamente concedidos a dois tipos de usuários: usuários comuns e administradores. Os usuários comuns só recebem os direitos de face, impressão digital ou verificação de senha, enquanto os administradores recebem acesso ao menu principal para várias operações à parte de ter todos os privilégios concedidos aos usuários comuns.

1. Na tela **[Add User]**, pressione **[Usuário]** para mudar um usuário para administrador.
2. Depois que a modificação for feita, a interface fica como mostrado abaixo. Pressione **[Save]** para salvar as informações atuais e retornar à interface anterior; pressione **[Volta]** para retornar à interface anterior sem salvar as informações atuais.



2.10 Registrar Foto*

Se você havia registrado sua foto no sistema, o sistema exibirá sua foto registrada, sua ID e nome depois de passar na verificação.

1. Pressione **[Foto]** na interface **[Add User]** para exibir a tela para registro de foto.
2. Na tela para registro de foto, fique de pé naturalmente na frente da tela.

Pressione **[Tirar foto]** para capturar a foto.

3. Depois de tirar a foto, pressione **[Feito]** para retornar à interface anterior.
4. Depois que a foto for tirada, pressione **[Salv]** para salvar as informações atuais e retornar à tela anterior; pressione **[Exit]** para retornar à tela anterior sem salvar as informações atuais.



2.11 Configurações de Acesso do Usuário*

Pressione [Acesso Usr] na janela [Add User] para exibir a tela de configurações de acesso.

As configurações de acesso do usuário são para definir os direitos do usuário para verificar e abrir a porta, tais como Verificar Tipo, Fuso Horário e gerenciamento de impressão digital de coação.



2.11.1 Verificar Tipo (verTipo)

(1) **Modo Verificar Grupo:** Se o usuário usar o modo verificar grupo, a qual ele pertence.

(2) **Modo Verificar individual:** Selecionar o modo verificação para este usuário em vez do modo verificar grupo. Isso não afetará outros usuários neste grupo.

Nota:(1) Apenas os produtos com um módulo de cartão de identificação integrado suportam a verificação de cartão de identificação.

Apenas alguns tipos de dispositivos suportam modo de autenticação multi-combinação.



2.11.2 Período

(1) **Período de Grupo:** Se o usuário usar o período de grupo, a qual ele pertence.

(2) **Período Individual:** Selecionar o período deste usuário em vez do período de grupo. Isso não afetará outros usuários neste grupo.

2.11.3 Estresse da impressão digital

O usuário pode registrar uma impressão digital de coação nova ou cancelar as impressões digitais de coação registradas. Se um dedo for registrado, as impressões digitais de coação, ao compará-lo, irá acionar o sinal de alarme de coação.

Se as impressões digitais de coação forem canceladas, os dados de impressões digitais não são excluídos, ainda se pode usar o processo de comparação de impressões digitais normalmente.



Gerenciamento de impressão digital de coação:

(1) Registrar Impressão Digital de Coação

Pressione [**Reg. FP Coação**] na tela [**Acesso Usr**] para exibir a janela [**Cadast.FP(4-0)**]. Na janela exibida [**Cadast.FP(4-0)**] colocar o dedo no sensor de impressão digital adequadamente de acordo com a mensagem do sistema.



(2) Cancelar Impressão Digital de Coação

Pressione [Can. FP coação] na tela [Acesso Usr] para aparecer a mensagem de confirmação. Selecione [Sim] para deletar a impressão digital de coação. Caso contrário, selecione [Não] para cancelar a operação.



3. Gerenciamento de Usuários

Procurar as informações do usuário, incluindo o nome do usuário, ID, impressão digital, face, cartão de identificação, senha, direitos, No. de grupo e configurações de acesso do usuário através desta interface. Para adicionar, editar ou deletar as informações básicas de usuários.

Pressione [Ger.Usuar] na tela do menu principal para exibir a janela de gerenciamento de usuários.



Este usuário é um administrador.

Nota: Os usuários são listados em ordem alfabética por sobrenome. Se pressionar em um nome de usuário, você pode acessar a janela de edição deste usuário para editar ou deletar as informações relacionadas ao usuário.



3.1 Editar um Usuário

Pressione no nome de um usuário na lista para entrar na janela **[Edit]**. A ID do usuário não pode ser modificada e as outras operações são semelhantes aquelas realizadas em *adicionar usuário*. Você pode registrar novamente sua impressão digital* e face, mudar senha, modificar os direitos de gerenciamento e No.de grupo*.

Por exemplo: Alterar os direitos do usuário de Administrador para usuário comum. Como mostrado abaixo:



3.2 Deletar um Usuário

Na janela **[Edit]**, você pode deletar todas informações do usuário ou parciais.

1. Pressione **[Apagar]** para deletar um usuário.
2. Clique em **[Sim]** para deletar o usuário atual ou **[Não]** para retornar à tela anterior.

3. Na janela **[Edit]**, pressione no nome, **[Fp]**, **[Face]**, **[Cartão]** ou **[Senha]** para deletar as informações relacionadas ao usuário e para registrar novamente as novas informações siga a mensagem do dispositivo.



3.3 Pesquisar um Usuário

Para facilitar aos administradores a localização de um usuário rapidamente para um grande número de usuários registrados, o dispositivo permite realizar pesquisas através do “ID do Usuário”.

Pesquisar ID do usuário:

1. Pressione [Pesq.] na tela [UsuárioAdm] para exibir a janela de pesquisa do ID de usuário.
2. Digite o ID de usuário na janela e clique em [OK] para localizar o cursor no usuário desejado.



4. Configurações de Comunicação

Você pode definir parâmetros relacionados para a comunicação entre o dispositivo e o PC, incluindo o endereço de IP, gateway, máscara de sub-rede, taxa de transmissão, ID de dispositivo e Tecla COM.



4.1 Configurações de Conexão

Ender.IP: O endereço de IP padrão é 192.168.1.201 e pode ser mudado conforme necessário.

Subnet Mask: A máscara de subnet padrão é 255.255.255.0 e pode ser mudada conforme necessário.

Gateway: O gateway padrão é 0.0.0.0 e pode ser mudado conforme necessário. (RS232/RS485), você deve verificar as seguintes configurações:

RS232*: Este parâmetro é usado para habilitar ou desabilitar a comunicação RS232. Se os cabos de comunicação RS232 forem usados, ajustar este parâmetro para “ON”.

RS485*: Este parâmetro é usado para habilitar ou desabilitar a comunicação RS485. Se os cabos de comunicação RS485 forem usados, ajustar este parâmetro para “ON”.

Taxa binária*: Este parâmetro é usado para configurar a taxa de transmissão para a comunicação entre o dispositivo e o PC. Inclui cinco opções: 9600, 19200, 38400, 57600, e 115200. A taxa de transmissão mais elevada é recomendada para a comunicação RS232 de alcançar comunicação de alta velocidade, enquanto a taxa de transmissão mais baixa é recomendada para a comunicação RS485 a fim de alcançar comunicação estável de baixa velocidade.

USB232*: Para se comunicar, decida se irá utilizar a comunicação USB ou não, isto é, caso for usar selecionar o item “Yes”. Caso contrário “No”.

ID terminal: Este parâmetro é usado para configurar a ID do dispositivo de 1 a 254. Se a comunicação RS232/RS485 for adotada, você deve entrar na ID do dispositivo na janela de comunicação de software.

Senha: Para aumentar a segurança de troca de dados, você pode definir uma senha para a conexão entre o dispositivo e o PC. Uma vez que a senha tenha sido definida, você pode conectar o PC com o dispositivo para acessar os dados somente depois de digitar a senha correta. A senha padrão é 0 (ou seja, nenhuma senha). Uma vez que uma senha tenha sido definida, você precisa digitar esta senha antes de conectar o software do PC com o dispositivo: caso contrário, a conexão será mal-sucedida. São suportadas senhas de 1-6 dígitos.

Considerando os dados consistentes, incluindo a impressão digital e modelos de face armazenados no dispositivo, é recomendado transferir os dados entre o dispositivo e o PC através da rede para melhorar a velocidade de transferência.

5. Configurações do Sistema

Através do menu **[Sistema]**, você pode definir os parâmetros relacionados ao sistema, incluindo Geral, Display, FP, Face, Presença, Definição de atalho, Opções de acesso e Atualizar, para permitir que o dispositivo atenda os requisitos do usuário na medida em termos de funcionalidade e exibição.

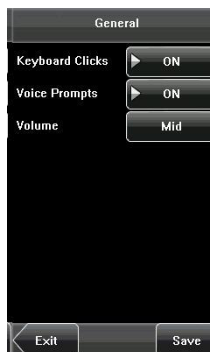


5.1 Parâmetros Gerais

Toque teclado: Esse parâmetro é utilizado para definir se o sinal de bipe em resposta a cada toque do teclado será gerado. Selecionar **“Lig”** para habilitar ou **“Des”** para silenciar.

Voz: Este parâmetro é usado para definir se o comando de voz será acionado durante a operação do dispositivo. Seleccione **“Lig”** para habilitar o comando de voz ou **“Des”** para silenciar.

Ajuste de som: Essa opção é utilizada para ajustar o volume das mensagens de voz.



5.2 Display

Linguagem: Essa opção é utilizada para exibir o idioma atual usado pelo dispositivo. Para dispositivos multilíngues habilitados, você pode alternar entre diferentes idiomas através dessa opção. Porém para efetivar as configurações deve-se reiniciar o dispositivo.

Estilo toolbar: Essa opção é utilizada para exibir o estilo das teclas de atalho na tela inicial. Pode-se definir como “*Escond Auto*” ou “*Sempre Exibe*”. Selecionando “*Escond Auto*”, você pode exibir ou ocultar a barra de ferramentas. Selecionando “*Sempre Exibe*”, você pode exibir permanentemente a barra de ferramentas na tela inicial.

TP dormida(S): Essa possui a finalidade de especificar um período posterior em que o dispositivo é posto no modo sono, caso não haja qualquer operação dentro deste período. Você pode ativar o dispositivo, em estado de inatividade, pressionando qualquer tecla ou toque na tela. Intervalo numérico 1 ~ 30 minutos, o padrão de fábrica para 3 minutos.

5.3 Parâmetros da Impressão Digital*

Limiar 1:1: Esse parâmetro é utilizado para ajustar o limiar da máquina para a atual impressão digital e o modelo de impressão digital inscrito no dispositivo no modo de verificação 1:1. Se a similaridade entre a impressão digital atual e do modelo de impressão digital registrada no dispositivo for maior que este limiar, a correspondência é bem sucedida, caso contrário, a correspondência não é bem sucedida.

Limiar 1:N: Este parâmetro é utilizado para definir o limite de correspondência entre a impressão digital atual e do modelo de impressão digital registrada no dispositivo em Modo de verificação 1:N. Se a similaridade entre a impressão digital atual e do modelo de impressão digital registrada no dispositivo for maior que este limiar, a correspondência é bem sucedida, caso contrário, a correspondência não é bem sucedida.



Os limiares recomendados são as seguintes:

(FRR)	(FAR)	Limiar	
		1:N	1:1
Alto	Baixo	45	25
Médio	Médio	35	15
Baixo	Alto	25	10

Imagem da Impressão Digital: Este parâmetro é usado para definir se deseja exibir a imagem da impressão digital na tela durante registro de impressões digitais ou comparação. Possui quatro opções:

Mostrar Cadastr.: Exibe a impressão digital na tela durante o processo de registro.

Mostrar Match: Exibe a impressão digital na tela durante o processo de verificação.

Mostrar Ambos: Exibe a impressão digital na tela no processo de registro e verificação.

Não mostra: Nunca exibe a impressão digital na tela em caso algum.

5.4 Parâmetros da Face

Limiar 1:1: Este parâmetro é usado para definir o limite de correspondência entre a face atual e o modelo de face registrado no dispositivo no modo de verificação 1:1. Se a similaridade entre a face atual e o modelo de face registrado no dispositivo for maior que este limiar, a correspondência é bem sucedida, caso contrário, a correspondência não é bem sucedida. O alcance de valor válido é 70-120. Quanto maior for o limiar mais baixa o FAR e quanto maior o FRR, e vice-versa.



Limiar N:1: Este parâmetro é usado para configurar o limiar de adequação entre a face atual e o modelo de face registrado no dispositivo no modo de verificação 1:N. Se a similaridade entre a face atual e o modelo de face registrado no dispositivo for maior que este limiar, a correspondência é bem sucedida, caso contrário, a correspondência não é bem sucedida. O alcance de valor válido é 65-120. Quanto maior for o limiar, mais baixo o FAR e quanto maior o FRR, e vice-versa.

Os limiares recomendados são os seguintes:

FRR	FAR	Limiar	
		1:N	1:1
Alto	Baixo	85	80
Médio	Médio	82	75
Baixo	Alto	80	70

Exposição: Essa especificação é utilizada para ajustar o valor da exposição da câmera.

Qualidade: Este parâmetro é usado para configurar um limiar de qualidade para as imagens de face obtidas. O dispositivo aceita as imagens da face e as processa, adotando o algoritmo de face quando a sua qualidade for maior do que o limiar; caso contrário, filtra as imagens de face.

Nota: O ajuste inadequado dos parâmetros de exposição e de qualidade pode afetar gravemente o desempenho do dispositivo. Por favor ajustar ajuste o parâmetro de exposição somente sob a orientação do pessoal de serviço pós-venda da nossa empresa.

5.5 Presença

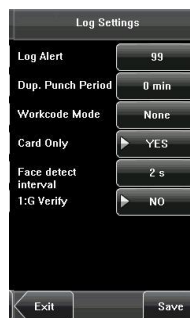
Log Alerta: Quando o espaço disponível for insuficiente para armazenar o número especificado de registros de acessibilidade, o dispositivo automaticamente gerará um alarme (alcance de Valor: 1-99).

Reveri. TP: Se o registro de acessibilidade de um usuário já existe e o mesmo bate o cartão novamente dentro do período especificado (unidade: minuto), o segundo registro de acessibilidade não será armazenado (Faixa de valor: 1-60 minutos).

Apenas o Cartão*: Se esse parâmetro for definido “YES” a verificação é feita somente por verificação do cartão. Se esse parâmetro for definido “NO”, você precisa verificar sua face ou impressão digital após a verificação do cartão.

Intervalo comparação face: De acordo com sua necessidade para defini-lo. O valor padrão é 0, ou seja, não há intervalo.

Verificar 1:G*: Selecionar “SIM” ou “NÃO”, ou seja, definir se a função é iniciada ou não.

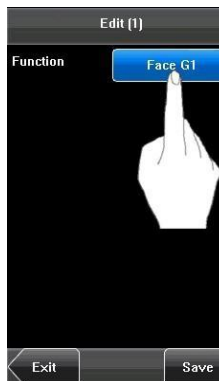
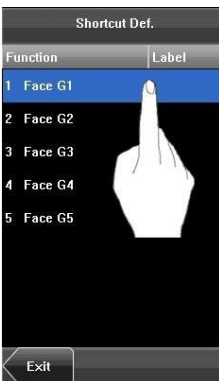


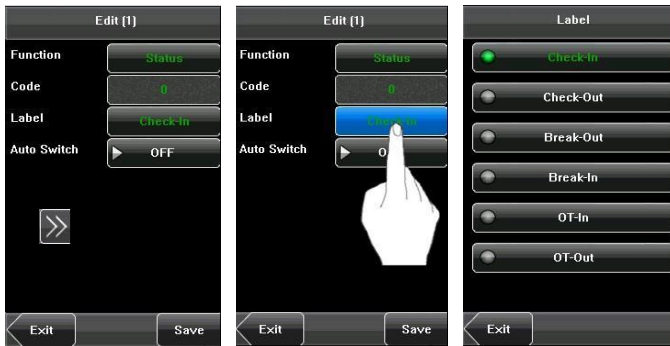
5.6 Definições de Atalho

Definir as teclas de atalho funcionais para o *touch screen*. Para o dispositivo com função de agrupamento de faces (MENU-System-Log Settings-1:G Verify), o método para definição das teclas de atalho é descrito a seguir:

1. Definir as teclas de atalho

(1) Clique no item **[Definição de atalho]** para exibir a lista das teclas de atalho existentes, clique na tecla de atalho para modificar. Entre na tela de edição, e clique na caixa **Função**. O usuário entrará na tela **Função**, podendo selecionar as configurações desejadas para os tipos de teclas de atalho de acordo com as necessidades práticas, tais como 1-5 grupos de faces (Ativar grupos, verifique a função), indefinido, status, (código de trabalho) e SMS.





(2) O usuário pode definir a tecla de atalho como de status. Clique no status, como mostra a figura acima. Entre na tela de edição da tecla de status. Clique na caixa Nr. Clique na linha da tela Nr (seis opções para status) para mudar a etiqueta correspondente, o usuário pode modificar a etiqueta da tecla Status de acordo com as necessidades práticas.

(3) O código não pode ser modificado. Somente será modificado de acordo com o **Nome** selecionado para a tecla de status. Selecione [Tecla Autom] e selecione [Definir].



4) Clique na caixa de tempo para os dias da semana, para entrar na tela de configuração de tempo. Clique na tecla na tela de toque para definir o tempo, clique em [OK] para salvar e retornar à tela de edição.

(5) Depois de concluída a configuração, clique em [Salv] para salvar a configuração e retornar a “Definição de atalho”.

2. Usar teclas de atalho

Clique em na tela inicial. O status relacionado e as teclas de função serão exibidas no canto direito da tela para o uso.

5.7 Opções de Acesso*

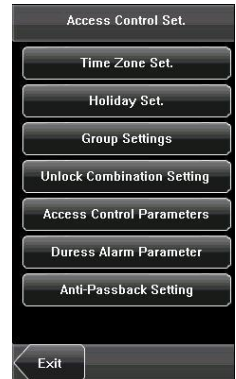
As configurações do controle de acesso são para definir os horários de acessibilidade para abertura de porta do usuário. Por padrão, é desabilitado de fábrica, para habilitar você pode acessar: [MENU]-[Sistema]-[Display]-[Accion.conf.aces.], selecione Sim ou NÃO.

Para desbloquear, o usuário registrado deve estar de acordo com as seguintes condições:

1. O tempo de desbloqueio atual deve ser efetivo na zona de tempo do usuário ou zona de grupo.

2. O grupo onde o usuário está deve estar em controle de acesso (ou no mesmo controle de acesso com outro grupo, para abrir a porta juntamente).

O novo usuário registrado estará no grupo 1 por padrão, zona de tempo e grupo de controle de acesso. Novos registros estarão em estado de desbloqueio (caso as configurações do controle de acesso forem alteradas, o sistema alterará automaticamente).



5.7.1 Opções de Hora

A zona de tempo é a opção mínima de unidade para o controle de acesso. O sistema pode definir 50 zonas de tempo. A zona é composta de 7 (sete) seções de tempo (que equivale a uma semana). Cada zona de tempo contém 24 horas todos os dias. Cada usuário pode ajustar 3 zonas de tempo. O formato das seções de tempo são de HH:MM-HH:MM.

Se o hora de encerramento é menor que a hora de início (23:57 23:56), não é válido. Se a hora de encerramento é maior que a hora inicial (00:00 23:59), a seção é válida.

A zona de tempo efetiva para desbloqueio do usuário: 00:00 23:59 o horário de encerramento é maior que o horário de início.

Nota: O padrão do sistema da zona de tempo 1 é de acessibilidade integral (ou seja, o usuário já possui o acesso liberado).



5.7.2 Opções de férias

O tempo de controle de acesso especial pode ser necessário durante os feriados. O controle de acesso é diferenciado por modificar a acessibilidade para todos os usuários.

1. Adicionar feriado:

(1) Entre na tela adicionar feriado, pressione a tecla para editar os itens.

(2) Pressione o teclado numérico na tela de toque para definir o valor. Depois de definido, pressione [OK] para salvar e pressione [X] para sair e retornar à tela anterior.

(3) Pressione [Salvar] para salvar as informações atuais e retornar à tela anterior ou pressione [Volta] para retornar à interface anterior sem salvar as informações atuais.



2. Editar feriado

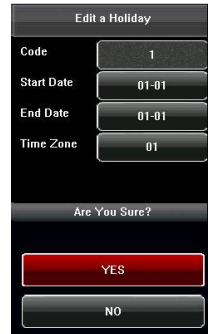
Selecione o feriado desejado para editar. Entre na tela de edição. A operação para edição é semelhante a adicionar feriado. Depois de editar, pressione [Salv] para salvar e retornar à tela anterior.

Nota: Se o tempo para o controle de acesso aos feriados for definido, o período para acessibilidade do usuário durante o feriado deve ser definido aqui.



3. Deletar feriado

Selecione o feriado a ser deletado. Pressione [Apagar] para aparecer a tela de confirmação. Selecione [Sim] para apagar este feriado ou selecionar [Não] para cancelar a operação.



5.7.3 Configuração da Zona de Tempo do Grupo

O agrupamento é utilizado para gerenciar os funcionários em grupos. Funcionários em grupos utilizam a zona de tempo padrão. Membros de grupos também podem ajustar a zona de tempo para usuários. Cada grupo pode possuir três zonas de tempo. Novos usuários registrados automaticamente pertencem ao Grupo 1, porém podem ser alocados em outros grupos.



1. Adicionar fuso horário de grupo

(1) Entre na janela [Opções de grupo], pressione a tecla para editar os itens.

Nr.: Entrar na tela de edição do código para definir o valor.

VerTipo: Selecionar Grupo VerTipo.

Férias: Selecione se a zona de tempo é válida no feriado.

Período: Selecionar o Fuso Horário de Grupo.

(2) Depois de editar, pressione [Salv] para salvar as informações atuais e retornar à tela anterior ou pressione [volta] diretamente para retornar à tela anterior sem salvar as informações atuais.



Nota: (1) RF quer dizer verificação do cartão de ID. Apenas os produtos que possuem módulo integrado para cartão de identificação suportam a verificação do cartão de ID.



Nota:

(1) Se o feriado for válido, apenas quando houver uma interseção entre zona de grupo e zona de tempo do feriado, um membro do grupo poderá abrir a porta.

(2) Se o feriado for inválido, o tempo de controle de acesso para membro de grupo não será afetado por finalidade do feriado.

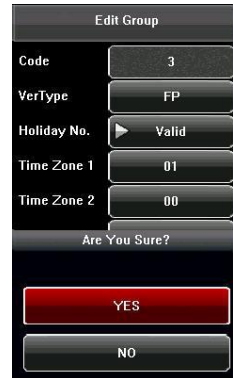
2. Editar zona de tempo do grupo

Pressione a opção para edição da zona de tempo e entre na tela de edição. Depois de editar, pressione **[Salv]** para salvar informações atuais e retornar à tela anterior. Pressione **[Volta]** para retornar diretamente à janela anterior sem salvar as informações.



3. Deletar zona de tempo do grupo

Selecione a zona de tempo que será deletada. Pressione **[Apagar]** para aparecer a tela a confirmação para deletar. Selecione **[Sim]** para deletar este feriado ou selecione **[Não]** para cancelar a operação.



5.7.4 Configuração da Combinação de Destravamento

Fazer com que vários grupos dentro de diferentes níveis de acesso realizem multiverificações, melhorando assim a segurança. Um controle de acesso pode ser realizado para até 5 grupos no máximo.

1. Adicionar Combinação de Destravamento

(1) Entre na interface Configuração de Combinação para adicionar feriado, pressione a tecla para editar os itens.

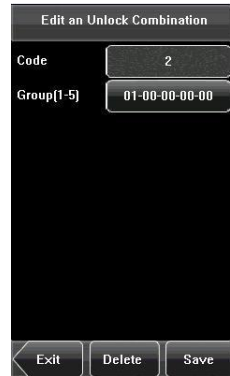
(2) Pressione o teclado numérico para definir o valor, depois de configurar, pressione **[OK]** para salvar ou pressione **[X]** para sair e retornar à tela anterior.

(3) Pressione **[salv]** para salvar as informações atuais e voltar à interface anterior, pressione **[Volta]** diretamente para voltar à interface anterior sem salvar as informações atualizadas.



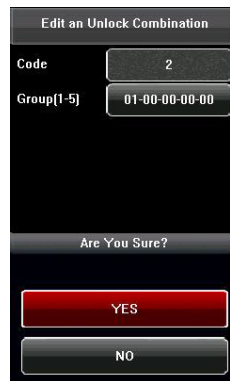
2. Editar Combinação de Destravamento

Selecione a opção a ser editada. Pressione o item para entrar na tela de edição. Depois da edição concluída, pressione **[Salv]** para salvar as informações alteradas e retorne à tela anterior ou pressione **[Volta]** para retornar à tela anterior sem salvar as informações atuais.



3. Deletar Combinação de Destravamento

Selecione a opção para ser deletada. Pressione **[Apagar]** para aparecer a confirmação na tela. Selecione **[Sim]** para deletar ou selecione **[Não]** para cancelar a operação.



5.7.5 Parâmetro de controle de acesso

Pelo menu **[Parâmetros de Acesso]**, você pode definir os parâmetros das travas eletrônicas e os dispositivos de controle de acesso relacionados.

Demora de bloq: Indica o tempo para o dispositivo colocar a trava elétrica em estado de desbloqueio. (Valor de alcance: 1-10 segundos)

Demora sensor porta: Indica o atraso para verificação do sensor de porta, depois que a mesma for aberta. Se o estado do sensor da porta for inconsistente com o estado normal definido pelo interruptor do sensor de porta, um alarme será desencadeado, e este período de tempo é considerado como “atraso do sensor de porta”. (Valor de alcance: 1-99 segundos)



Modo sensor de porta: Inclui os modos None (Nenhum), Normally Open (NA) (Normalmente Aberto), Normally Closed (NC) (Normalmente Fechado).

“None” indica que o interruptor do sensor de porta não está sendo usado.
“NO” Indica que o sensor da porta está aberto no estado normal.

“NC” Indica que o sensor da porta está fechado no estado normal.

Atraso do Alarme: Indica a duração da detecção do sensor da porta com exceção à geração do sinal de alarme. (Valor de alcance: 1-99 segundos)

Número de falsos alarmes: Quando o limite de tentativas para digitar a senha exceder, o alarme dispara. (Valor alcance: 1-9 vezes).

Período fechamento: Definir zona de tempo para controle de acesso NF. Nenhum usuário pode destravar durante esta zona de tempo.

Período da aberta permanente: Definir zona de tempo para controle de acesso NA. A trava está sempre em estado de desbloqueio durante esta zona de tempo.

As férias são válidas?: Definir zona de tempo para NA ou NF. Quando for definida zona de tempo no feriado é válida.

Nota:

1. Se a zona de tempo de NA ou NF for definida, mudar o sensor de porta para NA, caso contrário o mesmo irá emitir o alarme durante a abertura e fechamento de porta.

2. Se a zona de tempo NA ou NF ainda não estiver sido definida pelo tempo, o equipamento solicitará que você defina a zona de tempo, e você será direcionado para a tela da zona de tempo para inclusão.

5.7.6 Parâmetros do Alarme de Coação

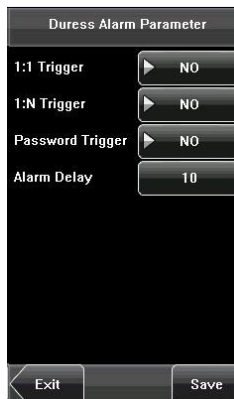
Existe a configuração de parâmetros de alarme de coação no dispositivo. Quando um funcionário estiver diante de uma situação de coação, é possível usar o modo de alarme de coação. O dispositivo abrirá a porta normalmente, mas o sinal de emergência será enviado ao sistema.

Acionamento 1: 1: se selecionar “Sim”, quando o usuário usar o modo de comparação 1: 1, o sinal de alarme irá disparar.

Acionamento 1: N: se selecionar “Sim”, quando o usuário usar o modo de comparação 1: N, o sinal de alarme irá disparar.

Acionamento de Senha: Se selecionar “Sim”, quando um usuário utilizar o modo verificação de senha, o sinal de alarme irá disparar.

Atraso de Alarme: Após o alarme de coação iniciado, o alarme não terá saída diretamente. Poderá ser definido. Depois do período de tempo definido, o sinal de alarme será gerado automaticamente (Variação de tempo: 0-255 segundos).



5.7.7 Configuração de Anti-passagem de retorno

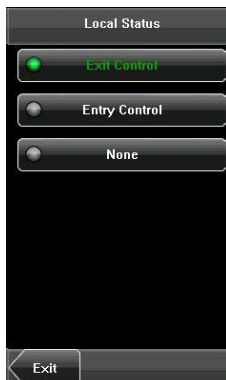
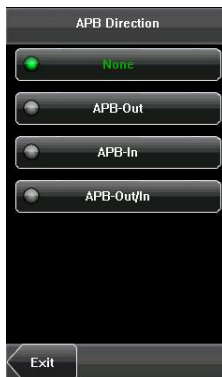
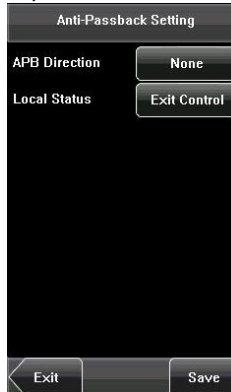
Configurar a função Anti-passagem de retorno do dispositivo.

Direção ASW: Há quatro opções: **Anti-ASW**, **Sair do ASW**, **Entrar no ASW**, **ASW-In/Out**.

Estado do dispositivo: Há três opções: **Controle de Saída**, **ControlDent**, **Nada**.

Operação de configuração da Anti-dupla passagem:

- (1) Entre na tela de configuração da **Conjunto ASW**, pressione a tecla para editar os itens.
- (2) Pressione a tecla do número da tela de toque para definir o valor, depois da configuração, pressione [OK] para salvar e pressione [X] para sair e retornar à interface anterior.
- (3) Pressione [Salv] para salvar as informações atuais e retornar à interface anterior; pressione [Volta] diretamente para retornar à interface anterior sem salvar as informações atuais.



5.8 Atualização

Você pode atualizar o firmware do dispositivo usando o arquivo de atualização no USB através desta função.



Caso haja necessidade de atualização do sistema, entre em contato com o departamento de suporte técnico para as devidas instruções.

6. Configuração Data/Hora

6.1 Configurar Data/Hora

A data e a hora do dispositivo devem ser definidas precisamente para garantir a exatidão de tempo para o controle da frequência.

1. Pressione **[Menu]** na tela inicial para exibir o menu principal.
2. Pressione **[Data/Hora]** na janela do menu principal para exibir a tela de configuração de tempo.
3. Selecione a data e a hora desejada pressionando o parâmetro. Para o ajuste de tempo, há como selecionar 10 formatos. A configuração de tempo suporta o formato de 12 e 24 horas.
4. Pressione **[Salv]** para salvar as informações atuais e retornar à tela anterior. Pressione **[Volta]** para retornar à tela anterior sem salvar as informações atuais.



6.2 Configuração da Campanha

Algumas empresas emitem campanhas para determinar o início e término da jornada de trabalho. Para reduzir os custos e facilitar o gerenciamento, foi integrada uma função para monitoramento de tempo da campanha ao dispositivo.

Você pode definir o tempo de duração para alarme e também tocar a campanha com base em suas necessidades de modo que o dispositivo reproduzirá automaticamente o toque selecionado, acionará o relé na hora de alarme e parará a reprodução do toque após a duração definida. Cada dispositivo pode adicionar 15 períodos para acionamento da campanha.

Pressione em **[Camp]** no menu **[Data/Hora]** para exibir a tela de configuração da campanha, como mostra na figura abaixo.



1. Adicionar uma campanha

1) A tela exibe a lista para configuração da campanha com todos os alarmes. Clique em **[Add]** para exibir a tela para adicionar alarme.

2) Na janela **[Add]**, definir os seguintes parâmetros:

Temp: Esse parâmetro é usado para definir o tempo em que o dispositivo reproduz automaticamente a campanha diariamente.

Data da Campanhia: Este parâmetro é utilizado para definir qual a data o dispositivo irá reproduzir automaticamente a campanha.

Ring: Este parâmetro é utilizado para definir o toque musical da campanha.

Volume: Este parâmetro é usado para configurar o volume do toque da campanha.

Repetir: Este parâmetro é usado para definir os horários do alarme.

Estado: Essa configuração permite definir se a campanha será habilitada ou não.

Tipo de campanha: Você pode selecionar entre a campanha interna e a campanha externa. Para campanha interna, será reproduzida pelo autofalante do dispositivo. Para externa, será reproduzida por uma campanha elétrica externa que está conectada ao dispositivo.

2. Editar e deletar uma campanha

Selecione uma campanha da lista exibida na tela de edição para apresentar a janela **[Edit]** para operação análoga **[Adi]** (Adicionar uma campanha).

Nota: Somente alguns modelos possuem essa função. Caso necessário, entre em contato com nosso representante comercial ou técnico.



6.3 Horário de Verão (DLST)

DLST, também chamado de Horário de Verão. É um sistema utilizado para ajustar a hora local com finalidade de economizar energia. O sistema normalmente adianta uma hora no verão. O regulamento pode diferir entre os países. Atualmente, aproximadamente 110 países adotam o sistema DLST.

Para atender aos requisitos do DLST, uma opção especial pode ser personalizar o cartão de tempo RF & gravador de frequência. Ajuste o tempo para uma hora à frente, em XX (minuto) XX (hora) XX (dia) XX (mês), e atrase uma hora XX (minuto) XX (hora) XX (dia) XX (mês) se for necessário.

Operação:

Primeiramente selecione o modo DLST. Dentro da janela há as opções “**Mode 1**”, “**Mode 2**” e “**Nada**” (Nenhum). A configuração padrão é “**Nada**”.

1. Clique em [**Nada**] para exibir a janela de seleção para o modo DLST.
2. Selecione o modo desejado para o DLST e retorne à interface

Date/Time:



3. Clique em [**DST settings**], entre na janela de edição DLST.
4. Após a configuração, clique em [**Salv**] para finalizar e retornar.

7.AutoTeste

O autoteste permite que o sistema automaticamente teste se as funções de vários módulos estão funcionando de acordo com o esperado, incluindo tela, sensor, voz, face, teclado e testes de relógio.



1. **Testar de écran:** O dispositivo automaticamente testa o efeito das cores TFT, com a exibição das cores: preto e branco. Verifique se a tela exibe corretamente. Você pode continuar o teste tocando na tela ou saindo pressionando [Volta].

2. **Teste de impressão digital:** O dispositivo automaticamente testa se o sensor de impressão digital funciona corretamente, verificando se as imagens das impressões digitais são claras e aceitáveis. Quando o usuário coloca o dedo sobre o sensor, a imagem da impressão digital coletada é exibida na tela em tempo real. Caso o usuário desejar sair do teste, pressionar [Volta].

3. **Teste de Voz:** O dispositivo automaticamente testa se os arquivos de voz estão completos e a qualidade de voz é adequada, reproduzindo os arquivos de voz armazenados no dispositivo. Caso o usuário desejar sair do teste, pressionar [Volta].

4. **Teste Face:** O dispositivo automaticamente testa se a câmera funciona corretamente verificando se as imagens de face coletadas são claras e aceitáveis. Pressione [Exit] para sair do teste.

5. **Testar Teclado:** O dispositivo testa se cada tecla no teclado funciona normalmente. Pressione qualquer tecla na interface [Keyboard Test] para verificar se a

tecla pressionada corresponde à tecla exibida na tela. As teclas são cinza escuro antes de pressionadas, e ficam azuis depois de pressionadas. Pressione [Volta] para sair do teste.

6. Teste do tempo: O dispositivo testa se seu relógio funciona adequadamente verificando o cronômetro do relógio. Pressione [Volta] para sair do teste.

7. Adjust:

Você pode realizar todas as operações de menu tocando na tela com um de seus dedos ou uma caneta de toque. Quando a tela de toque é menos sensível ao toque, você pode executar uma calibração da tela por meio de operações de menu.

Operação de Calibração de Tela:

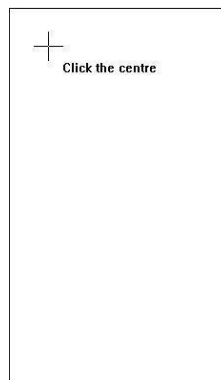
(1) Pressione **[Menu]** na interface inicial para exibir o menu principal.

(2) Pressione **[Adjust]** na interface **[Auto Test]** para exibir a interface de calibração da tela.

(3) Tocar o centro da cruz "+".

(4) Repetir o passo 3 seguindo o movimento do ícone "+" para diferentes locais na tela.

(5) Tocar o centro da cruz em cinco locais na tela corretamente. Quando a mensagem *"Calibrating screen, pls wait....."* (Calibrando a tela, favor aguardar.....) é exibida na tela, a calibração é bem sucedida e o sistema retorna automaticamente ao menu principal. Se a calibração falhar, o sistema iniciará a recalibração a partir do Passo 3.



8. Gerenciamento do USB

Pelo menu [USB] , você pode baixar as informações do usuário e os dados de frequência armazenados em um USB para software relacionado ou outro equipamento de reconhecimento de impressão digital.



1. **Download Attlog:** Download de todos os dados de frequência do dispositivo para um Pen Drive.

2. **Download Usuário:** Baixar todas as informações do usuário, impressões digitais e imagens de face do dispositivo para um Pen Drive.

3. **Baixar a foto do usador:** Baixa as fotos dos funcionários do dispositivo para um disco USB.

4. **Upload Usuário:** Carregar as informações do usuário, impressões digitais e imagens de face armazenadas em um Pen Drive para o dispositivo.

5. **Upload foto:** Carregar os documentos JPG que são nomeados de acordo com as IDs de usuário e armazenados em um Pen Drive para o dispositivo de modo que as fotos do usuário podem ser exibidas após o funcionário passar a verificação.

8.1 USB

1. Hospedeiro USB

O dispositivo de impressões digitais pode ser utilizado como hospedeiro USB para troca de dados com o USB externo.

A velocidade de transmissão de dados é rápida, o dispositivo de impressão digital tradicional suporta apenas o modo RS485, RS232 ou Ethernet para transmissão de dados, quando como resultado da condição física limite, a quantidade de dados é grande e a transmissão de dados leva bastante tempo. Mas a transmissão de dados USB é mais rápida do que qualquer dos modos de transmissão anterior, podendo completar download de dados pelo USB em um curto período de tempo, uma vez que isto aumenta significativamente a eficiência.

2. Cliente USB

O dispositivo de impressão digital será como dispositivos de armazenamento removível e os dados do dispositivo de impressão digital serão transferidos para um PC através de cabo USB.

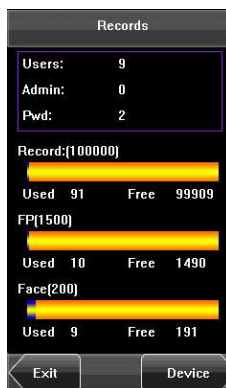
Quando o dispositivo de impressão digital é como um cliente USB, o menu das configurações de comunicação do dispositivo de impressão digital terá opções de comunicação USB.

9. Informações do Sistema

Você pode verificar o status do armazenamento, bem como informações sobre a versão do dispositivo através da opção **[InfoSis]**.

Registros: O número de usuários, administradores e senhas registrados é exibido na interface **[Records]**; A capacidade de armazenamento total e a ocupada de impressões digitais, bem como a capacidade total e a ocupada de frequência são exibidas graficamente, respectivamente.

Dispositivo: O nome de dispositivo, número de série, versão, fornecedor e data de fabricação são exibidos na interface **[Terminal]**.



10. Apêndice

10.1 Apêndice 1 Introdução a Wiegand

Wiegand26 é um protocolo de acesso de controle padrão estabelecido pela Subcomissão de Controle de Acesso Padrão filiado à Associação da Indústria de Segurança (SIA). É uma interface de leitor de cartão IC sem contato e protocolo de saída.

Wiegand26 define a interface entre o leitor de cartões e um controlador usado no controle de acesso, segurança e outros campos industriais relacionados. Wiegand26 ajuda

a padronizar o trabalho dos designers de leitor de cartão e os fabricantes de controlador. Os produtos de controle de acesso fabricados pela nossa empresa são projetados também seguindo este protocolo.

10.2 Sinais digitais

A figura abaixo é um diagrama de sequência em que o leitor de cartão envia os sinais digitais em formato de bits para o controlador de acesso. Neste diagrama de sequência, Wiegand segue o protocolo de controle de acesso padrão da SAI para o leitor de cartão Wiegand 26bit (um tempo de pulso entre 20us e 100 us e o tempo de salto de pulso variam entre 200us e 20ms). Data1 e Data0 são sinais de nível elevado (maior do que Vol) até que o leitor de cartões se prepara para enviar um fluxo de dados. O pulso de baixo nível assíncrono (menor do que Vol) gerado pelo leitor de cartões é enviado para o painel de controle de acesso (A onda em dente de serra, como mostrado na Figura abaixo) através de Data1 ou Data0. Os pulsos Data1 e Data0 não irão sobrepor-se nem ser gerados sincronicamente. A tabela abaixo mostra a largura de pulso máxima e mínima (um pulso consecutivo) e tempo de salto de pulso (tempo entre os pulsos) permitido pelo dispositivo de impressão digital controle de acesso série F.

Figure: Sequence Diagram

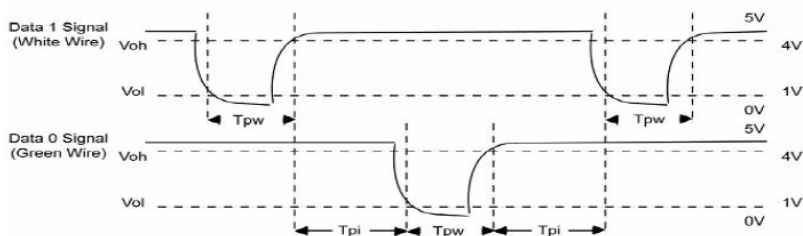


Table: Pulse Time

Symbol	Definition	Typical Value of Reader
Tpw	Pulse Width	100 μ s
Tpi	Pulse Interval	1 ms

10.3 Apêndice 2 Função ID de Foto

A função ID da foto é utilizada para exibir a foto registrada por um usuário ou armazenada em um disco USB na tela, além de informações como a identificação do usuário e nome.

[Passos Operacionais]

1. Quando a foto tirada pelo dispositivo é utilizada, a foto pode ser visualizada na verificação bem sucedida.

2. Para usar uma foto armazenada em um disco USB, proceda do seguinte modo:

1) Crie uma pasta com o nome de “fotografia” no disco USB e armazene as fotos do usuário nesta pasta.

2) As fotos do usuário devem estar no formato JPG e nomeadas de acordo com suas IDs. Por exemplo, para o usuário com a ID de usuário 154, o nome da foto deve ser 154.jpg.

3) Inserir o disco USB na entrada USB no dispositivo e selecionar USB Disk Management -> Upload -> Upload Photos. Em seguida, as fotos do usuário podem ser exibidas após a verificação bem sucedida.

Nota:

1) A extensão de um nome de usuário não pode exceder 24 dígitos.

2) O tamanho recomendado de uma foto do usuário é menos de 64k bit.

3) A foto do novo usuário carregada irá substituir a foto existente relacionada com a ID de usuário.

4) Para baixar as fotos do usuário, selecione USB Disk Management -> Download -> Download User Photos. Uma pasta com o nome de “foto” será automaticamente criada no disco USB e todas as fotos do usuário baixadas são armazenadas nesta pasta.

10.4 Apêndice 3 Modo de Autenticação de Multi-combinação

Além desta função ser somente de propriedade da máquina de controle de impressão digital de acesso que tiver sido nomeada, a maioria das máquinas de impressão digital só possuem duas maneiras de verificarem por impressão digital e senha, nós fornecemos um Modo de Autenticação pessoal ou de grupo Multicominação para área de controle de acesso de alta segurança, tipo de verificação principal inclui cinco elementos que são User Number (Número de Usuário (PIN), Fingerprint (impressão Digital) (FP), Face (Face) (FACE), Password (Senha) (PW) e RF card (Cartão RF) que pode combinar em multi-combinação.

Nota: O cartão de RF é usado para verificação do cartão de ID, a função de verificação de cartão ID só é válida na máquina que é equipada com esta função. Estes símbolos ilustram a seguinte tabela.

- “/” é ou
- “&” é e
- FP (impressão digital)
- RF (RF card)
- “+” seguir próxima operação
- FACE (Face)
- PWD (Senha)
- PIN (ID de usuário)

Se a impressão digital, face, senha e cartão foram inscritos para o usuário, o procedimento de verificação é o seguinte.

Type	What you do
FACE&PIN/FP/PW/RF	FACE+PIN or RF or PW or RF are verified
	1) PIN++FACE(1:1) 2) FP(1:N) 3) PIN+PW+“OK” 4) RF(1:N)

FACE&PIN	FACE + PIN are verified
	PIN+FACE(1:1)
FP/RF	FP or RF is verified
	1) PIN+FP(1:1)
	2) RF(1:N)
	3) FP(1:N)
PW/RF	FP or RF is verified
	1) PIN+PW+“OK”
	2) RF(1:N)
FP/PW	FP or PW is verified
	1) PIN+FP(1:1)
	2) FP(1:N)
	3) PIN+PW+“OK”
PIN&FP	PIN + FP are verified
	PIN+FP(1:1)
	2) PIN+FACE(1:1)+PW
	3) PIN+PW+FACE
FACE&RF	FACE + RF are verified
	1) FACE(1:N)+RF
	2) PIN+FACE(1:1)+RF
	3) RF(1:N)+FACE
FP	Only FP is verified.
	1) PIN+FP(1:1)
	2) FP(1:N)
PW	Only PW is verified
	PIN+PW+“OK”
RF	Only RF is verified
	RF(1:N)

	1) FACE(1:N)+FP+RF 2) FP+FACE(1:1)+RF 3) RF(1:N)+FACE+FP 4) PIN+FP(1:1)+FACE+RF 5) PIN+FACE(1:1)+FP+RF
FACE&FP&PW	FACE + FP + PW are verified
	1) FACE(1:N) +PW+“OK”+FP 2) FP+PW+“OK”+FACE(1:1) 3) PIN+FP(1:1) +PW+“OK”+FACE 4) PIN+FACE(1:1) +PW+“OK”+FP 5) PIN+PW+“OK”+FP+FACE
FP&PW&RF	FP + PW + RF are verified
	1) FP(1:N)+PW+“OK”+RF 2) PIN+FP(1:1)+PW+“OK”+RF 3) RF(1:N)+PW+“OK”+FP 4) PIN+ PW+“OK”+FP(1:1)+RF
PIN&FP& PW	PIN + FP + PW are verified
	1) PIN+PW+“OK”+FP(1:1) 2) PIN+FP(1:1)+PW+“OK”
FP & RF/PIN	FP + PIN, or FP + RF are verified
	1) RF+FP(1:1) 2) FP(1:N)+RF 3) PIN+FP(1:1)
FACE&FP&RF	FACE + FP + RF are verified

10.5 Apêndice 4 Anti-Passagem de Retorno

[Vista geral]

Às vezes, algumas pessoas ilegais seguem o outro no portão, causando problemas de segurança. Para prevenir tais riscos, esta função é habilitada.

O registro de entrada coincide com o registro de saída ou o portão não abrirá.

Esta função necessita que as duas máquinas trabalhem juntas. Uma é instalada dentro da porta (doravante máquina mestre) e a outra está instalada do lado de fora da porta (doravante máquina escrava). A comunicação do sinal Wiegand é adotada entre as duas máquinas.

[Princípio de funcionamento]

A máquina mestre tem a função Wiegand de entrada e a máquina escrava tem a função Wiegand de saída. Conectar Wiegand de Saída da máquina escrava ao Wiegand de Entrada da máquina mestre. Wiegand de Saída da máquina escrava não deve possuir a ID de máquina. O número enviado para a máquina mestre a partir da máquina escrava deve ser encontrado na máquina mestre.

[Função]

Avaliar se é anti-passagem de retorno acordo com o recente registro de entrada e saída do usuário.

O registro de entrada e o registro de saída devem coincidir. Esta máquina suporta saída, entrada ou entrada/saída anti-passagem de retorno.

Quando a máquina mestre é configurada com “saída anti-passagem de retorno”, se o usuário desejar entrar e sair normalmente, seu recente registro deve ser “entrada” ou ele não poderá sair. Qualquer tentativa de “saída” será recusada pela função de “anti-passagem de retorno”. Por exemplo, o recente registro de um usuário é “entrada”, seu segundo registro pode ser “saída” ou “entrada”.

Seu terceiro registro é baseado no seu segundo registro. O registro de saída e o registro de entrada devem coincidir. (Nota: Se o cliente não tem um registro anterior, então ele pode entrar, mas não pode sair).

Quando a máquina mestre é configurada como “entrada anti-passagem de retorno”, se o usuário desejar entrar e sair normalmente, seu recente registro deve ser “saída” ou

ele não poderá sair. Qualquer registro de saída será de “anti-passagem de retorno” negada pelo sistema. (Nota: Se o cliente não tem registro anterior, então ele pode sair, mas ele não pode entrar).

Quando a máquina mestre é configurada como “anti-passagem saída-entrada”, se o usuário desejar entrar e sair normalmente, se seu recente registro for “saída” e “entrada”, então seu próximo registro deve ser “entrada” e “saída”.

[Operação]

1. Selecione o modelo

Máquina mestre: A máquina com função Wiegand de entrada, exceto o leitor F10.

Máquina escrava: A máquina com a função Wiegand de saída.

2. Configuração do menu Anti-passagem de retorno

Há quatro opções: entrada/saída de anti-passagem de retorno, saída anti-passagem de retorno, entrada anti-passagem de retorno e nenhuma.

Saída anti-passagem de retorno: Apenas o último registro do usuário está como entrada, a porta pode ser aberta.

Entrada anti-passagem de retorno: Apenas o último registro do usuário está como saída, a porta pode ser aberta.

Status do dispositivo: Há três opções:

Controle-entrada, controle-saída e nenhum.

Controle-entrada: Quando é configurado, os registros verificados no dispositivo são registros de entrada.

Controle-saída: Quando é configurado, os registros verificados no dispositivo são registros de saída.

Nenhum: Quando é configurado, fecha a função de anti-passagem de retorno do dispositivo.

3. Modificar o formato de saída Wiegand do dispositivo

Quando os dois dispositivos estão se comunicando, apenas os sinais Wiegand sem ID do dispositivo são recebidos. Entre device menu-> communication option-> Wiegand option ou entre em software ->basic setting -> device management -> Wiegand, para modificar “formato definido” como “wiegand26 sem ID do dispositivo”.

4. Registrar usuário

O usuário deve estar na máquina mestre e na máquina escrava simultaneamente e o PIN do usuário deve ser o mesmo. Portanto, é necessário registrar o usuário na máquina mestre e na máquina escrava simultaneamente.

5. Instrução de conexão

A comunicação de Wiegand é adotada para máquina mestre e máquina escrava. Consultar o seguinte para a conexão:

Mestre		Escravo
IND0	<----->	WD0
IND1	<----->	WD1
GND	<----->	GND

Especificações

Câmera	Alta resolução Infravermelha
Display	Touch Screen
Capacidade de Armazenamento de faces	500
Capacidade de armazenamento de digitais	2.000
Capacidade de armazenamento RFID	10.000
Capacidade de armazenamento de logs	100.000
Wiegand para comunicação entre dispositivos	Entrada e saída
Tensão de Alimentação	12VCC

Corrente de Consumo (mA)	Estado normal	235
	Utilizando a Câmera	370
	Alternando os menus	200
	Verificando impressão Digital/cartão	243
	Relé atuando	252
	Modo stand by	155
	Inicializando	249
Temperatura de operação	0° ~ +50° C	
Umidade Relativa	20% ~ 80%	
Dimensões (AxLxP)	275x100x195mm	
Campainha	Contato seco	
Botão de Saída	NA	
Alarme	Contato seco	
Tamper	Sim	
Sensor de porta aberta	NA/NF	
Saída para fechadura	NA/C/NF	

Certificado de Garantia

1- Todas as partes, peças e componentes, são garantidos contra eventuais DEFEITOS DE FABRICAÇÃO que porventura venham a apresentar, pelo prazo de 1 (um) ano, contado a partir da data de emissão da nota fiscal do produto.

2- Constatado o defeito, deve-se imediatamente comunicar à empresa que efetuou a instalação ou serviço autorizado mais próximo. Somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia. Caso contrário esta garantia perde o efeito, pois o produto terá sido violado.

3- Em caso de atendimento domiciliar e/ou necessidade de retirada do produto, as despesas decorrentes de serviços, transporte, segurança de ida e volta do produto, ficam por conta e risco do consumidor.

4- A garantia ficará automaticamente cancelada se o produto for violado, receber maus tratos ou sofrer danos decorrentes de acidentes, quedas, agentes da natureza (raios, inundações), variações de tensão elétrica, sobrecarga acima do especificado e instalação em desacordo com o manual.

LOCAL: _____

REVENDA: _____

DATA: _____

Importado por: Khronos Indústria, Comércio e Serviço em Eletrônica LTDA. CNPJ 78.323.094/0004-70.

Fabricante:
DONGGUAN ZKTECO
ELECTRONIC
TECHNOLOGY CO., LTD.
PINGSHAN 188 INDUSTRY
ZONE 26 TANGXIA TOWN
DONGGUAN - CHINA



Informações e suporte técnico do produto:

www.cs.ind.br suporte@cs.ind.br

CS COMUNICAÇÃO E SEGURANÇA

Fone: +55 (48) 3246-8563



02.009.030.035.04

A CS Comunicação e Segurança fornece este documento no estado em que se encontra, não oferecendo nenhuma garantia quanto à precisão das informações fornecidas e se exime de qualquer responsabilidade por danos e prejuízos resultantes do seu uso.