

MODELO MA300



<http://www.newello.com.br/>

Índice

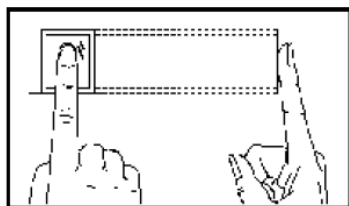
1	Instruções para Uso (Digitais e Cartões)	1
1.1	Posicionamento dos Dedos	1
1.2	Instruções para uso do cartão	2
1.3	Precauções	2
2	Introdução ao Dispositivo	2
2.1	Visão Geral das Funções	2
2.2	A aparência do produto	3
2.3	Utilização de um teclado externo USB	5
2.4	Estado de verificação	5
2.5	Cartão de Gerenciamento	5
2.6	Senha do sistema	6
2.7	Operação de tempo limite	6
3	Operações de dispositivos	7
3.1	Cartão de gerenciamento	7
3.1.1	Registra cartão de gerenciamento	7
3.1.2	Cadastrar um usuário comum	8
3.1.3	Excluir um único usuário	12
3.2	Operações teclado USB	14
3.2.1	Teclado Senha	14
3.2.2	Registrar um usuário através do teclado	15
3.2.3	Excluir um usuário especificado	17
3.2.4	Excluir todos os usuários	19
3.2.5	Restaurar padrões de fábrica	19
3.2.6	Função de Controle de Acesso	20
3.3	Verificação do usuário	21
3.4	Pen-drive	23
3.5	Botão Tamper	24
4	Anexo	25
4.1	Lista dos parâmetros	25
4.2	Anti-Pass Back	25

1 Instruções para Uso (Digitais e Cartões)

1.1 Posicionamento dos Dedos

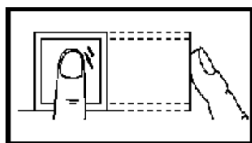
Os dedos mais recomendados são o Indicador, Anelar e dedo médio, não é recomendado o uso do Polegar e dedo mínimo devido a posição “não confortável” durante a leitura, mas isto é apenas uma recomendação.

Posição Correta para cadastro

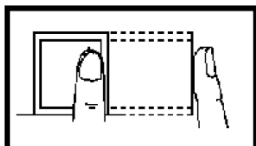


O DEDO DEVE ESTAR BEM CENTRALIZADO E COLADO A SUPERFÍCIE DE LEITURA PARA O CADASTRO MAIS CORRETO

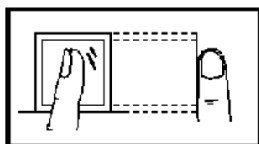
Posições Impróprias para cadastro



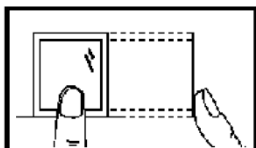
O DEDO NÃO ESTÁ COLADO A SUPERFÍCIE.



O DEDO NÃO ESTÁ CENTRALIZADO NA SUPERFÍCIE.



O DEDO ESTÁ POSICIONADO DE LADO.



O DEDO ESTÁ TOTALMENTE FORA DO CENTRO DA SUPERFÍCIE.

OBS: Recomendamos o Cadastro e uso das digitais na posição recomendada, isto auxilia a velocidade e assertividade do sistema.

1.2 Instruções para uso do cartão

O Dispositivo conta com um sensor de cartões de proximidade padrão 125 KHZ-EM e em alguns modelos o uso opcional do sensor padrão MI-FARE, este sistema de sensor permite apenas a aproximação do cartão a área de leitura e imediatamente o equipamento irá responder com o comando de voz, aceitando ou rejeitando ou alertando duplicidade, mais adiante iremos mostrar a forma de cadastro.

1.3 Precauções

É importante evitar a exposição direta a luz do SOL, que pode atrapalhar a coleta e verificações de leitura das digitais, o uso recomendado em termos de temperatura é entre 0 e 50° C, O uso externo pode acarretar um índice de FALSOS ACEITES, ou FALSOS REJEITES de acordo com as condições climáticas e de condensação.

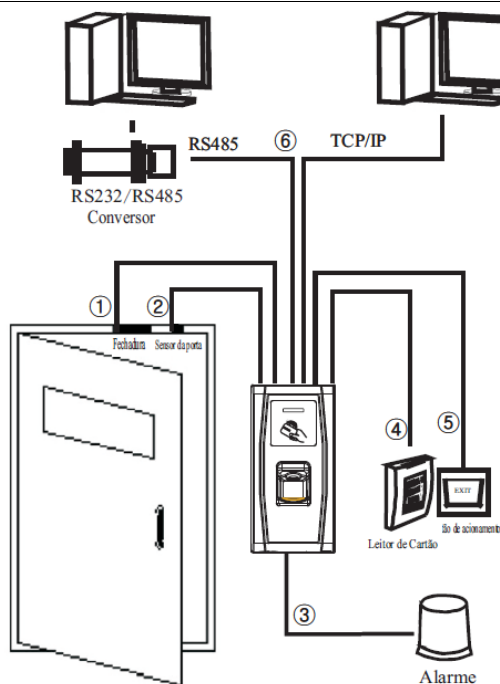
Recomenda-se a instalação do CABO DE ENERGIA (alimentação) apenas após realizar todas as ligações e proteções indicadas no esquema de ligações do produto. Quando estiver realizando a instalação do produto verifique as ligações elétricas existentes com ferramentas adequadas (multímetros) isto evitará descargas não cobertas pela garanti

2 Introdução ao Dispositivo

2.1 Visão Geral das Funções

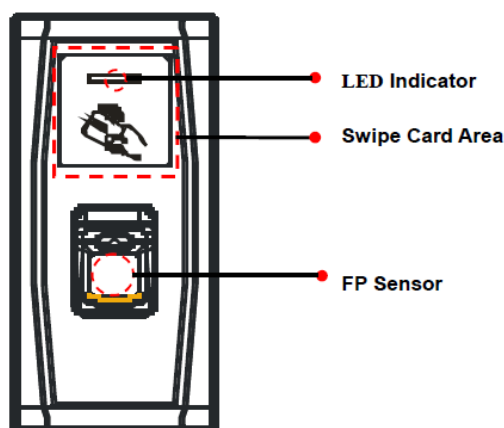
Como um dispositivo de impressão digital e controle de acesso integrado, o nosso produto pode controlar o acionamento de vários tipos de fechadura eletrônica, ou se comunicar com outros sistemas de acionamento. Este dispositivo possui operações simples e flexíveis, suportando o uso de cartão rf-id. Com um cartão de gerenciamento, você pode executar funções diretamente no aparelho como cadastramento e exclusão de usuários e backup via U-Disk. Os comandos de voz auxiliam através das operações sem o uso de Menu.

Este dispositivo permite que você conecte um teclado externo e oferece vários modos de operação, ele é direcionado para controle de acesso na gestão de segurança do local, e é compatível com várias formas de comunicação, seu design à prova d'água e caixa de metal permitem-lhe resistir a um forte impacto sem danos. Com um design compacto e simples, este dispositivo se comunica em rede para que seja realizado seu gerenciamento e monitoramento em tempo real.



2.2 A aparência do produto

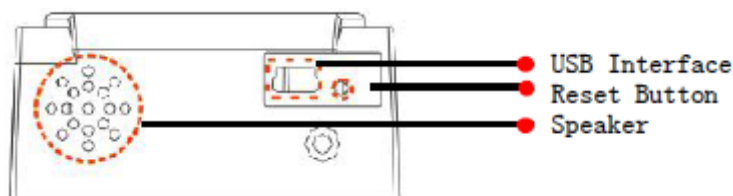
Vista Frontal:



- **Indicador LED:** O indicador LED é utilizado para apresentar resultados da operação do dispositivo e status excepcionais que são definidos da seguinte forma:
- **As regras comuns:** Se uma operação bem-sucedida, o indicador verde é ligado por um segundo; caso contrário, o indicador de vermelho é ligado durante um segundo.
- **Registro do usuário:** O LED verde pisca três vezes a cada um dos outros três segundos.
- **Exclusão única do usuário:** O LED vermelho pisca três vezes a cada um dos outros três segundos.
- **Estado de Verificação:** O LED verde pisca uma vez a cada dois segundos.
- **Área de cartão magnético:** Refere-se à área da caixa na linha tracejada vermelha com mostrado na figura acima.

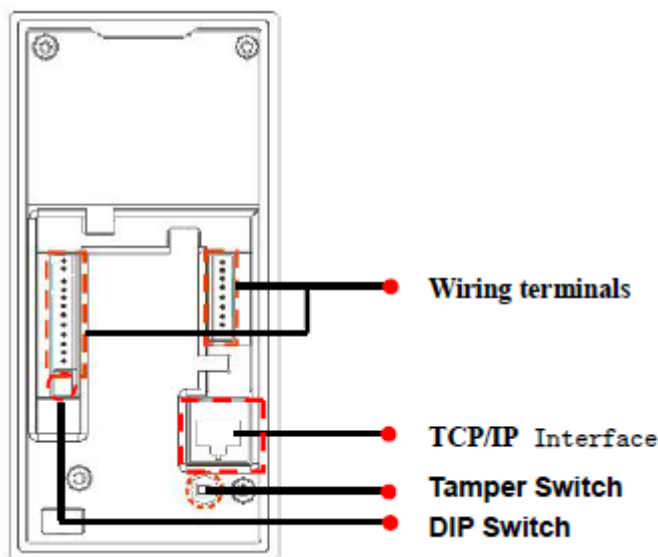
- **Sensor de impressão digital:** Usado para coletar e combinar as impressões digitais e excluir usuários.

Vista inferior:



- **Interface USB:** Usado para conectar com um pen drive ou um teclado.
- **Botão Reset:** Usado para reiniciar o dispositivo.
- **Alto-falante:** Usado para reproduzir o som de bipe e comandos de voz. Se um usuário passa a verificação, o alto-falante emite um sinal sonoro, se o usuário não consegue passar a verificação, o alto-falante emite dois sinais sonoros. O padrão pede durante a operação: bipe + VOZ.

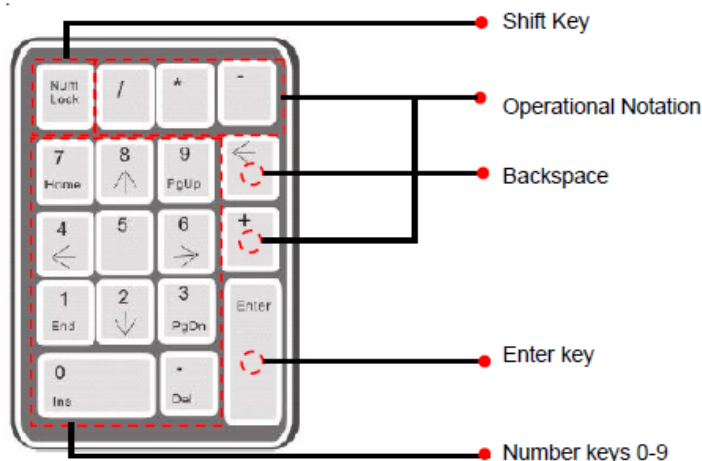
Vista traseira:



- **Terminal de fiação:** Conecta-se com fechaduras e fornecimento de energia através de Cabos.
- **Interface TCP/IP:** A interface TCP/IP se conecta com um PC através de um cabo de rede (para conexão detalhada, consulte o guia de instalação).
- **Interruptor de Tamper:** Usado para gerar um alarme de violação. Para mais detalhes, consulte [3.6 Tamper Switch](#).
- **DIP Switch:** O DIP tem quatro pinos numerados 1, 2, 3 e 4. Em um modo de comunicação RS485, o primeiro 1, 2 e 3 pinos são usados para definir número de dispositivo de hardware e o quarto pino é usado para selecionar o status de Resistência terminal. Para configurações detalhadas, consulte o guia de instalação.

2.3 Utilização de um teclado externo USB

Para facilitar as operações do dispositivo, você pode conectar o dispositivo com um externo Teclado USB (comprado pelos usuários) e convenientemente executar tais operações como registro de usuário, exclusão e restaurar padrões de fábrica, especialmente quando especificando IDs de usuário durante o registro do usuário e exclusão



Um teclado USB externo é mostrado acima (consulte o real produto). Num Lock é uma chave de alternância teclado numérico. Ele é ativado por padrão. Se for ativado, o indicador LED está ligado. Quando o dispositivo é ligado a um teclado externo, você só pode usar as teclas numéricas, tecla de retrocesso e Tecla enter no estado NumLock ativado.

2.4 Estado de verificação

Estado de verificação: Depois que o dispositivo estiver ligado, o dispositivo entra a verificação se você se inscreveu com sucesso ou se inscreve um cartão de gerenciamento ou em caso de timeout de qualquer operação. No estado de verificação, todos os usuários têm permissão para verificar sua identidade e desbloquear (o administrador tendo um cartão de gestão só pode desbloquear usando seu / sua impressão digital (s) inscrito anteriormente); o administrador pode realizar tal operações como inscrição/exclusão de usuário, gerenciamento de U-disco e teclado operação.

2.5 Cartão de Gerenciamento

Os usuários de dispositivos são classificados em administradores e usuários comuns.

Administradores: Um administrador tem permissão para executar todas as operações incluindo usuário inscrição/exclusão (excluindo todos os outros usuários exceto ele/ela) e gerenciamento de U-disco. Os privilégios dos administradores do dispositivo são implementados através dos cartões de gestão.

Usuários comuns: Usuários comuns só são permitidos para verificar sua identidade e desbloquear.

Um cartão de gerenciamento: é um cartão especialmente alocado para um super Administrador. Cada dispositivo deve pelo menos se registrar uma placa de gerenciamento. Se não há gestão cartão Registrado, Você não pode realizar qualquer operação, e o sistema irá gerar uma alerta da voz "□: Por favor, registre o cartão de gerenciamento".

Você pode implementar diferentes funções por passar um cartão de gerenciamento por diferentes vezes seguidas:

1. No U-disco ou teclado externo estiver ligado:

- Ao passar o cartão de gestão de uma vez, Você pode ir para o único usuário estado de registro.
- Ao passar o cartão de gestão de cinco vezes seguidas, você pode entrar no único estado de exclusão do usuário.

2. U-disk estiver conectado:

- Ao passar o cartão de gestão de uma vez, Você pode ir para o U-disco estado de gestão

3. Um teclado externo estiver conectado:

- Ao passar o cartão de gestão de uma vez, você pode ativar o teclado externo.

Passes consecutivos: Passes consecutivos significa o intervalo entre dois passes em uma fileira em menos de 5 segundos.

Os cartões de gestão podem ser apagados através da função " Limpar Tudo " do teclado, ou ter seus privilégios de administração apuradas através de software antes de serem eliminados como cartões de identificação comuns. Para mais detalhes, consulte o acesso manual do usuário do software de controle.

As impressões digitais do usuário que tem um cartão de gerenciamento podem ser inscritas através de software ou de inscrição teclado. Um dispositivo sem o cartão de gestão, se ele tem a senha do teclado, você pode ativar o teclado externo e registrar ou excluir usuários.

Observação: Os usuários que carregam placas de gestão só pode verificar a sua identidade e desbloquear usando suas impressões digitais previamente inscritos.

2.6 Senha do sistema

A senha do sistema é uma senha usada para aumentar a segurança de dados do dispositivo em RS485 ou comunicações TCP / IP.

Observação: A senha do sistema pode ser modificada através do software de controle de acesso. Para mais detalhes, consulte o manual do usuário do software de controle de acesso.

2.7 Operação de tempo limite

O tempo limite de operação padrão é de 30 segundos. Quando você registrar um cartão de gerenciamento ou de exclusão / registrar um usuário (incluindo o teclado externo inscrição e exclusão do usuário estados), o sistema solicita automaticamente uma vez que todos os outros 10 segundo, se não houver nenhuma operação e retorna para o estado de verificação após solicitando três vezes. O comando de voz é "□: Operação de tempo limite, O sistema retorna para o estado de verificação".

Observação: Você pode definir o tempo limite através do Software de controle de acesso.

3 Operações de dispositivos

3.1 Cartão de gerenciamento

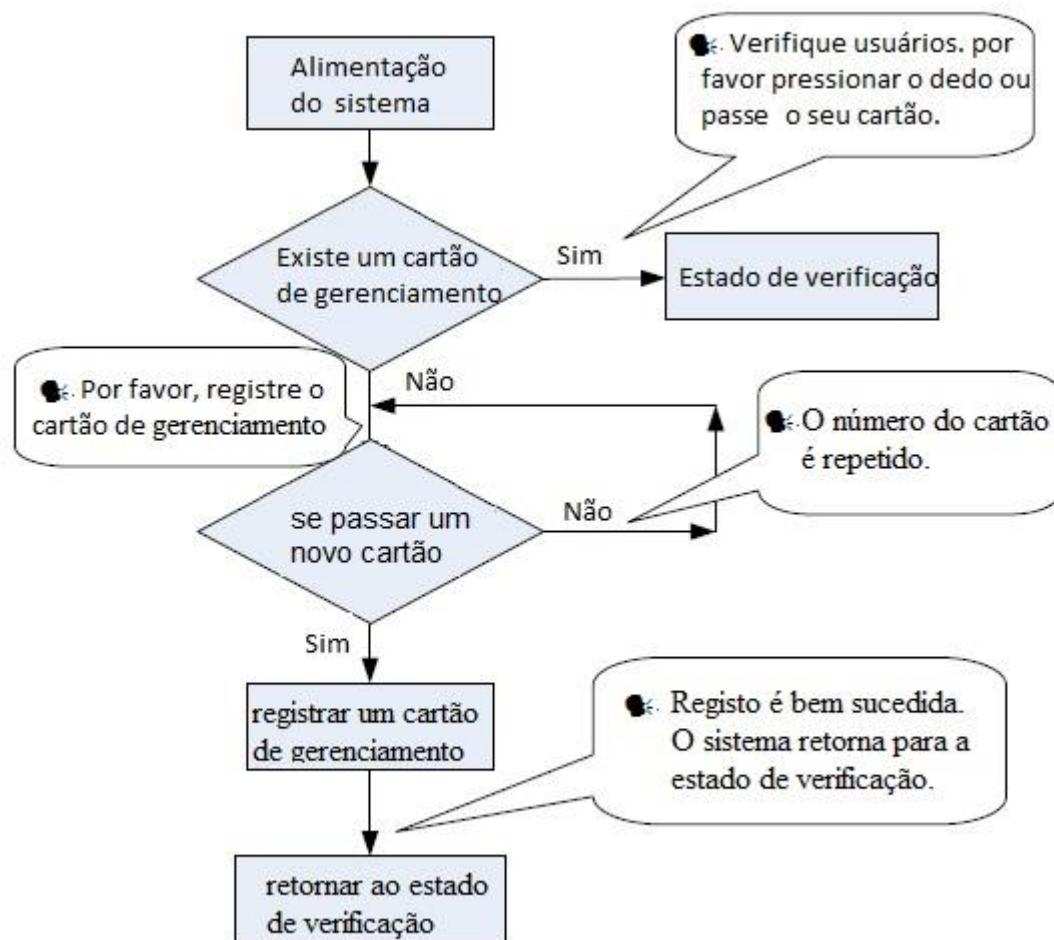
3.1.1 Registra cartão de gerenciamento

Para registrar um cartão de gerenciamento, proceda da seguinte forma:

1. O dispositivo detecta automaticamente se existe um gerenciamento de cartão.
2. Se o dispositivo não é possível detectar a presença de um cartão de gerenciamento, isto entra no estado de registro, de cartão de gestão. Em seguida, prossiga com o passo 3; caso contrário, o sistema gera a mensagem de voz “□: Verifique os usuários. Pressione seu dedo ou passe seu cartão”.
3. Depois que o sistema gera a mensagem de voz “□: Por favor, registre o cartão de gerenciamento”, você pode passar o cartão em toda a área do sensor.
4. Se o registrar falhar, o sistema gera a mensagem de voz “□. Se a inscrição falhar, o sistema gera a mensagem de voz” e retorna para o passo 3 e retorna para o passo 3 o sistema gera a mensagem de voz “□:Registro é bem-sucedido. O sistema retorna para o estado de verificação”.

Observação: O sistema retorna para o estado de verificação se qualquer operação no passo 3 vezes estiver fora e apenas pede-lhe para se inscrever o cartão de gerenciamento novamente depois de reiniciar o dispositivo novamente

O fluxo de registro de cartão de gerenciamento é mostrado abaixo:



3.1.2 Cadastrar um usuário comum

O modo de você entrar no estado de registro usando o gerenciamento de cartão é conhecido como o modo de registro de cartão de gerenciamento. Neste modo, você só pode registrar um usuário. Quando você registrar um novo usuário, o sistema atribui automaticamente um mínimo ID para o usuário. Além disso, Também é possível usar o modo de registro teclado externo (Para mais detalhes, consulte 3.2.2 inscrever um utilizador através do teclado) para implementar o registro de usuário ID especificado.

Em ambos estes dois modos de registro, você pode se registro novos usuários. Cada usuário é permitido a registrar de 10 impressões digitais e um cartão de identificação, no máximo. Para inscrever um utilizador, proceda da seguinte forma:

1. No estado de verificação, o sistema vai para o usuário comum de registro depois de passar um cartão de gerenciamento de uma vez (No estado de registro, passar um cartão de gerenciamento de uma vez, você voltará para o estado de verificação).
2. Depois que o sistema gera a mensagem de voz "□: Registrar usuários. Por favor, pressione o dedo ou com um soco o seu cartão ", você pode começar registrar usuários. Há dois casos a seguir:



(1) Cartão magnético ID primeiro

a. Quando você passar o novo cartão de identificação e ter sucesso em se registrar um usuário, o dispositivo irá gerar uma mensagem de voz “□: número de usuários **. Registro é sucesso!” (** refere-se à identificação atribuído automaticamente ao utilizador pelo sistema; mesmo abaixo) e você pode prosseguir para a etapa **b.** se você passar um cartão de identificação inscritos, o sistema gera a mensagem de voz “□: usuário número ** Registrar. Por favor, pressione o dedo! "E digite o usuário.

b. Depois que o dispositivo gera o comando de voz “□: Registrar. Por favor pressionar o dedo ", o sistema entra no registro da impressão digital especificada Estado. Pressione o mesmo dedo sobre o sensor três vezes após a comandos de voz.

c. Se o registro de impressões digitais é bem-sucedida, o sistema gera a voz imediato “□: Registro é bem sucedida. Registrar. Por favor, pressione o Dedo "e entra diretamente o próximo estado registro de impressões digitais; se registro da impressão digital falhar, o sistema gera a mensagem de voz “□: A impressão digital é repetido "e repete o passo b.

d. O sistema retorna automaticamente para o estado de verificação quando ambos 10 dedos e cartão de identificação estão registro, ou o cartão de gestão é passado uma vez ou operação expira.

(2) Impressão do primeiro dedo.

a. Pressione o mesmo dedo sobre o sensor três vezes seguindo a voz solicita ao adotar a colocação da impressão digital adequada. Se registro da impressão digital é bem-sucedida, o sistema gera a mensagem de voz “□: Número de usuários **. Registro é bem-sucedida "e você pode avançar para o passo b.

b. se a impressão digital registrada antes, o sistema gera a mensagem de voz “□: Número de usuários **, Registre, por favor, pressione o dedo ou com o seu cartão "e entrar no estado de registro usuário especificado. b. Depois de gerar o comando de voz “□: Registrar. Por favor, pressione o dedo ou passe o seu cartão ", o sistema entra com usuário especificado com registro informações, esperando por você para passar o novo cartão de identificação ou pressionar o dedo.

c. Se o registro do cartão de identificação bem-sucedida, o sistema gera a voz imediato “□: Registo é bem sucedida. Por favor, pressione o dedo "e entra no estado de registro da impressão digital diretamente; se você pressionar um dedo que não é registrado antes e consegue no registro deste dedo, o sistema gera o comando de voz: “□Registo é bem sucedida. Por favor, pressione o dedo ou passe seu cartão ", e você pode continuar registrando novo impressões digitais e cartão. Depois de inscrever 10 impressões digitais, o sistema gerar o comando de voz “□Por favor, passe o seu cartão "para inscrever o seu ID cartão se o seu cartão de identificação não está registrado.

d. O sistema retorna automaticamente para o estado de verificação quando ambos 10 dedos e cartão de identificação estão registrados, ou o cartão de gestão é passado uma vez ou operação expira.

3. Se você já está atribuído com um número de usuário, em seguida, há os dois casos seguintes:

(1) Registrar a impressão digital (s) quando você já tiver cartão de registrados.

a. Depois de passar o cartão registrado, o sistema irá gerar a voz imediato “□: Número do usuário. ** Registrar. Por favor, pressione o dedo "(** refere-se para o ID que lhe foi atribuído; mesmo abaixo) e entre a impressão digital estado de registro.

b. Pressione o mesmo dedo sobre o sensor três vezes seguindo a voz solicita ao adotar a colocação da impressão digital adequada. Se impressão digital inscrição bem-sucedida, o sistema gera a mensagem de voz “□: Número do usuário**. Registo é bem-sucedido "e se prepara para o registro da impressão digital.

c. O sistema retorna automaticamente para o estado de verificação quando ambos 10 dedos e cartão de identificação estão registrados, ou o cartão de gestão é passado uma vez ou operação expira.

• Observação:

1) Se o usuário registrar uma impressão digital e que repetir com o seu próprio registro impressão digital, a nova irá substituir a impressão digital previamente registrado.

2) Nesse modo, a impressão digital do usuário que tem a gestão cartão não pode ser registrado porque passar o cartão de gestão vai retornar o sistema ao estado de verificação automaticamente.

3) cartão e impressão digital (s) quando você já se registrou impressão digital (s)

a. Pressione o dedo com a impressão digital já registrado três vezes seguinte os comandos de voz. Se você está identificado como a mesma pessoa em cada um da tentativa de verificação, o sistema entra no estado de registro de impressões digitais.

b. Depois de gerar o comando de voz “□: Número do usuário. ** Registrar. Por favor, pressione o dedo ou passe o seu cartão ", o sistema começa a registrar sua impressão digital.

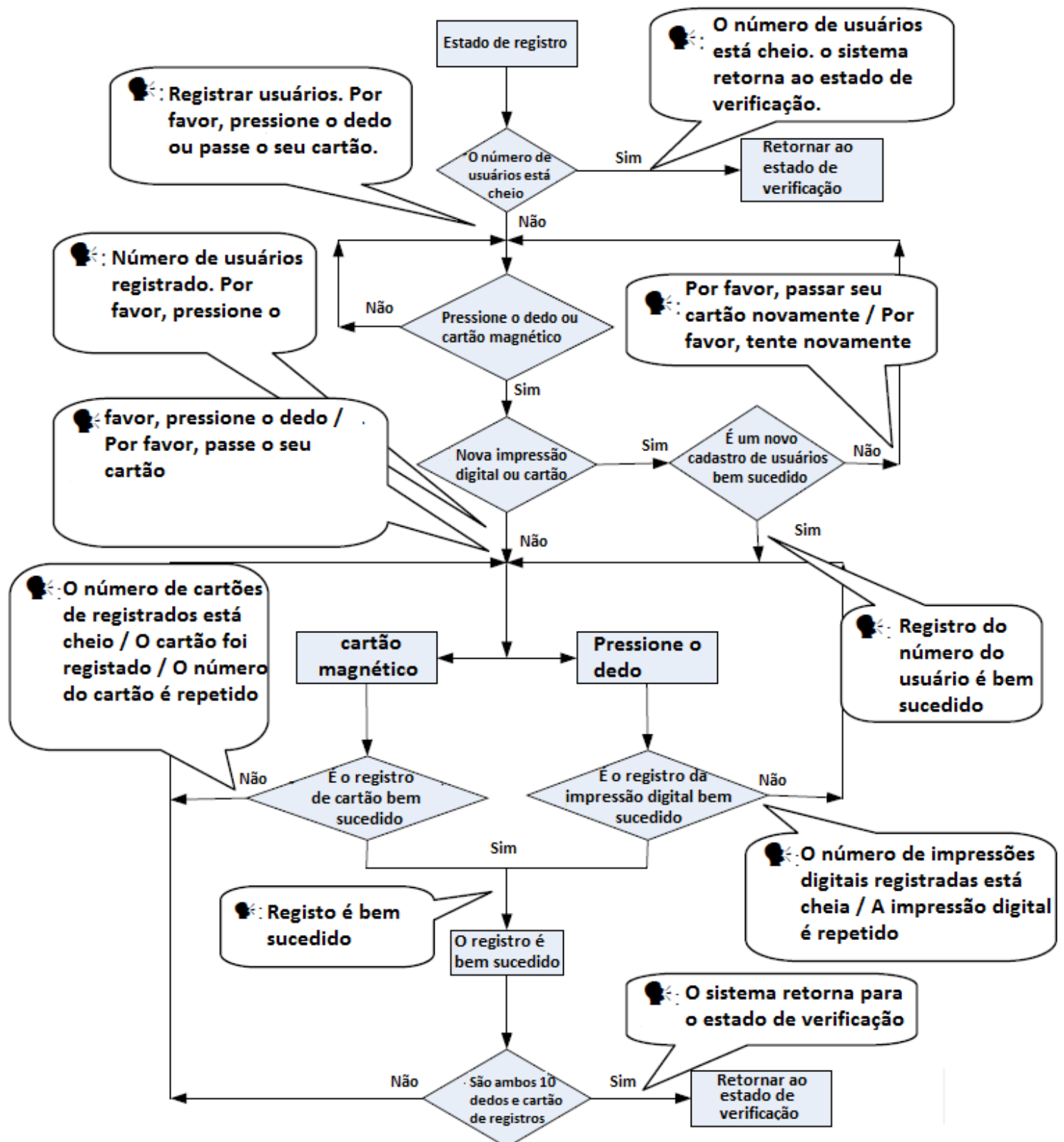
c. Se o registro do cartão de identificação bem-sucedida, o sistema gera a voz imediato “□: Registo é bem sucedido. Registrar. Por favor, pressione o Dedo "e entra no estado de registro da impressão digital diretamente; se você pressionar um dedo que não está registrado e consegue registrado deste dedo, o sistema gera a mensagem de voz “□: Registo é bem sucedido. Por favor, pressione o dedo ou com o seu cartão ", e você pode continuar registrando novas impressões digitais e cartão. Depois de registrar 10 impressões digitais, o sistema irá gerar o comando de voz “□: Por favor, passar o seu

cartão "para inscrever o seu cartão de identificação, se o seu cartão de identificação não está registrado.

d. O sistema retorna automaticamente para o estado de verificação quando ambos 10 dedos e cartão de

e. Identificação estão registrados, ou o cartão de gestão é passado uma vez ou operação expira.

O fluxograma é mostrado abaixo:

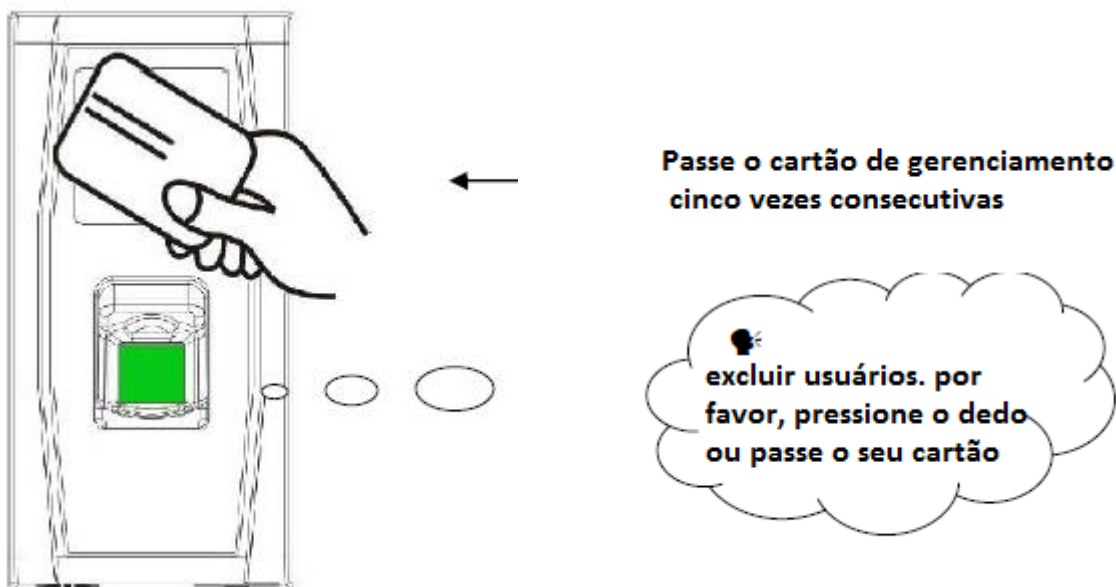


3.1.3 Excluir um único usuário

A exclusão de um usuário usando um cartão de gerenciamento é chamado de simples modo de eliminação de usuário único. A exclusão de um usuário usando um externo teclado é chamado o modo de exclusão do usuário especificado. (Veja 3.2.3 Excluir um usuário específico).

As etapas da operação de simples eliminação de um único usuário:

1. No estado de verificação, passar o cartão de gerenciamento para cinco vezes consecutivo para entrar no estado de simples eliminação de um único usuário (passe com o um cartão mais tempo a regressar ao estado de verificação). No estado de verificação, passar o cartão de gerenciamento para cinco vezes consecutivo para entrar no usuário (passe com o um cartão mais tempo a regressar ao estado de verificação).



2. O sistema irá gerar o comando de voz "□: Excluir usuários. Por favor pressione o dedo ou passe o seu cartão.

3. Pressione o dedo no sensor de impressão digital ou passar o cartão no leitor de cartão.

(1) Pressione o dedo no sensor para excluir um usuário.

Pressione um dos vossos dedos registrados adequadamente no sensor. Se a verificação for bem sucedida, o sistema irá gerar o comando de voz "□: Número do usuário. ** Exclusão é bem sucedida. Excluir usuários. Por favor, pressione o dedo ou passe o seu cartão. "(** indica que o número de identificação do usuário) e volta automaticamente ao estado de exclusão. Se a verificação falhar, o sistema irá gerar o comando de voz "□: "Por favor, tente novamente"

(2) Passe o cartão sobre o leitor para excluir um usuário.

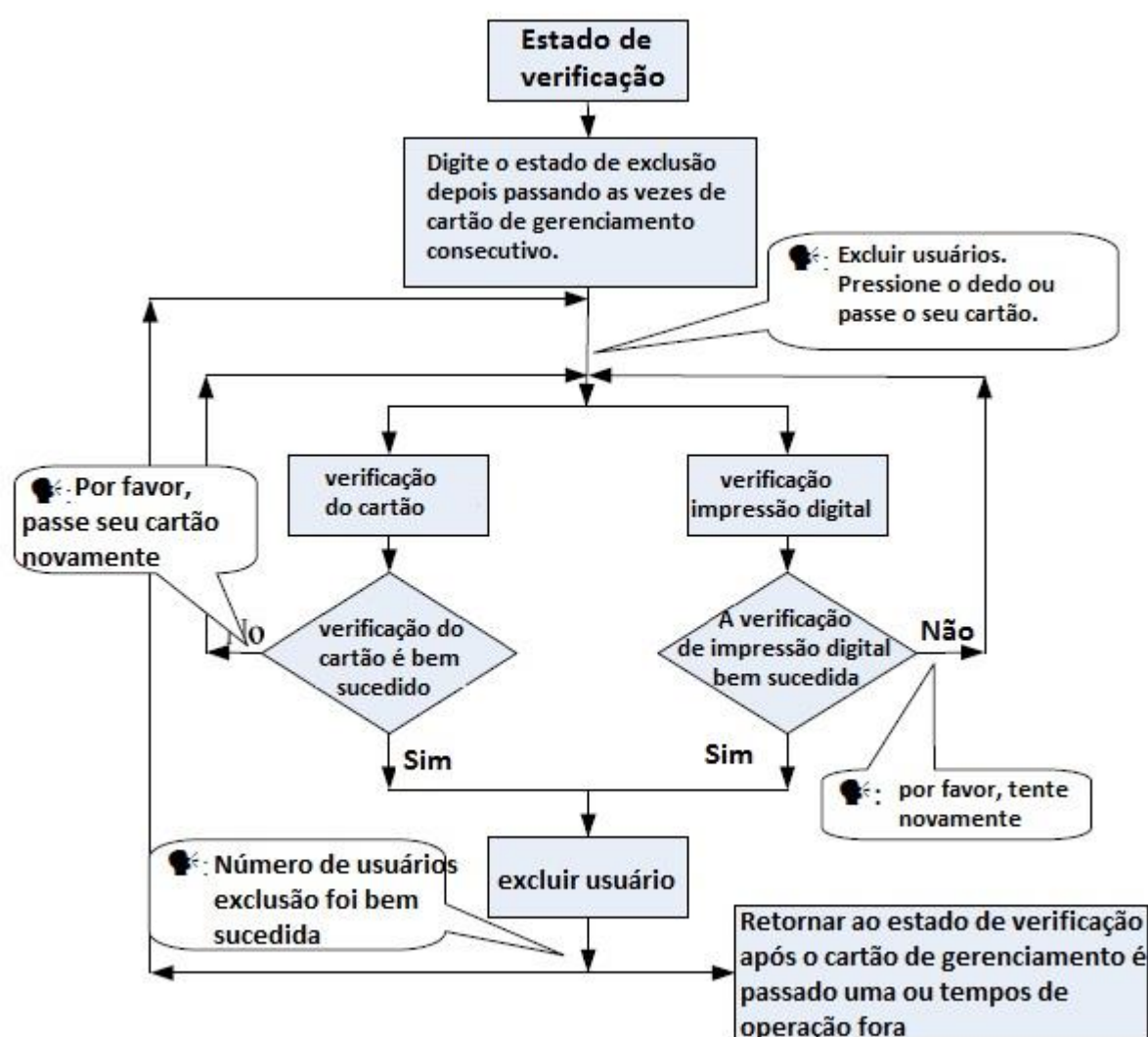
Passe um cartão registrado sobre o leitor. Se a verificação for bem sucedida, o sistema irá gerar o comando de voz "□: número do usuário. ** A exclusão é bem sucedida. Excluir usuários. Por favor, pressione o dedo ou passar o cartão. " e retornar automaticamente para o estado de exclusão. Se a verificação falhar, o sistema irá gerar o comando de voz "□: Por favor passe o seu cartão novamente. "

4. Se você passar o cartão de gerenciamento mais de um tempo ou o seu funcionamento vezes para fora, o sistema irá retornar ao estado de verificação.

Em simples de usuário único modo de eliminação, cartão de gerenciamento os usuários não pode ser excluído porque passar o cartão de gerenciamento vai retornar o sistema ao estado de verificação.

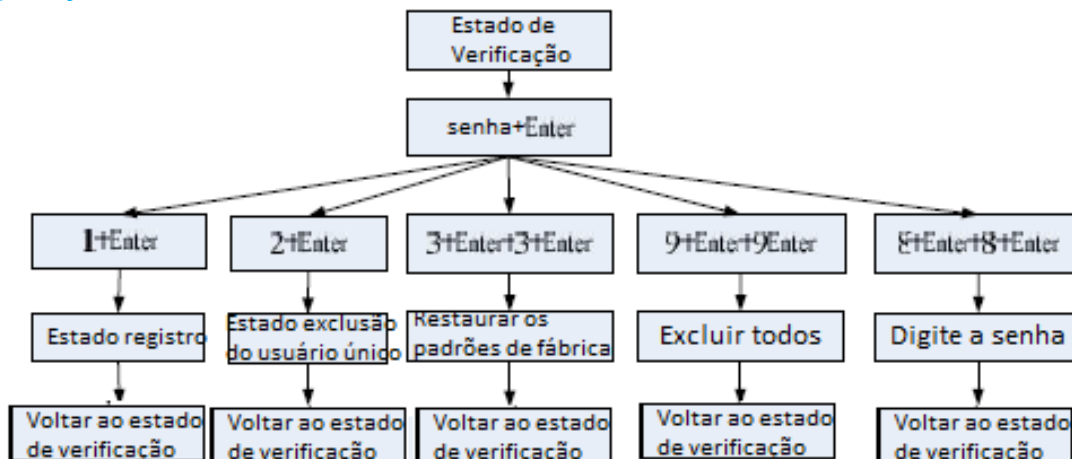
- **Nota:** Em simples de usuário único modo de eliminação, cartão de gerenciamento o usuário não pode ser excluído porque passar o cartão de gerenciamento vai retornar o sistema ao estado de verificação.

Simple-Procedimento de exclusão único usuário



3.2 Operações teclado USB

O fluxograma operações do teclado é mostrado abaixo:



3.2.1 Teclado Senha

Se o usuário precisar de um teclado externo, ele / ela pode conectar o teclado para o dispositivo e, em seguida, passar o cartão de gerenciamento para ativar o teclado externo. O sistema permite que o usuário defina uma senha específica para o teclado externo.

Etapas de operações

1. No estado de verificação, conectar um teclado externo com o dispositivo através da interface USB.
2. Passe o cartão de gerenciamento uma vez para ativar o teclado. O sistema gera a mensagem de voz "□□Por favor, pressione o teclado".
3. Digite "8" e pressione Enter. Em seguida, digite "8" e pressione Enter novamente. O sistema gera o comando de voz "□: Por favor, defina a senha. "Tipo em sua senha desejada e pressione Enter. O sistema gera o comando de voz "□: A operação é bem sucedida. O sistema retorna ao estado de verificação. "Se não há pressionamento de teclas dentro de 30 segundos, o sistema irá gerar o comando de voz "□ Tempo limite de operação. O sistema retorna ao estado de verificação ". (A senha deve ter entre 4 e 6 dígitos.) O usuário pode digitar essa senha para ativar as funções do teclado externo na próxima utilização, ou passar um cartão de gerenciamento uma vez (o que é obrigatória para o primeiro uso do teclado externo).



1. Se você digitar uma senha errada por seis vezes consecutivas, o teclado será bloqueado e você terá que ligar o teclado novamente para desbloqueá-lo.
2. Se não há pressionamento de teclas dentro de 3 segundos, após o teclado é ativado, as funções do teclado serão desativadas automaticamente e você terá que reativá-lo.
3. O teclado deve ser inserido ou removido em um intervalo de mais de 15 segundos, caso contrário o sistema não consegue identificar o seu estado.

3.2.2 Registrar um usuário através do teclado

Registrando um usuário usando um teclado USB é chamado de base de teclado modo de inscrição. Neste modo, o usuário pode registrar um usuário com o especificado ID de usuário.

Etapas de operações

1. Conforme mostrado na 3.2 Operações teclado USB fluxograma, digite "1" e pressione Enter para entrar no estado de registro.
2. Quando o sistema gera a mensagem de voz Registrar usuários. Por favor coloque o número do usuário. ", Digite um ID de usuário.
3. O sistema gera a mensagem de voz "□: Número do usuário. ** registrar usuários. Por favor, pressione o dedo ou passe o seu cartão "(** indica que o número de identificação do usuário; mesmo abaixo) O sistema entra o ID especificado estado inscrição.

- **Nota:**

(1) Se um usuário tiver registrado no sistema com um cartão de gerenciamento, o sistema irá gerar o comando de voz "□: Número do usuário. ** Por favor, pressione seu dedo. "

(2) Se um usuário tiver registrado no sistema com um ID do usuário e 10 impressões digitais, o sistema irá gerar o comando de voz "□□Número do usuário. ** por favor passe o seu cartão.

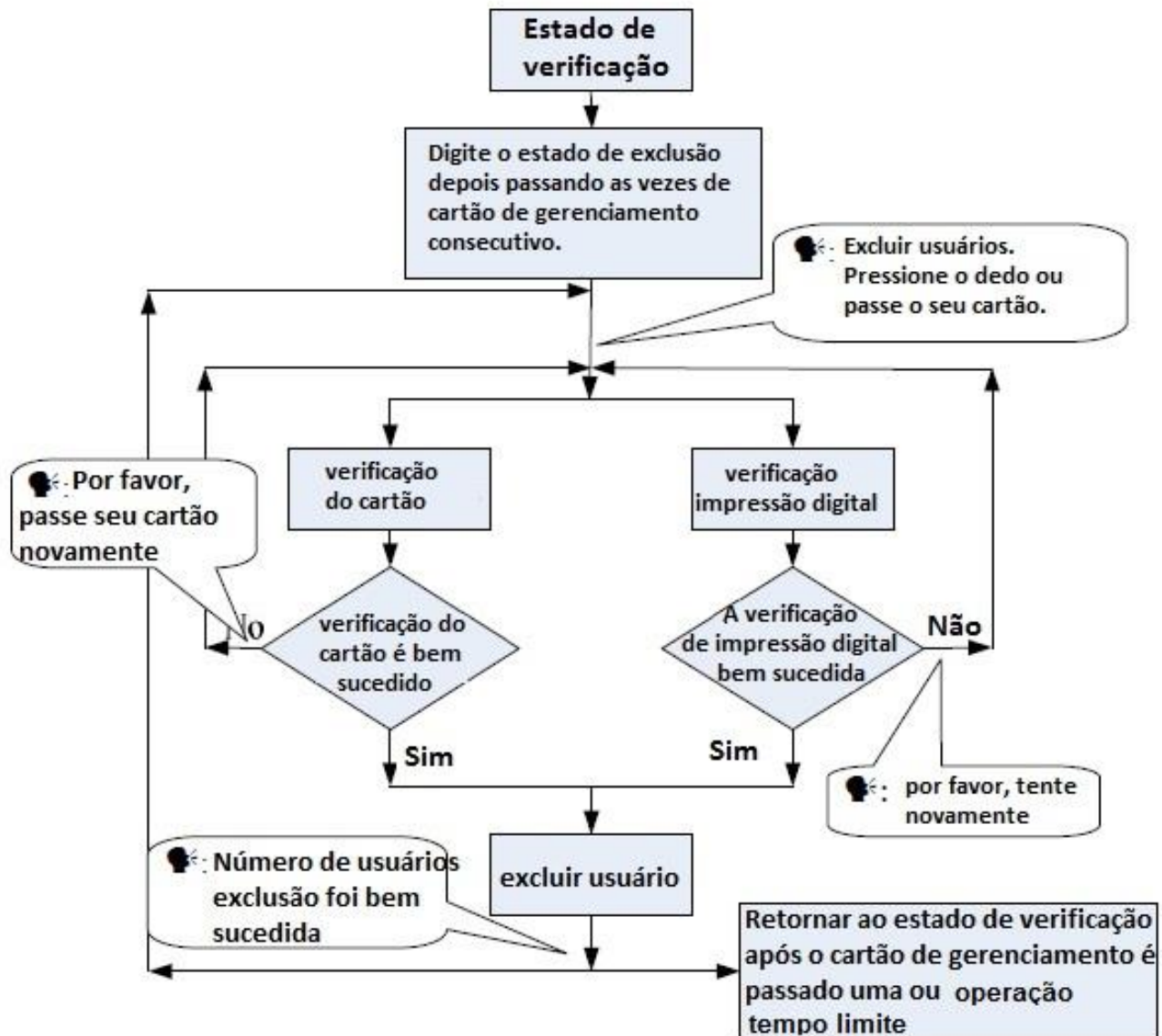
"4. A operação usuário registrado no estado inscrição ID especificado é semelhante à operação ID registrar especificado no cartão de inscrição de gerenciamento modo. Para mais detalhes, consulte 3.1.2 Cadastrar um usuário comum

5. No estado de espera registro ID de usuário, pressione ESC para retornar à estado de verificação. No estado de registro ID de usuário especificado, pressione ESC duas vezes para voltar para o estado de verificação.

- Nota:**

No modo de registro baseado teclado, você pode registrar usuários consecutivamente. Após o registro bem sucedido, o sistema retorna automaticamente para o Estado de registro.

O fluxograma de registro com base teclado é mostrado abaixo:





Declaração Importante:

1. No modo de registro baseado teclado, se houver tempos de operação para fora, o sistema solicita automaticamente desta operação uma vez que todos os outros 10 segundos e retorna ao estado após a verificação solicitando três vezes.
2. Impressões digitais recém-registrados irá substituir os originais em modo de registro de cartão de gerenciamento baseado, e o teclado baseado Modo de inscrição da mesma forma.
3. Um usuário só pode registrar um cartão. Quando o usuário com um cartão registrado no sistema, o sistema gera a mensagem de voz "□:Registrar. Por favor, pressione o dedo. "Quando o usuário passar o cartão, o sistema gera a mensagem de voz "□ "O cartão foi registrado. "
4. Um cartão não pode ser registrado de maneira repetitiva, caso contrário, o sistema irá gerar o comando de voz "□: O número do cartão é repetido. "Durante a passagem do cartão. Diferentes usuários não pode registrar a mesma impressão digital, caso contrário, o sistema irá gerar o comando de voz "□:A impressão digital é repetido. "durante o registro de impressões digitais. Novas impressões digitais de um usuário vai substituir os já existentes.



A diferença entre os dois modos de registro do utilizador no que diz respeito à inscrição estado de saída:

1. No cartão de registro com base modo gerenciamento com um ID de usuário especificado, o sistema retorna ao estado de verificação depois de passar o cartão uma vez.
2. No modo de registro com base teclado com um ID de usuário especificado, quando você pressiona ESC, o sistema retorna ao estado de registro e gera o comando de voz "🔊 Registrar usuários. Por favor coloque o número do usuário. "Você pode registrar um ID de usuário e pressione ESC. Em seguida, o sistema gera a mensagem de voz "🔊 O sistema retorna a verificação do estado. "

3.2.3 Excluir um usuário especificado

A exclusão de um usuário usando um teclado externo é chamado o especificado modo de exclusão do usuário.

Passos das operações:

1. Conecte um teclado USB para o dispositivo, e passe seu cartão de gerenciamento uma vez ou digite a sua senha para ativar o teclado
2. Pressione "2" e Enter para entrar no modo de exclusão do usuário especificado. O sistema irá gerar o comando de voz."□: Excluir usuários. Por favor coloque o número do usuário. "e você pode avançar para o passo 3.

- **Atenção:** Caso especial: Se não houver nenhum usuário (incluem usuário do cartão de gerenciamento) inscritos, e você tem a senha do teclado, você pode usar a senha para ativar o teclado e pressione 2 e Enter para entrar no estado exclusão do usuário, o sistema irá gerar o comando de voz "□: Não utilizador registrado. O sistema retorna para o estado de verificação".

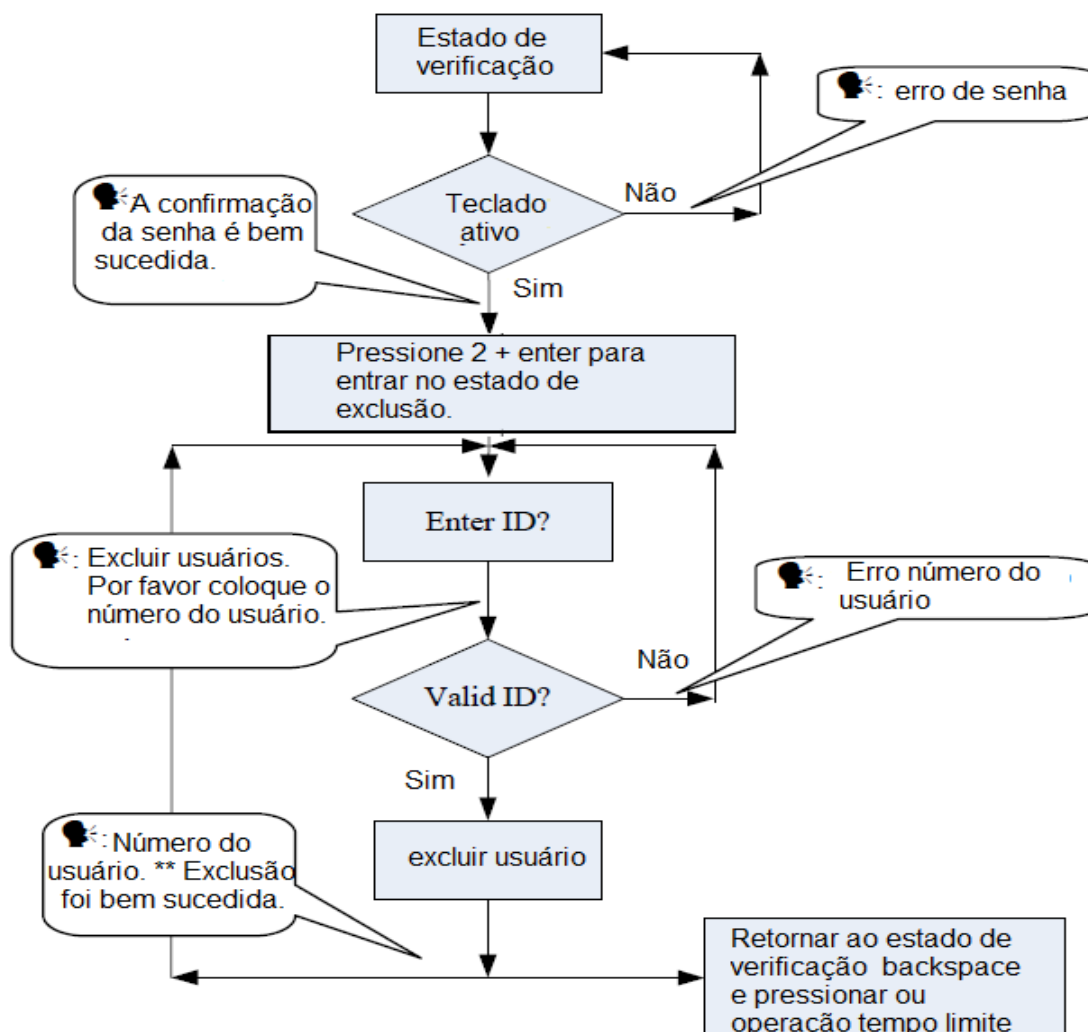
3. Digite um ID de usuário e o sistema verifica se o ID do usuário é válido.

4. Se o ID do usuário é válido, o sistema irá gerar o comando de voz "□: Número do usuário. ** Exclusão é bem sucedida. Excluir usuários. Por favor coloque o número do usuário. "e automaticamente retornar ao estado de exclusão. Se o ID do usuário é inválido, o sistema irá gerar o comando de voz "□: ID de usuário errado. "6. Se você pressionar ESC ou seus tempos de operação para fora, o sistema irá retornar ao o estado de verificação.

- **Nota:**

- 1) No modo de exclusão do usuário especificado, IDs de usuário e usuário de cartão de gerenciamento IDs que estão registrados no sistema são todos considerados inválidos.
- 2) No modo de exclusão baseado em teclado, o sistema desativar a impressão digital sensor e leitor de cartão e, portanto, qualquer operação sobre eles é inválida.

O fluxograma a exclusão usuário especificado é mostrado abaixo:



3.2.4 Excluir todos os usuários.

Etapas de operações

1. Conecte um teclado USB ao o dispositivo, e passe seu cartão de gerenciamento uma vez ou digite a sua senha para ativar o teclado.
2. Pressione "9" e Enter. Em seguida, pressione "9" e Enter novamente. o sistema exclui todos os usuários.
3. Se a operação for bem sucedida, o sistema irá gerar o comando de voz "□: Excluir todos os usuários. A operação é bem sucedida. O sistema retorna ao estado de verificação. Por favor, registre o cartão de gestão. "

- **Nota:**

- 1) Você pode excluir um cartão de gerenciamento usando o Excluir Todos função.
- 2) Você pode usar a função Apagar para apagar todos os usuários inscritos, impressões digitais e registros.
- 3) O cuidado extremo deve ser exercido durante a realização desta operação, como uma vez excluídos, os dados não podem ser recuperados.

3.2.5 Restaurar padrões de fábrica

Etapas de operações

1. Conecte um teclado USB ao o dispositivo, e passe seu cartão de gerenciamento uma vez ou digite a sua senha para ativar o teclado.
2. Pressione "3" e Enter. Em seguida, pressione "3" e Enter novamente. O sistema restaura os padrões de fábrica.
3. Após a operação for bem sucedida, o sistema gera a mensagem de voz "□: Restaurar para configurações padrão. A operação é bem sucedida. O sistema retorna ao estado de verificação ". Você também pode restaurar os padrões de fábrica, redefinindo o tamper. [Veja 3.6 Tamper Switch](#). Depois que o dispositivo é restaurado para os padrões de fábrica, as informações do dispositivo é restauradas para os padrões de fábrica, incluindo o número do dispositivo, o sistema de senha, endereço de IP, 485 endereço e senha do teclado.

Nota: As informações do usuário armazenadas no dispositivo não serão apagadas depois o dispositivo é restaurado ao os padrões de fábrica.

3.2.6 Função de Controle de Acesso

Configuração de controle de acesso é aberta para definir fuso horário porta do usuário, controle de bloqueio e parâmetros do dispositivo relacionado.

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

1. O atual Horário de desbloqueio deve ser em tempo real do usuário zona horária ou grupo zona.
2. O grupo onde é utilizador deve estar em controle de acesso (ou no mesmo controle de acesso com outro grupo, para abrir a porta em conjunto).

O sistema padrão, o novo usuário inscrito como o primeiro grupo, o grupo padrão fuso horário 1, controle de acesso, como o primeiro grupo, e os novos registrados usuário está em desbloqueio (O usuário pode modificar a configuração relacionada de controle de acesso, através de um software de controle de acesso).

Atenção: A função de controle de acesso de dispositivo necessário definir e modificar através do software de controle de acesso, para o detalhe, por favor consulte o manual do usuário do software.

Função de Controle de Acesso:

1. Controle de Acesso Tempo horário:

Tempo horário é a unidade mínima de opção de controle de acesso. o conjunto sistema pode definir 50 tempos horários. Cada tempo horário define sete vezes seções (ou seja, uma semana). Cada seção de tempo é o tempo horário eficaz dentro de 24 horas todos os dias. Cada usuário pode definir três tempos horários. "Ou" existe entre as três zonas. É eficaz se apenas um está satisfeito.

2. Acesse Configuração de Feriado:

Tempo de controle de acesso especial pode precisar durante o feriado. É diferente modificar o tempo de controle de acesso de todos. Assim, um tempo de controle de acesso de férias pode ser definido, que é aplicável para todos os funcionários.

3. Grupo de Acesso tempo horário:

Agrupamento é gerenciar os funcionários em grupos. Empregado em grupos usam grupo zona horária por padrão. Os membros do grupo também pode definir o tempo horário do usuário. Cada grupo pode segurar lá fusos horários. O novo usuário registrado pertence Grupo 1, por padrão, e também podem ser alocados a outros grupos.

4. Desbloquear Combinação Ambiente:

Faça vários grupos em diferentes controles de acesso para alcançar multi-verificação e melhorar a segurança. Um controle de acesso pode ser feito de 5 grupos de, no máximo.

5. Parâmetros de controle de acesso:

Bloqueio de Controle de atraso: Aplicar para determinar desbloqueio hora, os minutos medidos unidade é de 20 ms, na condição normal é 100-200 ms.

Modo Anti-Pass-Back Pode ser definido como "None", "Out", "In", "InOut".

Estado registro do Mestre: Pode ser definido como "None", "Out", "In".

Modo Sensor: Definir Modo Sensor porta. Ele pode ser definido como "None", "NA", Estado "NC".

Sensor de atraso: Defina o tempo de atraso do sensor quando a porta é aberta. Após este tempo definido o sensor detecta a porta. Se a porta não é coerente o alarme será disparado. Preto e branco dispositivo de tela Intervalo é 0-254. Faixa de dispositivo de tela colorida é 0-99.

Sensor de alarme: Definir o tempo de atraso de alarme após o alarme é acionado. O alcance é de 0-999 segundos.

Tempos de erro para o alarme: Definir os tempos de erro máximo para acionar o alarme. Quando a verificar não é através de e exceder este horário definido, o sinal de alarme será acionado automaticamente.

6. Configuração Anti-Passe back:

Anti-Pass back function please refer to 4.2 Anti-Pass back.

7. Desativar o alarme:

Quando o dispositivo está no estado de alarme, verificação do usuário pode desativar o alarme e o dispositivo irá recuperar o estado normal. Se não, ele vai alarme todo o tempo.

Os tipos de alarme: alarme sensor de porta e alarme de violação.

3.3 Verificação do usuário

A verificação padrão do dispositivo é a verificação de PF / RF, o usuário pode usar o software de controle de acesso para modificar o modo de verificar a RF, FP ou RF e PF verificação. Para mais detalhes, consulte o manual do usuário do software.

Etapas de operações

Quando o dispositivo está no estado de controle, o sistema gera a voz imediato □: Verifique usuários. Por favor, pressione o dedo ou passe o seu cartão. "2. Comece verificação do usuário. O dispositivo suporta os modos quatro verificações: FP / RF, FP, RF e PF e verificação de RF.

(1) verificação de impressão digital

Pressione o dedo no sensor de impressão digital de forma adequada. Se o verificação for bem sucedida, o sistema gera a mensagem de voz □: Número do usuário **. Obrigado. "E ao mesmo tempo aciona um sinal de desbloqueio. Se a verificação falhar, o sistema gera a mensagem de voz □□por favor tente novamente. "

(2) verificação do cartão

Passe o cartão através do leitor de cartão. Se a verificação for bem sucedida, o sistema gera a mensagem de voz □: Número do usuário. ** Obrigado. "e ao mesmo tempo aciona um sinal de desbloqueio. Se a verificação falhar, o sistema gera a mensagem de voz □: Por favor, passe o cartão de novo. "

(3) impressão digital + verificação do cartão

Defina o modo de verificação do usuário para FP & RF com controle de acesso software, a operação de verificação da seguinte forma:

Pressione dedo primeiro:

Pressione o dedo no sensor de impressão digital de forma adequada. Se a verificação for bem

sucedida, o sistema gera a mensagem de voz "□: Número do usuário **, por favor, passe o seu cartão. "após verificação do cartão de sucesso, e ao mesmo tempo aciona um sinal de desbloqueio. Se a verificação falhar, o sistema gera a mensagem de voz "□: Por favor, passe o cartão de novo. "

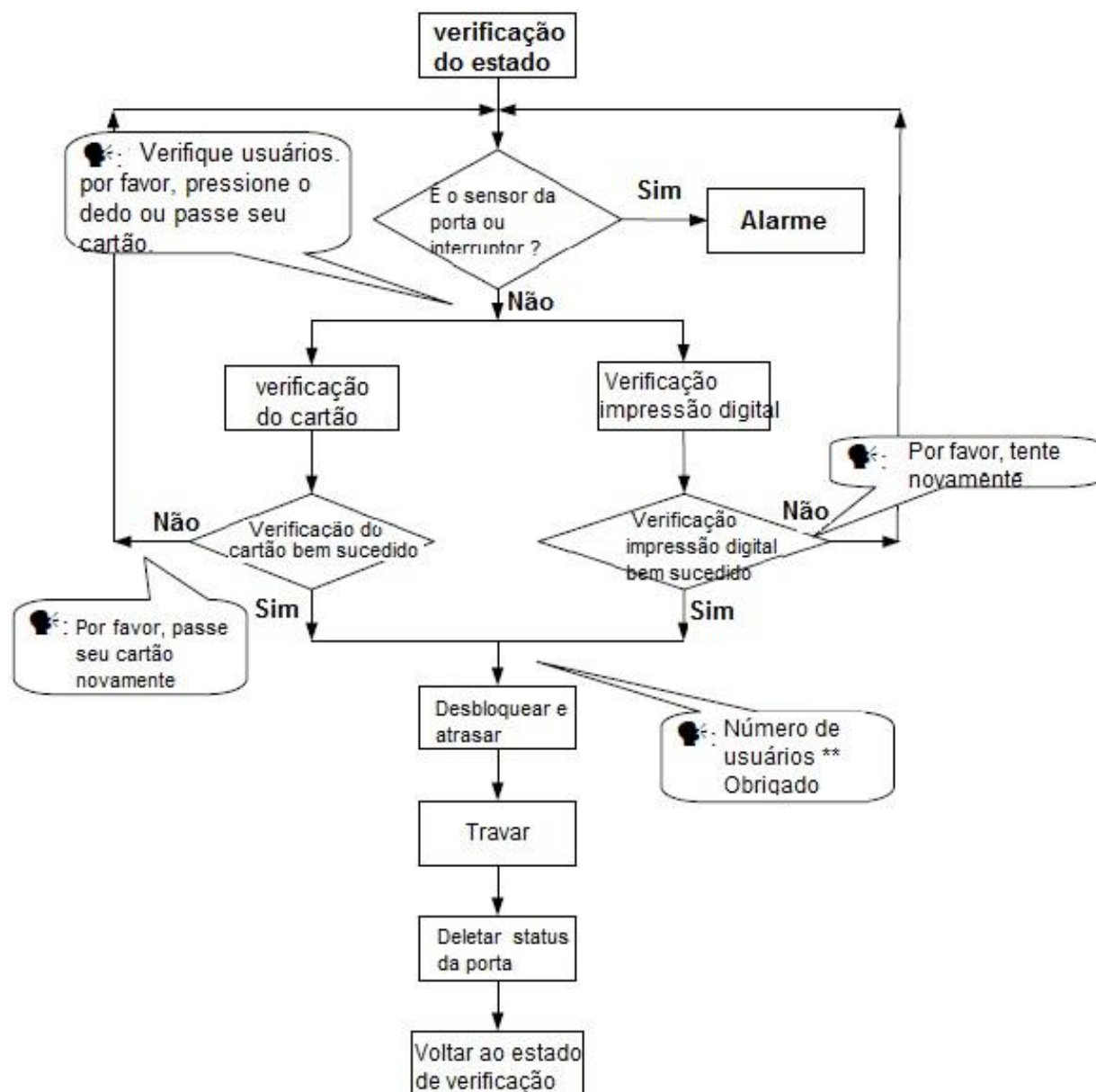
Primeiro cartão magnético:

Passe o cartão através do leitor de cartão. Se a verificação for bem sucedida, o sistema gera a mensagem de Voz "□: Número de usuários ** Por favor, pressione seu dedo. "Após a verificação de impressões digitais com sucesso, e ao mesmo tempo aciona um sinal de desbloqueio. Se a verificação falhar, o sistema gerar o comando de voz. "□: Por favor, tente novamente. "

Impressão digital ou verificação do cartão

Isto é, a operação de verificação de (1) ou (2) ambos eficazes.

O fluxograma do usuário de verificação é mostrado como abaixo:



Tipo:

- (1) Se o usuário não estiver na zona horária de controle de acesso eficaz, ele não pode verificar e abrir a porta, o sistema gera a mensagem de voz “□: zona horária inválido.”
- (2) Se o usuário não for usar o modo de verificação conjunto para verificar, ele não consegue verificar e abrir a porta, o sistema gera a mensagem de voz “□: Modo de verificação inválido.”

3.4 Pen-drive

O usuário pode realizar transferência de registro, faça o download do usuário, envio de usuário, e atualização de firmware através de um Pen-drive

a. **Registro de download:** Faça o download dos registros de atendimento de todos os usuários do dispositivo para uma pen-drive.

b. **Download de usuário:** Baixar todas as informações do usuário, tais como impressões digitais e números de cartão do dispositivo para um pen-drive.

c. **Upload de Usuário:** Envie as informações do usuário a partir de um pen-drive para o dispositivo.

d. **Atualização de firmware.** Atualizar o firmware do dispositivo através de um pen-drive. os arquivos de configuração do pen-drive pode ser criado e modificado por meio do software de controle de acesso. A operação, consulte o software manual do usuário.



Aviso: Por favor, não atualizar o firmware a seu critério, pois pode trazer problemas e afectar a utilização normal do dispositivo. contrate nossos distribuidores para suporte técnico ou de notificação de atualização.

Operações do pen drive inclui os dois casos seguintes:

1. Se você conectar um pen-drive sem arquivo de configuração no dispositivo, o sistema solicitará automaticamente das operações em sequência.

- (1) Depois de conectar um pen drive no dispositivo, você pode passar o cartão uma vez para entrar no estado de gerenciamento do pen drive.
- (2) O sistema gera o comando de voz “□:****. Por favor, passe o seu cartão de gerenciamento para confirmação.” (**** indica os quatro itens de operação de um a d em sequência; mesmo a seguir).
- (3) Se você quiser executar o gerenciamento do Pen drive, passar o cartão para confirmação. Se a operação for bem sucedida, o sistema irá gerar o comando de voz “A operação é bem-sucedida.” E pedir-lhe para avançar para a próxima etapa. Depois de concluir os quatro itens, o sistema gera o

comando de voz “: O sistema retorna para o estado de verificação “. Se a operação falhar, o sistema irá gerar o comando de voz “: A operação falhou. O sistema retorna para o estado de verificação “.

(4) Se você não passar o cartão de gerenciamento o sistema irá pular automaticamente este passo após 5 segundos, e pedir-lhe próximo passo. Depois de terminar os quatro itens, o sistema retorna para o estado de verificação automaticamente.

2. Se você conectar um pen drive com arquivo de configuração para o dispositivo, o sistema vai realizar operações com base nas configurações do arquivo de configuração.

(1) Depois de conectar um pen drive ao dispositivo, você pode passar o cartão uma vez para entrar no estado de gerenciamento de pen drive.

(2) O sistema obtém comandos de operação através da leitura da configuração arquivo sobre um pen drive e gera o comando de voz “□: Configuração de execução arquivos do pen drive. Por favor, passar o cartão de gerenciamento para confirmação. ”

(3) Depois de passar o cartão e realizar todas as operações com sucesso, o sistema irá gerar o comando de voz. “□: ****. A operação é bem-sucedida. "em sequência para cada etapa da operação. Se qualquer uma das operações falhar, o sistema irá gerar o comando de voz “□: A operação falhou “. Depois de terminar todas as operações, o sistema gera um aviso de voz “□: O sistema retorna a verificação do estado."

Atenção: Por favor, esperar 8 segundos depois de inserir o pen drive no dispositivo, caso contrário, o sistema pode não detectar o U-disco, provavelmente.

3.5 Botão Tamper

O tamper é pressionado e mantido baixo com uma tampa traseira. Quando o dispositivo é desmontado, o tamper será levantado e, em seguida, ele vai enviar um sinal de alarme para disparar um alarme.

Cancelar o alarme: O usuário pode apagar o alarme destravando a porta sobre correspondência bem sucedido.

Restaurar os padrões de fábrica: Os padrões de fábrica podem ser restaurados através do botão tamper. Quando o sistema gera um alarme durante 30-60 segundos, o utilizador pode pressione o tamper três vezes (até o alto-falante sons) para restaurar configurações padrão, incluindo o número do dispositivo, a senha do sistema, IP endereço, 485 endereço e senha do teclado.

- **Nota:**

1. As informações do usuário armazenadas no dispositivo não serão apagadas após o dispositivo ser restaurado para os padrões de fábrica.

2. O padrão de fábrica pode ser restaurado através do teclado USB. Para detalhes, consulte [3.2.5 Restaurar padrões de fábrica](#).

4 Anexo

4.1 Lista dos parâmetros

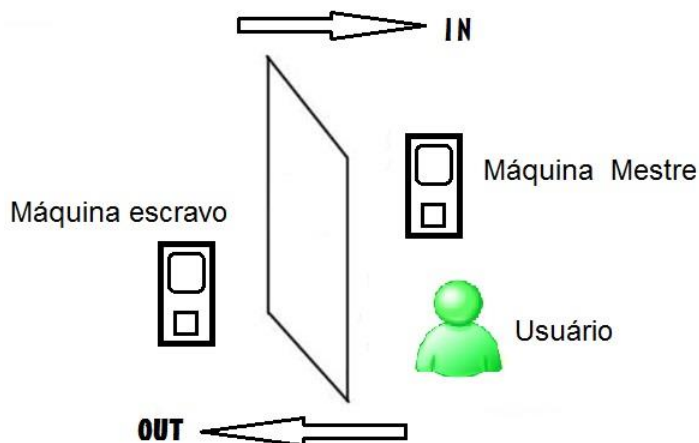
A tabela a seguir lista os parâmetros funcionais básicas do dispositivo.

Item	Note
Fonte de alimentação	12V 3A
Função	Dispositivo de controle de acesso, Alarme, Fechadura, Botão de saída
	Uma entrada wiegand e uma saída wiegand
Quantidade de usuários	10000 (Impressão digital e cartão de identificação)
Capacidade de registro	100000 Partes de registros
Capacidade de registro (impressão digital / cartão)	1500 impressão digital 10000 Cartão
Modo de verificação	ID(mifare)cartão, impreção digitão, carrtão+impreção digital
Comunicações	TCP/IP, RS485, Pen Drive
Alto-falante	Voz, BEEP
LED	Indicação do cabo colorido(vermelho/verde)
Teclado	Teclas válidas : 0-9, Enter, ESC

4.2 Anti-Pass Back

[Visão geral]

Às vezes, uma pessoa ilegal segue para a outra porta, a qual trará problema de segurança. Para evitar esse risco, esta função é ativada. No registro deve coincidir com o registro, ou a porta não será aberta. Esta função precisa de duas máquinas para trabalhar juntos. Um está instalado no interior da porta (máquina mestre adiante), o outro é instalado fora da porta (máquina escravo adiante). Comunicação é sinal Wigand adotado entre as duas máquinas.



[Princípio de funcionamento]

A máquina principal tem wigand In e máquina escravo tem wigand Out. Conecte máquina wigand escravo Out na máquina Mestre wigand. A saída da máquina wigand escravo não deve possuir identificação. O número enviado para a máquina mestre da máquina escravo deve ser encontrado na máquina mestre.

[Função]

Se o anti-pass back está de acordo com o usuário recente in-out no registro. No registro e registro out deve ser correspondido. Esta máquina suporta fora, dentro, ou fora-in anti-pass-back.

Quando a máquina mestre é definido como "o anti-pass back", se o usuário deseja entrar e sair normalmente, o seu registro recente deve ser "in", ou ele não pode sair. Qualquer registro "out" será "anti-passar-back recusada". Por exemplo, um registro recente do usuário é "in", seu segundo disco pode ser "out" ou "in". Seu terceiro disco é baseado em seu segundo disco. Out registro e no registro deve partida (**Aviso:** Se o cliente não tem qualquer registro antes, então ele pode vir, mas não pode sair).

Quando a máquina mestre é definido como "em anti-passar back", se o usuário quiser para entrar e sair normalmente, o seu registro recente deve ser "out", ou ele não pode sair. Qualquer fora registro será "anti-passar de volta recusada" pelo sistema (**Aviso:** Se o cliente não tem recorde anterior, então ele pode ir para fora, mas não pode entrar). Quando a máquina mestre é definido como "fora-in anti-pass back", se o usuário quer entrar e sair normalmente, se seu recorde recente é "out" e "in", então o seu próximo disco deve ser "in" e "out".

【Operação】

1. Selecione o modelo

Máquina principal: Máquina com Wiegand na função, exceto para leitor F10. Máquina escravo: máquina com função Wiegand Out

2. Definir anti-pass back direção e status do dispositivo.

3. Modifique o formato de saída Wiegand do dispositivo

Quando os dois dispositivos estão se comunicando, apenas sinais sem Wiegand ID do dispositivo são recebidos.

4. Matricular usuário

O usuário deve estar na máquina mestre e escravo da máquina, ao mesmo tempo, e PIN utilizador tem de ser o mesmo. Portanto, é necessário registrar usuário na máquina mestre e da máquina escravo ao mesmo tempo.

5. Instruções de Ligações

Comunicação Wiegand é adotado para a máquina mestre e máquina escravo. Consulte o seguinte para conexão:

Mestre	Escravo
IND0	WD0
IND1	WD1
GND	GND

- **Atenção:** Você só pode definir os parâmetros anti-pass back através do software de controle de acesso, para o detalhe consulte o usuário do software Manual.