

MODELO TF 1700



Sobre este manual:

Este manual apresenta as operações de interface e menu dispositivo, incluído Sistema de Segurança Access3.5 são usados juntos. Para a instalação do equipamento, veja o manual de instalação.

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

Índice

1. Aviso para Uso	5
2. Conceitos Básicos	6
2.1 Registro do usuário	7
2.2 Verificação do usuário	7
2.3 ID do usuário	7
2.4 Autoridade Classes	7
2.5 Aparência do Dispositivo	8
3. Inscrição e Verificação	9
3.1 registrar um usuário	9
3.1.1 Inscrever impressão digital	10
3.1.2 Registros de backup	11
3.1.3 Cadastrar Senha	11
3.1.4 Registrar cartão de identificação	13
3.2 Solicita inscrição de sucesso	14
3.3 Modos de verificação	15
3.3.1 . Verificação de Impressões Digitais	15
3.3.2 Senha de Verificação	17
3.3.3 Verificação por meio de cartão	17
3.4 Registro do Administrador	18
3.5 Excluir dados de inscrição	19
4. Configurações	19
4.1 Configurações do Sistema	20
4.1.1 Configurações de tempo	20
4.1.2 Idiomas	21
4.1.3 Formatos de data	21
4.1.4 Configurações avançadas	22
4.2 Gerenciamento de Energia	23
4.3 As definições relacionadas com comunicação	23
4.4 Opções de acesso	24

4.4.1 Fechaduras	25
4.4.2 DSEN. Atraso.....	25
4.4.3 DSEN. Modo.....	25
4.4.4 485 Reader.....	25
4.4.5 Estado Mestre.....	27
4.4.6 Modos de Verificação.....	27
4.5 Teste Automático.....	27
5. Gerenciamento USB Pen Drive	28
5.1 Baixar dados de Presença.....	28
5.2 Baixar dados do usuário.....	29
5.3 Carregar Dados do Usuário	29
6.Sistemas de Informação	30
7. Desligar o alarme	31
8.Manutenção	31
9.Perguntas mais frequentes	32
10. Apêndice.....	33
10.1 USB.....	34
10.2 Agendada de Bell	34
10.3 Conexão Externa com o Leitor de Impressões Digitais.....	35
10.4 Funções GPRS.....	35
10.5 Funções WIFI.....	35
10.6 Consulta atendimento	35
10.7 Descrição da função MP3.....	36
10.8 Mensagem Curta.....	36
10.9 Vários modos de verificação.....	37
10.10 EM Readonly Card, cartão HID, Mifare cartão, cartão iClass	38
10.11 Função mestre/escravo	39
10.12 Identificação Remota do Servidor (RIS).....	42
10.13 Controle de Acesso do Servidor Web	43
10.14 Coletas automática de endereços IP	44
10.15 Protocolo Wiegand	44

10.16 Função POE	45
10.17 Bateria reserva (Mini-UPS)	46
10.18 9 Dígito Número da inscrição	46
10.19 Calibração Automática da Hora	46
10.20 Horários de Verão (configurações de fuso horário)	47
10.21 Reproduzir voz dentro de um prazo determinado segmento (segmento de tempo ou de um grupo)	48
10.22 Código de Trabalho	49
10.23 DHCP	49
10.24 Agrupamentos de Usuários	49
10.25 Métodos de Entrada T9	50
10.26 Função TTS	50

1. Aviso para Uso

Obrigado por usar o nosso preto e branco (B & W) Tela Series Access Controle Standalone e Reader Produtos. Por favor, leia com atenção este manual antes de utilizar este produto para uma compreensão abrangente de modo como para evitar causar danos desnecessários ao produto.

Proteger o aparelho contra a exposição à luz solar direta ou feixe forte como feixe forte afeta muito coleta de impressão digital e impressão digital leva a falha de verificação.

Evite utilizar o produto ao ar livre no verão. A temperatura de trabalho de B & W série de tela varia de 0-40 ° C. O calor dissipado durante longa operação pode levar facilmente a resposta abrandamento e verificação de diminuição da frequência. É recomendado para uso guarda-sóis e o dissipador de calor os dispositivos para proteção do produto no exterior. Recomendamos que você use o dispositivo adequadamente, de modo a obter o efeito ideal e reconhecimento de

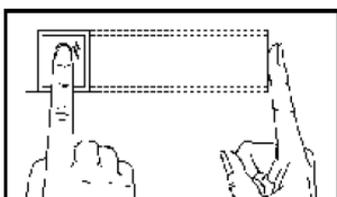
Velocidade de verificação.

1. Dedos recomendados

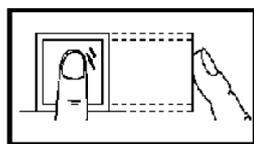
Dedos recomendados: O dedo indicador, dedo médio ou o dedo anelar; o polegar e o dedo mindinho não são recomendados (porque eles são geralmente desajeitados na tela de coleta de impressões digitais).

2. Colocação dos Dedos

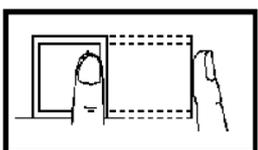
1) O dedo deve estar bem centralizado e colado a superfície de leitura para o cadastro mais correto.



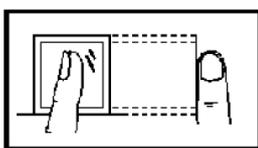
2) Posições Impróprias para cadastro



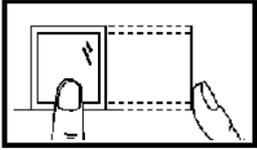
O DEDO NÃO ESTÁ COLADO A SUPERFÍCIE.



O DEDO NÃO ESTÁ CENTRALIZADO NA SUPERFÍCIE.



O DEDO ESTÁ POSICIONADO DE LADO.



O DEDO ESTÁ TOTALMENTE FORA DO CENTRO DA SUPERFÍCIE.

 **Observação:** Por favor, se inscrever e verificar a sua impressão digital, utilizando o modo de posicionamento do dedo adequado para evitar a degradação de verificação desempenho devido a operações impróprias.

3. Cores de LED e seus significados

Funciona normalmente: O LED verde pisca uma vez a cada segundo.

Verificação de falha: O LED vermelho é contínuo em 3 segundos

Verificação for bem sucedida: O LED verde é contínuo por 3 segundos.

 **Observação:** Se o display LED é inconsistente com as condições acima, por favor, entre em contato com nosso pessoal técnico.

4. Sobre este manual

- Nossos produtos estão sujeitos a atualizar de tempos em tempos, por isso a nossa empresa vai nem fazer um compromisso de garantir a coerência entre os produtos reais e neste documento, nem assume qualquer responsabilidade por qualquer litígio decorrente da diferença entre os parâmetros técnicos reais e este manual. Este documento está sujeito a alterações sem aviso prévio.
- As funções marcadas com . Neste manual são opcionais para alguns B & W série de tela de acesso independente controlador e produtos de leitor. Por favor, consulte o produto real para a descrição específica de função.
- Imagem descrições neste manual podem variar ligeiramente do produto real. Por favor, consulte o real produto para obter as descrições exatas.
- Reserve o direito de alterar e interpretar pela nossa empresa.

2. Conceitos Básicos

Esta seção apresenta as definições e descrições dos seguintes conceitos básicos:

- Registro de usuário

- Verificação do usuário
- ID do usuário
- Classe Autoridade
- Aparência do dispositivo

As duas mais importantes funções suportadas pelo cadastro de usuários e verificação.

2.1 Registro do usuário

Um usuário pode se inscrever até 10 impressões digitais diferentes, utilizando um número de identificação para ter várias seleções de verificação.

Teoricamente todos os dedos de um usuário precisam ser registrados para que o usuário pode usar qualquer uma das impressões digitais para o reconhecimento, mesmo que ele / ela se esquece que impressão digital foi registrado.

Geralmente é recomendável que um utilizador deve inscrever pelo menos, duas impressões digitais, por exemplo, o dedo indicador de ambas as mãos, de modo que o usuário pode ainda fazer a combinação de impressão digital, mesmo que um ou mais de seu / seus dedos são cortados ou danificado.

2.2 Verificação do usuário

Quando um usuário verifica seu / sua impressão digital no leitor de impressões digitais (1: N), ou entra em uma senha / colocando sua / seu dedo depois de entrar um número de identificação (1:1), o dispositivo compara a impressão digital recém-digitalizada com uma impressão digital armazenada no modelo. O modelo de impressão digital é usado para verificar o ID do usuário. Após a verificação, o sistema exibe uma voz de comando sobre se a verificação for bem sucedida ou não, e, em seguida, armazena o registro correspondente sucesso no dispositivo.

2.3 ID do usuário

Ao registrar as impressões digitais, o usuário será alocado com um ID não utilizado. Quando o usuário começa a verificar o seu / sua identidade, essa identificação é usada para associar o modelo de recurso de impressão digital ou senha.

Você pode digitar o ID através do mini-teclado ou outros meios de armazenamento, por exemplo, o cartão de RF (o dispositivo de reconhecimento de impressões digitais deve ser configurado com o leitor de cartão de RF).

2.4 Autoridade Classes

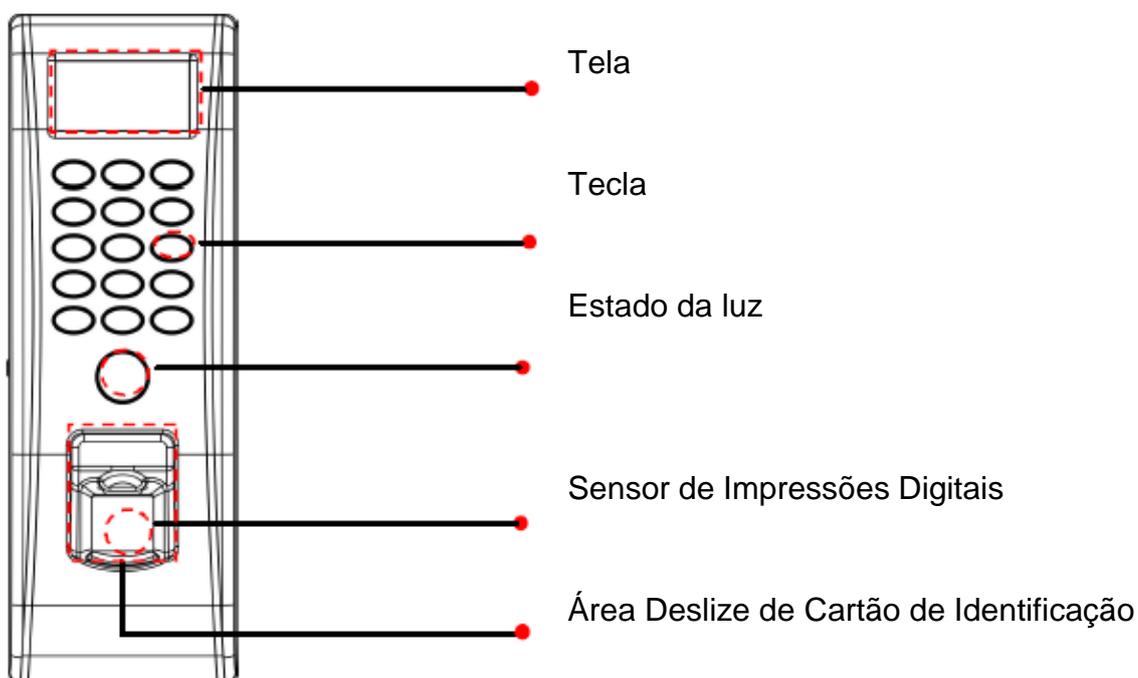
O dispositivo tem duas classes de autoridade:

I Usuários: referem-se aos que são obrigados a verificar a sua identidade com um propósito, por exemplo, abrir a porta ou manter seus registros de entrada / saída.

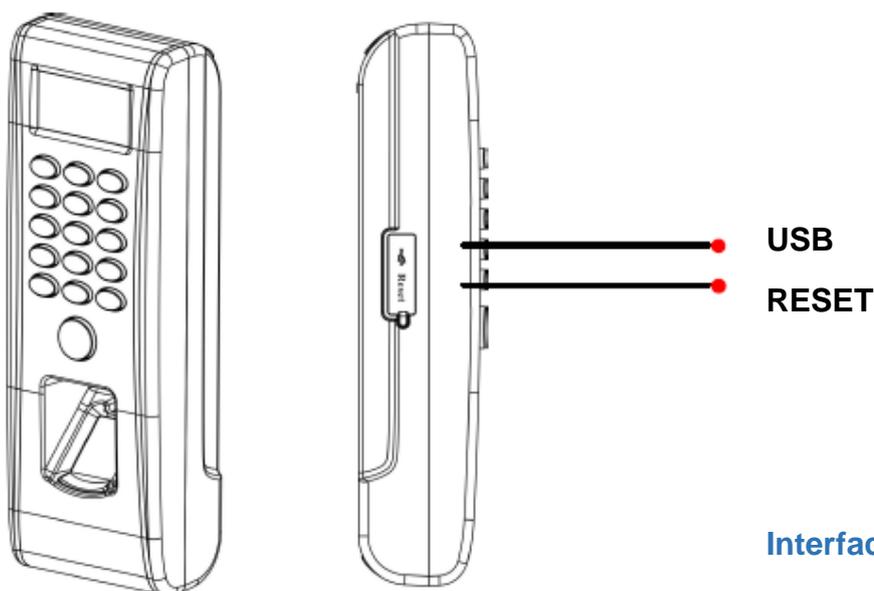
I Administradores: Ter todos os privilégios concedidos aos usuários comuns, e acesso ao menu principal para várias operações.

2.5 Aparência do Dispositivo

Vista frontal:



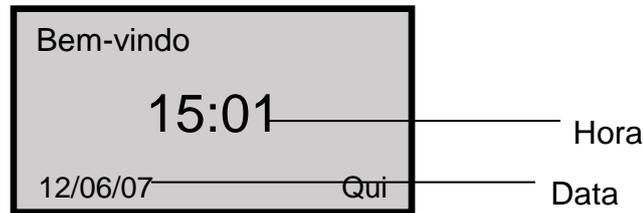
Vista Lateral:



Interface inicial:

A primeira interface exibida na tela ao ligar

o equipamento é referida como a "interface inicial", como mostrado na figura a seguir.



3. Inscrição e Verificação

Este capítulo apresenta como se inscrever usuários no dispositivo. Além disso, ele descreve como verificar a validade de impressões digitais registradas.

Este capítulo inclui as seguintes peças

- Inscrever os usuários
- Registrar impressões digitais de backup
- Solicita inscrição bem sucedida
- Verificar a identidade.
- Inscrição do Administrador
- Excluir dados de inscrição

Observação: Para registrar um novo usuário, você deve ter a autoridade de administrador. Para mais detalhes, consulte 2.4 Authority Classes

3.1 registrar um usuário

O dispositivo suporta três modos matrículas: registro de impressão digital, senha de inscrição e matrícula RFID.

Se nenhum administrador foi inscrito, qualquer usuário tem o direito de inscrever um novo usuário.

Caso o administrador já inscrito, que você registrar um novo usuário, precisamos verificar o administrador identidade em primeiro lugar, pressionando MENU. O sistema então solicita que você pressione o dedo ou digite a senha ou cartão magnético para verificação de administrador.

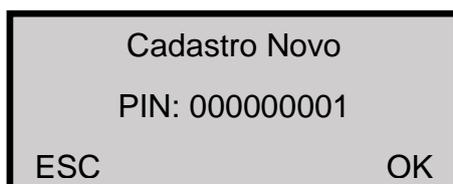
□ Observação:

1. Se você quiser limpar o privilégio de administrador, por favor clique em " Configurações " --" Configurações avançadas "para selecionar.

2. Verificar a tipo de impressão digital ou cartão de furto por padrão, então se você registro, escolha inscrever impressão digital ou cartão é a melhor.
3. Para garantir a segurança do dispositivo, recomenda-se para definir um administrador ao usar o terminal inicialmente.

3.1.1 Inscrever impressão digital

- 1) Selecione o Menu → usuário Gerenciar → Registro de Usuário para exibir o [registro do usuário] interface. Selecione [Se Inscrever PQ] e pressione OK para visualizar o [Cadastrar PQ] interface.



- 2) Introduza um número (de 1999999999) no [ID do usuário]. Pressione OK para exibir a interface de registro de impressões digitais.



Observação:

O último dígito "0" no "0000000010" indica a primeira impressão digital. "0000000011"

O último dígito "1" denota a segunda impressão digital, impressão digital significa backup.

O dispositivo apresenta 9 dígitos números, e automaticamente adiciona 0 como prefixo para os números com menos de 9 dígitos. Para exemplo, se você digitar "11", o dispositivo irá exibir "000000011".

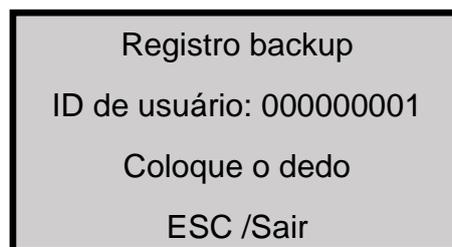
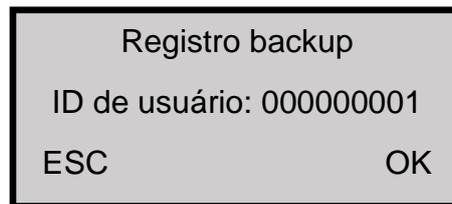
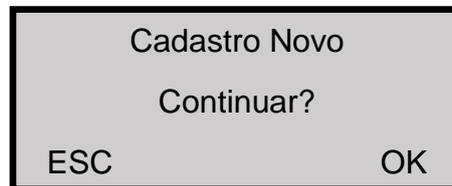
- 3) Coloque o mesmo dedo por três vezes consecutivas no leitor de impressões digitais de acordo com instruções do sistema. Se a inscrição bem-sucedida, a seguinte informação é exibida:



- 4) Pressione OK para salvar a impressão digital registrada. Se o registro falhar, o sistema pedirá que você insira novamente sua identificação de usuário e reiniciar a inscrição a partir do Passo 2.

3.1.2 Registros de backup

Se você pressionar ESC no [Novo Registro] interface, você pode cancelar a nova inscrição e apresentar o [Registro backup] interface, pressione OK e, em seguida, como mostrado na figura a seguir:



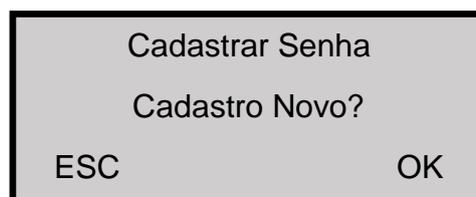
As seguintes etapas de inscrição de backup são os mesmos com os da nova matrícula.

Observação:

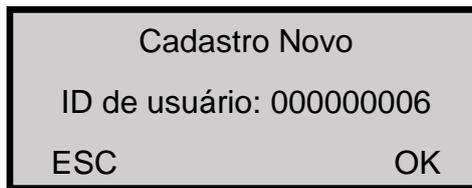
Recomenda-se que a longo prazo usuário deve se inscrever duas impressões digitais, pelo menos. Registro de Backup pode escolher impressão digital ou senha ou o cartão.

3.1.3 Cadastrar Senha

1) Selecione o Menu → usuário Gerenciar → Registro de Usuário para exibir o [registro do usuário] interface. Selecione [Inscrever PWD] e pressione OK para visualizar o [Cadastrar Senha] interface.

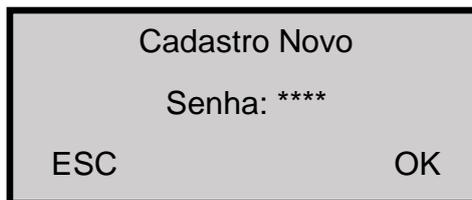


- 2) Pressione OK para confirmar e prosseguir.



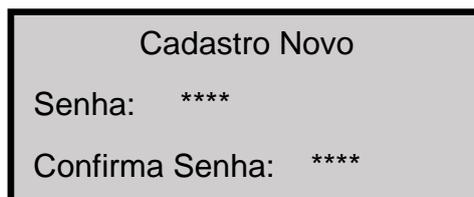
Cadastro Novo
ID de usuário: 000000006
ESC OK

- 3) Introduza um número (1-999999999) no campo [ID do usuário]. Pressione **OK** para exibir a interface de entrada de senha.



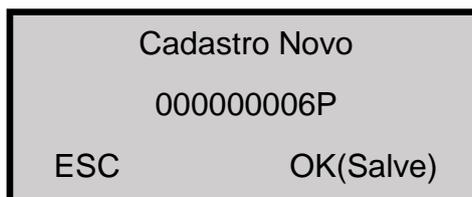
Cadastro Novo
Senha: ****
ESC OK

- 4) Introduza a sua palavra-passe no campo [Senha de entrada] e pressione **OK** para continuar.



Cadastro Novo
Senha: ****
Confirma Senha: ****

- 5) Digite novamente a senha no campo [Confirma Senha] e pressione OK para confirmar a sua entrada e prossiga.



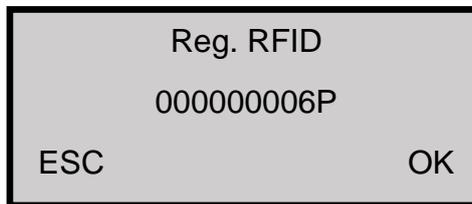
Cadastro Novo
000000006P
ESC OK(Salve)

Nota: O último dígito "P" em "000000006P" denota senha.

- 6) Pressione OK para salvar os dados registrados e sair da inscrição senha. Pressione ESC para modificação entrada interface de senha, as seguintes etapas são as mesmas com as da nova matrícula senha.

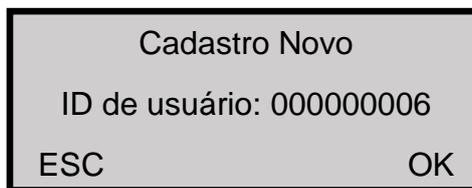
3.1.4 Registrar cartão de identificação

1) Selecione Menu → Gerenciar usuário → Inscrição usuário para exibir o [Inscrição usuário] interface. Selecione [Registrar RFID] e pressione OK para continuar.



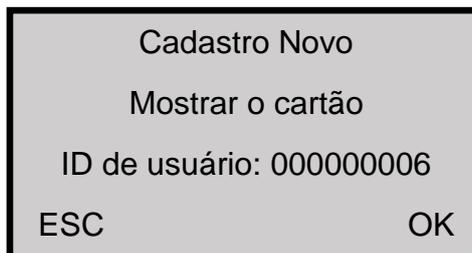
Reg. RFID
000000006P
ESC OK

2) Pressione OK para confirmar e prosseguir.



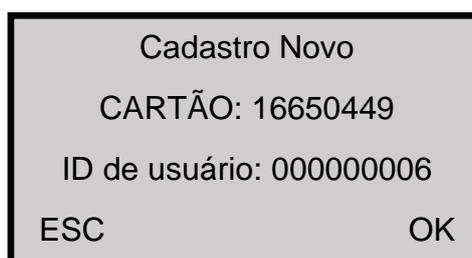
Cadastro Novo
ID de usuário: 000000006
ESC OK

3) Introduza um número (1-999999999) no campo [ID do usuário]. Pressione OK para exibir a interface de registro de cartão de identificação.



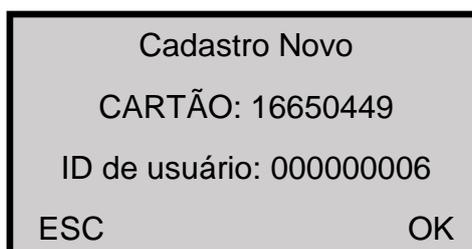
Cadastro Novo
Mostrar o cartão
ID de usuário: 000000006
ESC OK

4) Passe o cartão e o sistema lê o número do cartão.



Cadastro Novo
CARTÃO: 16650449
ID de usuário: 000000006
ESC OK

5) Pressione OK para confirmar e prosseguir.



Cadastro Novo
CARTÃO: 16650449
ID de usuário: 000000006
ESC OK

6) Pressione OK para salvar os dados registrados e completar a inscrição carteira de identidade. Pressione ESC para modificação entrada ID da interface série.

☐ **Observação:** HID cartão de débito ou Mifare é uma função opcional. Se você deseja personalizar, por favor, consulte os nossos representantes comerciais pré-venda ou engenheiros de suporte técnico.

3.2 Solicita inscrição de sucesso

Uma impressão digital registrada com alta qualidade garante velocidade de verificação rápida, enquanto aquele com má qualidade pode facilmente levar a falsa rejeição e verificação lenta.

Para melhorar a qualidade das impressões digitais registradas, consulte a Tabela 31

Tabela Contém 31 causas comuns de falha de inscrição ou baixa qualidade de impressão digital

Dedo está muito seco ou sujo	Esfregue os dedos contra a palma da mão, porque a esfregar óleo de rendimentos. Hidratar o seu dedo através da respiração nele.
Aplicar insuficiente a pressão	Aplicar uma pressão ligeira e uniformemente durante o processo de captura.
Selecione dedos para Inscrição	<p>Dedos indicadores esquerdo e direito ou dedos médios são recomendados.</p> <p>Selecione os dedos sem wornout ou impressões digitais danificadas.</p> <p>Os usuários costumam escolher os seus dedos indicadores, mas se os seus dedos indicadores não têm alta qualidade de impressões digitais, eles podem selecionar seus dedos médios ou dedos anelares.</p> <p>Para os usuários com dedos pequenos, eles podem optar por seus polegares. Para inscrever-se livre impressões digitais, os usuários podem selecionar os dedos não propenso a wearout ou danos, por Exemplo, os dedos anelares.</p>
Posicionamento do dedo	<p>Pressione seu dedo sem rodeios sobre o sensor de impressão digital e ter certeza de que o bloco (não o ponta), abrange tanto a janela do sensor quanto possível. Não pressione seu dedo</p> <p>Perpendicularmente ao sensor de impressões digitais, não bater o seu dedo no sensor</p> <p>Rapidamente, mantenha o dedo ainda.</p>
Impacto da mudança de imagem da impressão digital	A mudança da imagem da impressão digital devido a pele peelingoff ou prejuízo afetará a verificação desempenho. Se a impressão digital qualidade de um usuário é ruim devido à pele e o usuário não poderá passar a verificação uma semana mais tarde, o

	usuário precisa se registrar novamente a sua impressão digital ou adotar o modo verificação de senha.
Outras causas	<p>Podem haver uma pequena quantidade de pessoas que não conseguem passar a verificação não importa o quão difícil, tente devido às impressões digitais muito pobre qualidade. Nesse caso, você pode adotar o ID + modo verificação de impressões digitais, devidamente inferior a 1: UM jogo limite ou adotar a senha modo de verificação.</p>

3.3 Modos de verificação

Após a inscrição, você pode verificar a validade que as impressões digitais registradas ou carteira de identidade ou a senha na interface inicial.

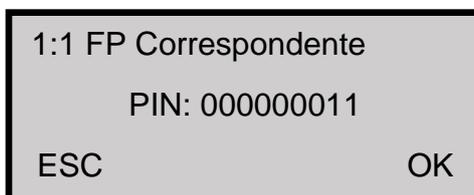
3.3.1 . Verificação de Impressões Digitais

1:1 e 1: N modos de identificação de impressão digital correspondente.

(1) 1:1 correspondência de impressões digitais

No modo correspondente 01:01 de impressões digitais, o dispositivo compara a impressão digital atual coletadas através do leitor de impressões digitais, com isso em relação ao usuário ID inseridos através do teclado.

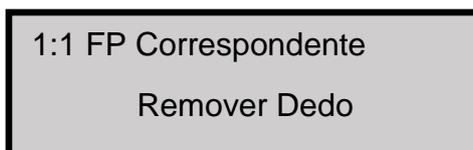
Operação passos:



Digite um ID de usuário através do teclado na interface inicial.

Observação: Caso o usuário tenha sido registrado senha, pressione OK para a verificação, ele será automaticamente entra na interface verificação de senha. Se não tiver, pode entrar a verificação de impressão digital interface.

Sugerimos aos usuários no uso de impressões digitais 1:1 comparação, pressionar diretamente impressões digitais, não pressione o botão OK.



E, em seguida, coloque diretamente o dedo no leitor de impressões digitais para exibir a seguinte interface:

Verificar
ID de usuário: 000000006
Verificado!

Após a interface acima é exibida de cerca de 0,5 segundos, e então a seguinte interface será apresentada:

FP Verificar
Por favor, Tente Novamente

Se a verificação falhar, o sistema irá gerar um anúncio de voz "Por favor, tente novamente!" E exibir a seguinte interface:

(2) 1: N verificação de impressão digital

No 1: O modo de reconhecimento de impressões digitais de N, o dispositivo compara a impressão digital atual recolhido através do leitor de impressões digitais com as impressões digitais armazenados no dispositivo.

Passos de operação:

FP Verificar
Remover Dedo

Coloque o dedo sobre a interface inicial para exibir a seguinte interface:

Verificar
ID de usuário: 000000001
Verificado!

Se a verificação for bem sucedida, o sistema irá gerar um anúncio de voz "Obrigado!" Depois do acima interface é exibida cerca de 0,5 segundos, e então a seguinte interface será exibida:

Se a verificação falhar, o sistema irá gerar um anúncio de voz "Por favor, tente novamente!" E exibir a seguinte interface:

FP Verificar
Por favor, Tente Novamente

Após a interface acima é apresentada 0,5 segundo, o sistema voltará para a interface inicial.

3.3.2 Senha de Verificação

Insira seu número de ID na interface inicial.

1:1 FP Correspondente

ID de usuário: 000000008

ESC OK

Pressione OK e o sistema exibe uma mensagem de alerta " Verificado!"

Verificar Senha

ID de usuário: 000000008

Senha de entrada*****

Entrada a senha correta e pressione OK para confirmar a sua entrada.

Verificar Senha

ID de usuário: 000000008

Verificado

Se você digitar uma senha errada, o sistema exibe " Senha errada" como mostrado abaixo e volta para a senha interface de entrada, você deve proceder senha verificar novamente.

Verificar Senha

Senha errada

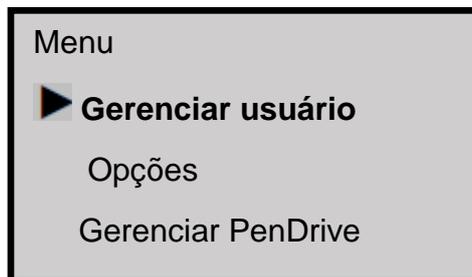
3.3.3 Verificação por meio de cartão

Se você tiver o seu número de cartão de identificação inscritos no sistema, você pode passar a verificação, passando o cartão de identificação na área de deslize de maneira adequada

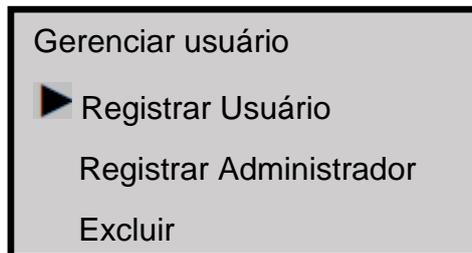
3.4 Registro do Administrador

O dispositivo fornecer configurações de administrador para impedir que usuários não autorizados alteração de dados do sistema e garantir a segurança do sistema. As operações em definições do administrador são as seguintes:

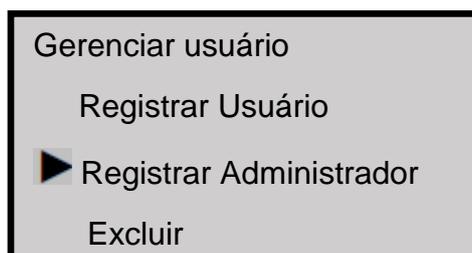
1) O novo dispositivo não atribui qualquer administrador, de modo que você pode pressionar Menu para acessar o sistema diretamente e a seguinte interface será exibida.



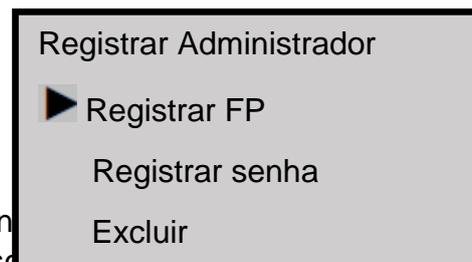
2) Pressione OK para exibir a interface [Gerenciar usuário].



3) Selecione Registrar Administração através da tecla ▲ / ▼.



4) Pressione OK para exibir a interface [Registrar Administrador]:

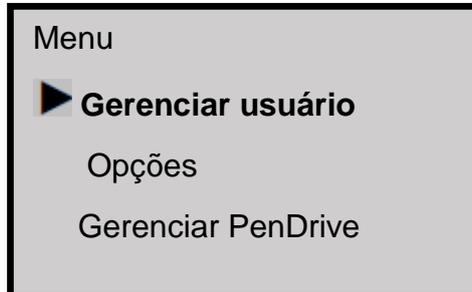


5) Selecione um modo de inscrição para exibir a interface de inscrição de administrador. O modo de inscrição é exibido com a de um novo usuário registrado. Para mais detalhes, consulte 3.1.1 registrar um usuário.

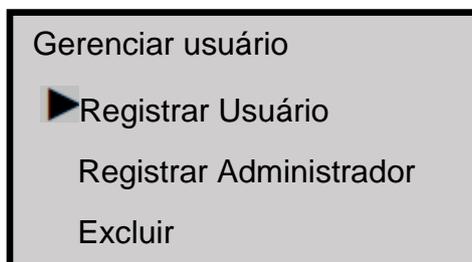
3.5 Excluir dados de inscrição

Para excluir um usuário registrado no sistema, execute o seguinte:

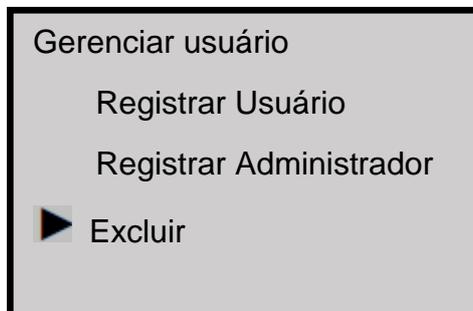
- 1) Pressione Menu para acessar item de menu relacionado para verificação, e a interface a seguir é exibida:



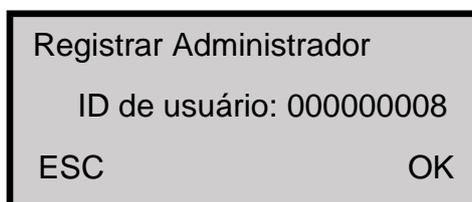
- 2) Pressione **OK** para exibir a interface [Gerenciar usuário].



- 3) Selecione Excluir através da tecla ▲ / ▼.



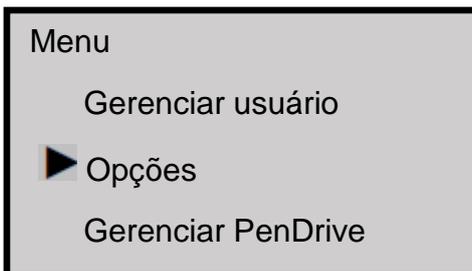
- 4) Pressione OK para exibir a interface [Delete]. excluir



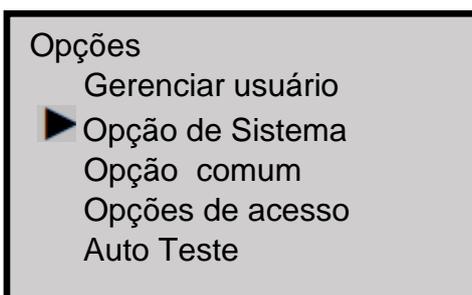
- 5) Digite um número no campo [ID do usuário] e pressione OK para confirmar a sua entrada. Em seguida, excluir o usuário de acordo com o aviso do sistema.

4. Configurações.

Pressione Menu na interface inicial. Depois de verificar os seus direitos administrativos, o sistema exibe a seguinte interface.



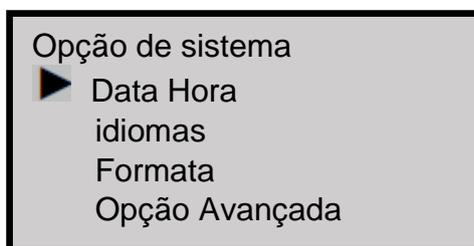
Selecione Opções e pressione **OK** para continuar.



O menu Opções contém cinco submenus: **Gerenciar usuário, Opção de Sistema, Comum Opt, Opções de acesso, Auto Teste.** Estes submenus serão descritos nas secções seguintes.

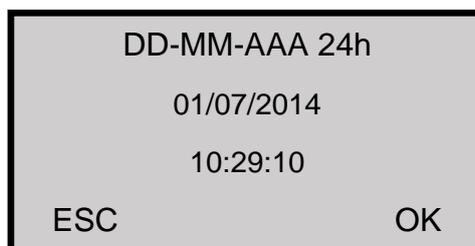
4.1 Configurações do Sistema

Selecione Sistema Opt e as informações exibidas na tela são mostrados na figura a seguir:



4.1.1 Configurações de tempo

Defina a data e hora atual exibido na tela do dispositivo. Selecione Definir Data Hora e pressione OK para exibir a seguinte interface.

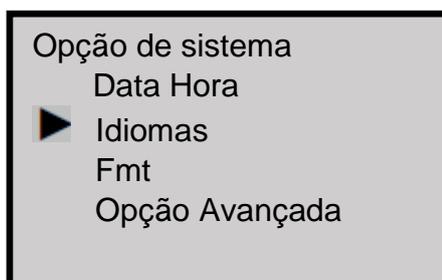


Para modificar a data e a hora, coloque o cursor para o campo desejado através do ▲ / ▼ chave, entrada data correta e tempo, e pressione OK para salvar as alterações.

□ **Observação:** Para alguns tipos de dispositivos, é preciso pressionar a tecla Menu sobre três segundo para confirmar.

4.1.2 Idiomas

Você pode definir o idioma exibido na tela do dispositivo. Selecione o idioma e pressione OK para exibir a interface de edição de linguagem. Se você selecionar Inglês, as informações na tela serão exibidas em Inglês.



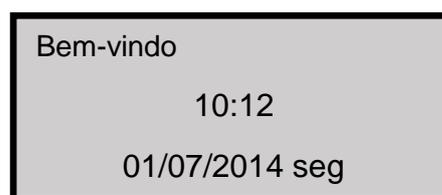
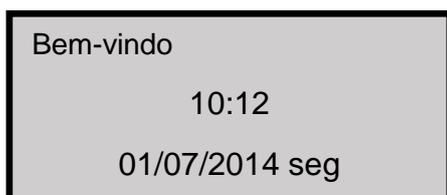
Você pode alterar os tipos de línguas através da tecla ▲ / ▼. Selecione o idioma desejado e pressione OK. Em seguida, pressione ESC para sair do [Sistema Opt] interface. Quando solicitado para salvar as configurações, pressione OK para salvar as configurações. O sistema solicita que as suas definições terão efeito após a reinicialização do dispositivo.

Observação: Seleção de idioma é uma função padrão. Se você precisa desta função, consulte nossos representantes comerciais ou engenheiros de suporte técnico pré-vendas

4.1.3 Formatos de data.

Você pode definir o formato de data exibido na tela do dispositivo. Selecione Formatar e pressione OK para exibir a interface de configuração do formato. Selecione um formato de data desejado através da tecla ▲ / ▼. O dispositivo suporta 10 formatos de data: YYMMDD, YY/MM/DD,YY.MM.DD, MMDDYY,MM/DD/YY, MM.DD.YY, DDMMYY,DD/MM/YY,DD.MM.YY e YYYYMMDD. Selecione o formato de data desejada e pressione OK para confirmar sua seleção. Em seguida, pressionar ESC para sair das configurações do sistema. Quando solicitado a salvar as configurações, pressione OK e o formato da data do sistema é modificado.

Por exemplo, os formatos de data MM / DD / AA e YYMMDD são apresentados nas figuras acima, à esquerda e direita, respectivamente.



4.1.4 Configurações avançadas

Através das configurações avançadas, você pode realizar operações como restaurar os padrões de fábrica, a exclusão de registros de frequência, limpando todos os dados, limpando privilégio de administrador, atualizar o firmware, campainha, ao ar livre modo como mostrado abaixo:



□ **Observação:** As opções do menu acima contêm algumas funções opcionais. Se o produto real não tem uma ou várias das opções acima, então este produto não suporta a função relacionada (s).

Selecione a opção desejada através da tecla ▲ / ▼, e realizar ajustes conforme necessário.

1) Reset Opts

Esta opção é usada para restaurar todas as configurações aos padrões de fábrica.

2) Deletar todos os Logs

Esta opção é usada para excluir todos os registros de verificação no chip.

3) Limpar Todos os Dados

Esta opção é usada para apagar todas as impressões digitais registradas e registros.

4) Clr administrador pri

Esta opção é usada para definir todos os administradores para usuários comuns.

5) Upd firmware

Você pode selecionar "UPD Firmware" para atualizar o firmware do dispositivo através dos arquivos de atualização no pen drive USB.

Observação: Se você precisa de arquivos de atualização de firmware, por favor, entre em contato com nossos engenheiros de suporte técnico. Geralmente não é recomendado para atualizar o firmware.

6) Campanha

O dispositivo faz com que som da campanha, a seleção de "Y" para abrir a campanha para que botões ou função de menu pode fazer um som ao selecionar "N" para fechar.

7) Modo de Outdoor

Escolhendo o modo exterior, por favor, selecione "Y" e a tela exibirá títulos pretos em fundo branco após dispositivo reiniciar, o que é conveniente para o uso ao ar livre.

Pelo contrário, selecione "N" e a tela exibirá títulos brancas em fundo preto após dispositivo reiniciar, o que é conveniente para uso em interiores.

4.2 Gerenciamento de Energia

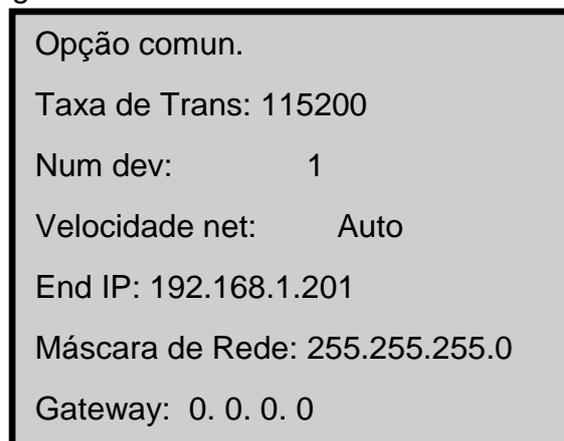
Pressione Menu para selecionar **Opções** → Gerenciamento e as informações exibidas na tela é mostrada na figura a seguir:



Ocioso Vs Ocioso mim Estas duas opções estão intimamente associadas. Quando ocioso min é 0, a função ociosa está desativada. Quando inativo min é um número diferente de zero (unidade: minuto), por exemplo, 1, o sistema entrará em um estado especificado se não houver operação em 1 minuto.

4.3 As definições relacionadas com comunicação

Pressione **Menu** para selecionar **Opções** → **Comm. Opte** e as informações exibidas na tela é mostrada na figura a seguir:



1. Transmissão

Esta opção é usada para definir a taxa de transmissão para a comunicação entre o dispositivo e o PC. Ele inclui cinco opções: 9600, 19200, 38400, 57600 e 115200 A taxa de transmissão de alta é recomendada para a comunicação RS232 para atingir alta velocidade de comunicação, enquanto a taxa de transmissão baixa é recomendada para a comunicação RS485 para conseguir uma comunicação baixa velocidade estável.

2. Num dev

Esta opção refere-se ao dispositivo de identificação numeradas de 1 a 255.

3. Velocidade net

Este parâmetro refere-se à taxa de rede, incluindo cinco opções: Auto, 10mH, 100MH, 10MF e 100MF.

4. IP final.

O endereço IP predefinido é 192168.1.201 . Você pode alterar o endereço IP conforme necessário.

5. Máscara de Rede

A máscara de sub-rede padrão é 255.255.255.0. Você pode modificar o endereço de sub-rede, conforme necessário.

6. Gateway

O gateway padrão é 0.0.0.0. Você pode modificar a porta de entrada conforme necessário.

4.4 Opções de acesso

O dispositivo, o trabalho com o Access 3.5 Pacotes de sistema de segurança como a configuração padrão para alcançar uma série de funções, incluindo Time zones de acesso, tempo feriados, Linkage, Anti Passback, First Card, Normal, Mult iCartão funções de abertura, etc.,

Mas nenhuma função Interlock. Em operação detalhes, consulte Access3.5 Software Manual do Usuário.

Pressione **Menu** para selecionar **Opções** → **Opções de acesso** e as informações exibidas na tela é mostrada na figura a seguir:

Opções de acesso	
▶ Fechadura	5
DSEN. Atraso	15
DSEN. Modo	Nenhum
485 Reader	Mestre
Estado Mestre	Out
Modo de Verificação	FP/RF

4.4.1 Fechaduras

O tempo de duração de bloqueio eletrônico funciona a partir de abrir a fechar quando a verificação do usuário consegue (No caso de a porta está fechada).

Para definir este período, proceder da seguinte forma: Selecione Lock, e pressione OK. Em seguida, digite um número desejado através do teclado numérico e pressione ESC para sair e salvar a configuração.

"S (segundo)" é escolhida como a unidade de duração motorista de bloqueio, e você pode configurá-lo 1 ~ 10s (alguns dispositivos pode definir 254s no máximo).

Se definir a duração do " 0 ", significa bloquear condutor duração é fechada. Normalmente, nós não sugerimos que é " 0 ".

4.4.2 DSEN. Atraso

Definir o atraso sensor da porta. Um alarme será gerado se a porta é deixada aberta por um período de tempo, e este período é chamado de atraso de sensor de porta.

4.4.3 DSEN. Modo

Interruptor do sensor da porta inclui três modos: NENHUM, Normal Aberto (NO) e normalmente fechado (NC).

"NENHUM": interruptor do sensor da porta não é usado.

"NÃO": a porta e fechadura são open; caso contrário, um alarme será gerado após o sensor de porta demora.

"NC": a porta e fechadura são closed; caso contrário, um alarme será gerado após o sensor de porta demora.

4.4.4 485 Reader

Pressione **Menu** para selecionar **Opções** → **Opções de Acesso** → **485Reader**, como mostrado abaixo:

Opções de acesso	
Fechadura	5
DSEN. Atraso	15
DSEN. Modo	Nenhum
▶ 485 Reader	Mestre
Estado Mestre	Out
Modo de Verificação	FP/RF

Equipamento suporta a função 485reader, pode ser através da comunicação 485 conectar com leitor FR1200;

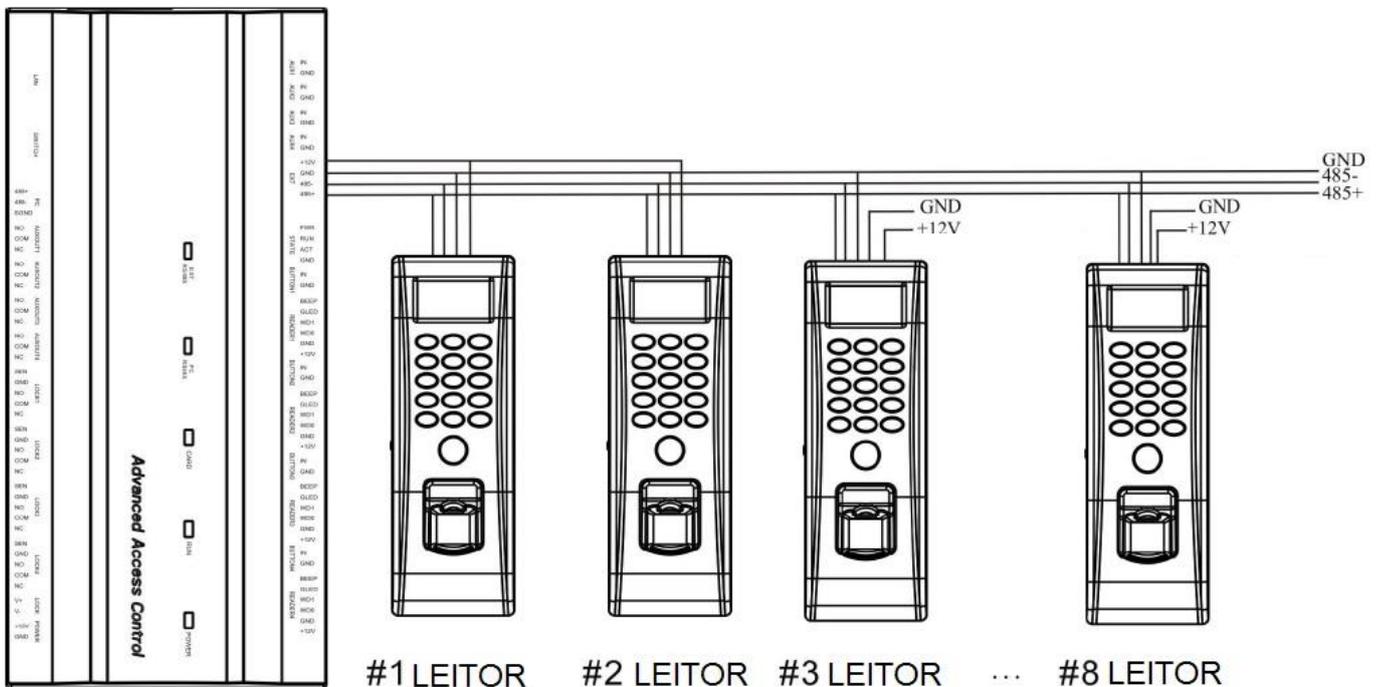
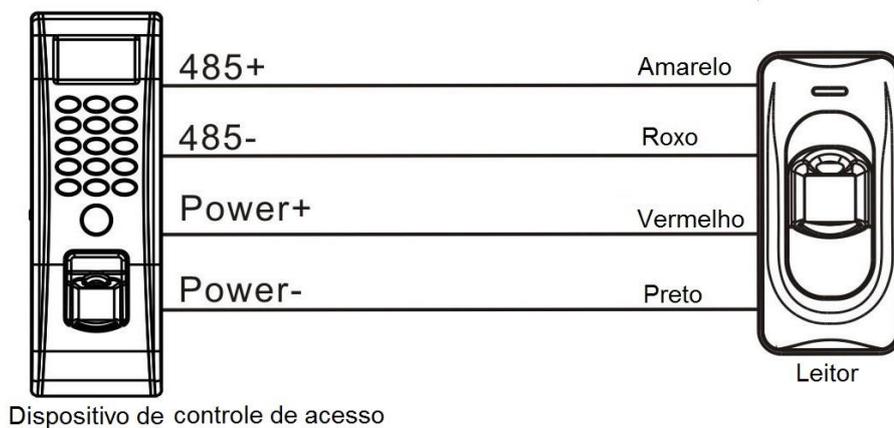
Enquanto isso, ele pode atuar como Mestre Escravo qual o Access Controle for mestre, leitor FR1200 para escravos, para atingir 485 Anti-pass-Black funções.

Se selecionar "Master", função 485reader é aberto, e o ato dispositivo como controlador de acesso;

Se selecionar "Escravo", o dispositivo irá funcionar como leitor;

Se selecionar "Não", a função 485reader está fechado, o dispositivo pode se conectar com o PC através do 485.

☐ **Observação:** O dispositivo funcionar como Mestre ou Escravo, devido aos 485função do leitor é aberta, de modo que o dispositivo não pode com o PC por 485communications. Além disso, alterar qualquer um passo, deve reiniciar o equipamento para ter efeito.



4.4.5 Estado Mestre

Estado Mestre tem dois tipos: fora ou dentro.

Estado mestre definir "Out" por padrão, e instalar em ambientes fechados; Estado Slaver definir "In" e instalar no exterior. Registros de fora são salvos no dispositivo mestre.

4.4.6 Modos de Verificação

O dispositivo suporta vários modos de verificação, incluindo impressão digital ou cartão de identificação (PF / RF), além de impressão digital ID (FP & RF), senha e cartão de identificação (PW & RF), impressão digital, senha (PW), Cartão de Proximidade (RF). Padrão modo de verificação é de impressão digital ou cartão de identificação (PF / RF).

Se você precisa escolher um modo de verificação, exceto o inadimplente, você pode entrar no Menu para modificar o modo de verificação em primeiro lugar. Os caminhos: Menu → Opções → Opções → Acesso Verifique MD.

4.5 Teste Automático

Selecione Teste de Auto e as informações exibidas na tela são mostrados na figura a seguir:



Através desse menu, você pode testar os componentes do sistema. A função de teste de auto ajuda a solucionar o dispositivo de forma rápida e facilita a manutenção do dispositivo.

Teste de LCD: O dispositivo testa automaticamente o efeito de seu display LCD e verifique se o seu LCD exibe imagens integrais.

Teste de Leitor impressão digital: O dispositivo testa automaticamente se o leitor de impressões digitais funciona corretamente, verificando. Depois de selecioná-lo, pressione "OK" para testar e verificar se ele normal. Pressione "ESC" para sair do teste.

Teste do teclado: Os testes de dispositivo se cada tecla do teclado funciona normalmente. Pressione qualquer tecla na interface [Test Teclado] para verificar se a tecla pressionada corresponde à chave exibida na tela. Pressione "ESC" para sair do teste.]

Teste Real Relógio de ponto (RTC): Os testes de dispositivos se o seu relógio funciona corretamente, verificando o cronômetro do relógio. Depois de selecioná-lo, pressione "OK" para testar e pressione "ESC" para sair do teste.

5. Gerenciamento USB Pen Drive

Selecione Gerenciamento Pen Drive e as informações exibidas na tela é mostrada na figura a seguir:



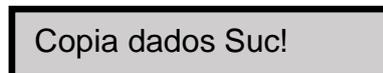
Você pode fazer o download dos dados de presença, os dados dos funcionários e mensagens curtas e carregar os dados dos funcionários e mensagens curtas com um pen drive USB.

5.1 Baixar dados de Presença

1. Insira um pen drive USB na interface USB no aparelho.
2. Selecione Pen Drive Mng e selecionar os dados de controle de acesso desejados para ser baixado através da tecla "▲ / ▼". A interface apresentada é mostrada como segue:



3. Pressione **OK** para confirmar sua seleção e iniciar o download. A interface exibida na bem-sucedida download são mostradas como se segue:

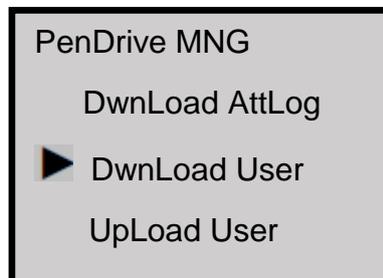


4. Pressione ESC para retornar à interface inicial e, em seguida, remover o pen drive USB. A forma de arquivos é **attlog.dat**.

☐ **Observação:** Se a transferência for bem sucedida, um aviso "Copiar dados Suc" irá aparecer. Se o sistema exibe o aviso "Plug Pen Drive?" Por favor verifica se o pen drive USB está conectado corretamente.

5.2 Baixar dados do usuário

Dados de download do usuário é semelhante ao download de registros de controle de acesso. Pressione ▲ / ▼ para selecionar "download usuário" no menu "Pen Drive Mng".

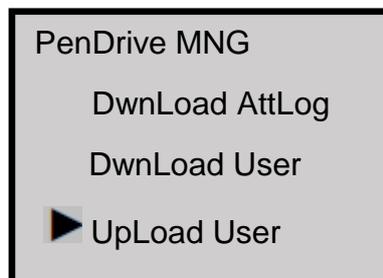


Os arquivos user.dat (informações do usuário), auth.dat usuário (privilegio de usuário) e timezone.dat (período de tempo) será simultaneamente transferido para o pen drive USB. Três arquivos de download ao mesmo tempo.

☐ **Observação:** Tem o download do nome do modelo da função de impressão digital dispositivo de impressão digital para "template.fp10".

5.3 Carregar Dados do Usuário

Pressione ▲ / ▼ para selecionar "Enviar Utilizador" do menu "PenDrive Mng" e pressione OK. Os arquivos user.dat (informações do usuário), userauth.dat (privilegio de usuário) e timezone.dat (fuso horário) armazenados no pen drive USB ser simultaneamente enviados para o dispositivo.



6. Sistemas de Informação

Através do menu Informação Sistema, você pode conferir todas as informações do dispositivo, incluindo a contagem de impressão digital registrada, os usuários inscritos, registros de frequência, registros administrativos e informações sobre o equipamento. Na interface do menu, selecione Informação Sistema e pressione OK para exibir a interface, como mostrado na figura a seguir:

Sistemas de Informação	
▶ Usuário Cnt	206
FP Cnt	173
Att Log	8046
Admin Cnt	0
Usuário Senha	1
S Logs	4096
Infor. Esp. Livre	
Infor. Dispositivo	

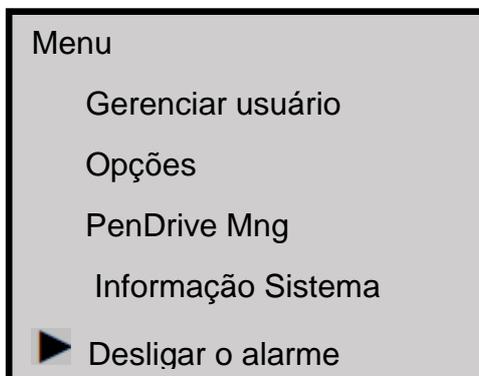
Na tela, como mostrado na figura acima, você pode conferir o Cnt Usuário (Número de usuários inscritos), FP Cnt (Número de impressões digitais registradas), Att Log (Parte de registros de frequência), Administração Cnt (Número de administradores inscritos), Senha Usuário (Número de senhas) e Super Logs (Número de super administradores inscritos). Através Espaço Livre Inf, você pode verificar o espaço livre no dispositivo de armazenamento.

Através Dev Info, você pode conferir informações como a capacidade de armazenamento, data de fabricação, número de série, fabricante, número da versão do algoritmo eo número da versão do firmware.

Infor. Dispositivo	
▶ FPCnt(100)	30
Attlog(10K)	10
S Logs	4096
Menu tempo	
Num serial	
Fornecedor	
Nome do Disp.	
Versão alg.	
Versão Firmware	
Ver MAC	
Versão MCU	

7. Desligar o alarme

A opção de desativar o alarme está disponível somente depois que o dispositivo gera um alarme e é usado para limpar um alarme. Caminho: Na interface do menu, selecione desativar o alarme.



□ **Observação:** A opção de desativar o alarme só está disponível depois de um sinal de alarme é gerado.

8. Manutenção

1. limpeza

Às vezes, a lente ótica, teclados e telas precisam ser limpos. Embora o específico o ciclo de limpeza é dependente do meio ambiente, em que o dispositivo opera, a seguir guia de manutenção pode ser de alguma ajuda para você:

Tabela 1-1 Manutenção Descrição:

Item	Limpeza
Teclados e exibição de telas	Limpe os teclados ou telas de exibição quando a superfície deles é suja ou as telas de olhar embaçado. Por favor, consulte as seguintes descrições.
Lente ótica	Não limpe a lente ótica com frequência. As lentes óticas funcionam melhor com óleo ou graxa. Limpe a lente ótica, se ficar embaçada e o desempenho de verificação é afetada. Por favor, consulte as seguintes descrições.

2. Limpe teclados e telas de LCD

Antes de limpar teclados e telas de LCD, desligue-o, limpe-os com um pedaço de pano úmido ou detergente neutro e, em seguida, limpe-os com um pedaço de pano seco.

3. Lente ótica Limpa

Siga as sugestões abaixo para limpar a lente ótica após desligar o dispositivo:

- 1) Sopre a poeira ou sujeira na superfície da lente ótica.
- 2) Limpe as telas com fita adesiva.

Aviso: Não limpe a lente ótica com água ou não neutro detergentes; pois a lente ótica pode ser danificada.

- 3) Limpe a lente óptica com um bom pano de microfibra. Tenha cuidado para não arranhar a lente. Se existem micro fibras à esquerda da lente, tente soprar-lhes depois a lente chegar seco.

9. Perguntas mais frequentes

1. Pergunta: Como faço para resolver o problema que alguns funcionários não conseguem passar a verificação de impressão digital na maioria das vezes?

Resposta: Os seguintes fatores farão com que a verificação de impressões digitais difícil ou mesmo impossível para alguns usuários:

- As impressões digitais de alguns dedos desgastam-se.
- Os dedos têm muitas rugas que mudam com frequência.
- A Pele sobre o dorso dos Dedos descola-se mal.

Para usuários cujas impressões digitais estão além do reconhecimento, eles podem excluir essas impressões digitais e inscrevê-los novamente ou registrar uma impressão digital de outro dedo. Recomenda-se para selecionar os dedos com boa qualidade de impressão digital (algumas rugas, não descascando e impressão digital distinta) para o registro de impressões digitais. Pressione o flatley dedo no sensor de impressão digital e ter certeza de que o bloco (não a ponta), abrange tanto a janela do sensor quanto possível. Realizar teste de jogo de impressões digitais depois de terminar a inscrição. Recomenda-se a inscrever as impressões digitais de vários dedos como backup.

Além disso, o dispositivo fornece as 01:01 de correspondência e verificação de senha funções especialmente para os usuários que têm dificuldade ou não pode passar a verificação de impressões digitais.

2. Pergunta: Quais são as possíveis causas da falha de comunicação do dispositivo?

Resposta: As possíveis causas são listadas a seguir:

- A configuração da porta de comunicação está incorreta. A porta de comunicação não é a porta de comunicação utilizada
- A configuração da taxa de transmissão da porta de comunicação do PC não é compatível com a do dispositivo.
- O dispositivo não está conectado com a fonte de alimentação ou o PC.
- O dispositivo está conectado com o PC, mas não ligado.
- O n^o do terminal conectado está incorreto.
- O cabo de dados ou conversor está com defeito.
- A porta COM do PC está com defeito.

3. Pergunta: Quais são as possíveis causas de exibição incompleta (meia tela às vezes display) ou a tela borrada depois que o dispositivo está ligado? Como corrigir isso?

Resposta: As possíveis causas são listadas a seguir:

- A placa principal está com defeito.
- O visor LCD está com defeito.

Em qualquer um dos casos acima, você precisa entrar em contato com o fornecedor e devolver o aparelho para conserto.

4. Pergunta: Como posso excluir administrador?

Resposta: Você pode pressionar **Menu de Opções—SymsOpt— Adv option— Clr Modifique Pri** excluir administrador.

Além disso, Ligue o dispositivo com um PC e estabelecer a comunicação entre eles. Selecione a guia de gerenciamento de dispositivo e clique em Excluir administrador para apagar o administrador do dispositivo. Você pode acessar o menu do dispositivo depois de desligar o aparelho com o PC.

5. Pergunta: Por que há um som de bipe durante a comunicação entre o dispositivo eo PC?

Resposta:

- Se o sinal sonoro ocorre em modo de comunicação RS232, as configurações de velocidade de transmissão do PC e do dispositivo são inconsistentes.
- Se o sinal sonoro ocorre no modo de comunicação RS485, é possível que os dois cabos de comunicação do conversor são inversamente ligada ou presos juntos.

6. Pergunta: Por que razão o aparelho constantemente exibir "por favor prima (retirar) o dedo novamente"? Como corrigir isso?

Resposta: As possíveis causas são as seguintes:

- Há sujeira, graxa ou arranhão na superfície do sensor de impressões digitais, o que pode levar o sensor de impressão digital por engano pensar que há um dedo pressionando na superfície. Remover a sujidade ou gordura na superfície do sensor de impressões digitais com uma fita adesiva.
- O cabo de conexão do sensor de impressão digital vem solto ou desconectado.
- O chip da placa principal está com defeito.

Nos últimos dois casos, entre em contato com o fornecedor e devolver o aparelho para manutenção.

7. Pergunta: Por que não uma falha ou erro ocorre quando eu ler os dados de participação enquanto posso baixar impressão digital e senha os dados corretamente? Como corrigir isso?

Resposta: Este problema pode estar relacionado com o cabo de dados, conversor ou a configuração da porta COM do PC. Você pode tentar diminuir a taxa de transmissão do PC e um dispositivo, por exemplo, configurá-lo para 19200 vs 9600 antes de ler os dados de frequência novamente.

10. Apêndice

As funções descritas no Anexo são todos opcionais. Se você precisa dessas funções, consulte os nossos representantes comerciais ou pré-vendas engenheiros de suporte técnico.

10.1 USB

USB Host

O dispositivo é usado como o host USB para conectar externamente com um pen drive USB para troca de dados. Os leitores de impressões digitais convencionais transferir dados somente através da RS232, RS485 ou Ethernet. Dados em massa transferência pode demorar muito tempo, devido à restrição das condições físicas. O USB para supera quaisquer outros modos de transferência anteriores, em termos de taxa de transferência de dados. Insira o pen drive USB ao slot USB no dispositivo, download de dados para o pen drive USB, e, em seguida, conecte o pen drive USB ao computador para importar os dados para o computador. Além disso, o dispositivo também suporta a troca de informações do usuário e os dados de impressões digitais entre dois dispositivos, o que ajuda a dispensar o trabalho de conexão de cabo convencional para transferência de dados entre o dispositivo e computadores.

Para as operações do dispositivo usado como o host USB, consulte Gerenciamento de [5.USB Pen Drive](#)

USB Cliente

Conectar o dispositivo com o PC como o dispositivo de armazenamento móvel, e transferir os dados armazenados no dispositivo para o PC através do cabo de ligação.

Quando o dispositivo é usado como o cliente USB, as opções de comunicação USB será exibido no menu de configuração de comunicação do dispositivo. Para mais detalhes, consulte [4.3 Configurações de comunicação relacionados](#)

Nota: Quando o aparelho se conecta com o PC como o cliente USB, o PC deve ser instalado com o driver relacionado.

10.2 Agendada de Bell

Muitas empresas precisam para tocar os sinos para marcar o início e o fim dos turnos de trabalho, e eles geralmente manualmente os sinos anel elétrico ou use os sinos. Para poupar custos e facilitar a gestão, nossa empresa integra a função Campanha programados dentro do dispositivo. As opções Sino Sino atraso e Segmento de Tempo estão disponíveis sobre os dispositivos que suportam a função Campanha regulares. Existem 8 segmentos de tempo disponível todos os dias da semana. Você pode definir o tempo de toque conforme necessário. O dispositivo irá tocar automaticamente no horário especificado em cada semana e parar o anel após anel tempos de duração.

O aparelho toca a campanha nas seguintes formas:

Toque o sino no alto-falante configurado no dispositivo.

Ligue uma campanha elétrica para o dispositivo. O dispositivo irá enviar um sinal de relé para acionar a campanha elétrica no horário especificado.

10.3 Conexão Externa com o Leitor de Impressões Digitais

Esta função é especialmente para os dispositivos configurados com as interfaces USB. Inserir o leitor no slot USB, selecione o leitor de impressão digital Menu → Opções → Adv Opção → Conexão com leitor FP e defina a opção Conectar-se com leitor de Y. depois, o conectado externamente leitor de impressão digital e o leitor de impressões digitais integrado do dispositivo podem ser usadas em simultâneo.

Quando utilizado para o tempo & gestão de assiduidade, o conectado externamente leitor de impressões digitais pode ajudar drenar alguns dos usuários no pico time; quando utilizado para o controle de acesso, o leitor biométrico conectado externamente pode ser colocado fora da porta e o host é colocado no seu interior, que não só implementa o controle de acesso biométrico tanto no interior como no exterior da porta, mas também garante a segurança do servidor.

- 1) Depois de ligado, o leitor de impressões digitais só pode ser utilizado após a reinicialização.
- 2) Apenas os leitores de impressão digital com a licença SDK pode ser usado para conexão externa.

10.4 Funções GPRS

O GPRS (General Packet Radio Service) é um novo serviço de suporte pacotes de dados desenvolvidos com base no Sistema Global para Comunicações Móveis (GSM). Como o pacote sistema de comutação, o GPRS é especialmente adequado para intermitente e esporádica ou pacotes pequenos e frequentes e a transmissão de dados também é adequada para transmissão de dados volumosos ocasionais. Este recurso é ideal para a maioria das aplicações móveis, por exemplo, o escritório móvel e acesso à Internet.

Para obter informações detalhadas sobre as operações GPRS, veja as instruções de operação.

10.5 Funções WIFI

Funções Wi-Fi Wireless Fidelity (WiFi) é também conhecido como o padrão 802.11b. A maior vantagem de WiFi é a sua alta taxa de transmissão de até 11Mbps. Wi-fi também apresenta a distância de transmissão longa e excelente compatibilidade com diversos dispositivos 802.11 DSSS existentes. IEEE 802.11b é um rádio base variante de IEEE 802.11. A largura de banda IEEE 802.11b pode ser de até 11 Mbps e automaticamente ajustado para 5,5 Mbps, 2 Mbps e 1 Mbps e pendente a força do sinal e nível de interferência, garantindo efetivamente a estabilidade da rede e confiabilidade. Principais vantagens: Alta velocidade de transferência e confiabilidade. A distância de comunicação pode ser de até 305 m em área aberta e 76 m a 122 m em uma área fechada. WiFi pode ser convenientemente integrados com a telefonia convencional existente Ethernet, tornando a rede custo ainda menor.

Nosso dispositivo também é capaz WiFi. Ele suporta módulo Wi-Fi ou embutido ou externo para implementar a transmissão de dados sem fio sobre o WIFI.

Para operações detalhadas Wi-Fi, veja as instruções de operação relacionadas.

10.6 Consulta atendimento

Você pode consultar os dados de participação de um indivíduo ou todos os empregados diretamente no dispositivo que suporta o atendimento consulta recurso. Isso ajuda a eliminar o

incômodo de instalação de software e dispositivos de ligação para o atendimento o download e consulta, e facilita os funcionários para consulta os seus próprios dados de participação. Pode consultar os dados de frequência de não apenas um indivíduo, mas também todos os funcionários no dispositivo.

10.7 Descrição da função MP3

A função MP3, que permite a reprodução de músicas MP3, hifi, decodificação em tempo real arquivos MP3, com um leitor de MP3. Os dispositivos compatíveis com MP3, um formato MP 3 players para reproduzir MP3, arquivos de voz do MPEG 1.0: formato. Semelhante à programada bell, a função MP3, permite que os usuários para definir 8 segmentos de tempo e reproduz automaticamente arquivos em MP3, segmentos de tempo especificado pelo usuário.

Você também pode definir um arquivo MP3, para marcar o início do trabalho e ao meio-dia romper, ou colocar um anúncio em um arquivo MP3, para o dispositivo para jogar no horário especificado, tornando assim o seu escritório mais amigável-empregado.

O dispositivo ou pode reproduzir arquivos MP3 através de seus próprios alto-falantes ou através de uma caixa de som externa. Há 8 segmentos de tempo disponíveis para você selecionar. Você pode definir o segmento de tempo, conforme necessário. O dispositivo reproduz automaticamente um arquivo MP3 no segmento de tempo especificado.

10.8 Mensagem Curta

Alguns modelos de dispositivos oferecem suporte à transferência de público e privado as mensagens curtas no tempo especificado e para um determinado indivíduo. Você pode editar ou mensagens curtas através do software em segundo plano e, em seguida, transferi-los para o dispositivo. O público mensagens curtas são exibidas na tela o tempo todo quando o dispositivo é ligado, enquanto as mensagens curtas são exibidas mediante a verificação de impressões digitais.

Uma mensagem curta para uma pessoa: por exemplo, se um funcionário o dia do aniversário é dia 20 de Outubro, em seguida, você pode editar uma mensagem curta "feliz aniversário para você!" por meio do software em segundo plano, carrega a mensagem curta para o dispositivo, e configurá-lo para ser exibido no dia 20 de Outubro. Esta mensagem será exibida na tela quando esse funcionário verifica a sua impressão digital.

Uma mensagem curta para um grupo de funcionários: por exemplo, para uma reunião plenária prevista para ser realizada no dia 19 de Junho, você pode editar uma mensagem curta "Por favor, participe da reunião plenária em x xx x xx a sala de reunião" (você pode editá-lo conforme necessário) através do software em segundo plano e carregá-lo para o dispositivo. Em seguida, no dia 19 de Junho, esta mensagem curta será exibida o tempo todo na tela quando o dispositivo está ligado

Configuração de mensagens curtas: Após a definição da mensagem curta no atendimento software, carregá-lo para o dispositivo. O dispositivo suporta a importação de mensagens curtas em dois modos:

- Importação direta, ligando o software para o dispositivo.
- Importação a partir de um pen drive USB.

Descrição de funcionamento:

1 Editar uma curta mensagem, selecionando o SMS Programa → Mng externo menu item do atendimento software, conectar o atendimento software e carregá-lo para o dispositivo.

2 Editar uma curta mensagem, selecionando o SMS Programa → Mng externo menu item do atendimento software. Selecione externo Pen Drive Mng → Programa → Exportação → Exportação para Pen Drive para exportar a curta mensagem editada para o pen drive USB. Insira o pen drive USB no slot do dispositivo mediante exportação bem-sucedida e, em seguida, selecione Menu → Pen Drive GNV → Carregar o SMS para carregar a mensagem curta de o pen drive USB.

Exibição de mensagens curtas: Público mensagens curtas são exibidas o tempo todo na tela quando o dispositivo está ligado. Private mensagens curtas são exibidas mediante verificação de impressões digitais.

□ **Observação:** Você pode enviar um máximo de 1024 mensagens curtas públicas ou privadas para o dispositivo.

10.9 Vários modos de verificação

Atualmente, o dispositivo fica aquém das exigências de alta segurança controle de acesso, fornecendo a impressão digital única, apenas senha e ID + modos verificação de impressões digitais. Rica em recursos para fornecer sistemas de controle de acesso, que suporta a personalização de vários modos de verificação para os indivíduos ou grupos para atender as mais rígidas exigências de segurança dos clientes. Para além da impressão digital, senha e ID + impressão digital modos de verificação, o dispositivo também suporta uma combinação do ID (PINO), impressão digital (FP), uma palavra-chave (PW) e RF verificação de atingir até 15 modos de verificação, conforme listado nas tabelas a seguir.

1) Mifare pode ser considerado como RF no processo de verificação e verificação do cartão Mifare está disponível apenas para dispositivos compatíveis com cartão Mifare

2) Com exceção de alguns dispositivos de modelos específicos, a B&W os dispositivos da série tela suporte apenas a impressão digital e senha modos de verificação. A Mifare cartão dispositivos capazes também de apoiar a verificação do cartão Mifare para além da impressão digital e senha modos de verificação. .

3) O dispositivo suporta até 15 modos de verificação para atender as exigências de clientes diferentes. " / " significa " ou", " & " significa "e" e "←", confirmação (OK).

Os usuários se inscrever as suas impressões digitais e senhas do dispositivo. Os modos de verificação estão listados a seguir:

Tipo	Descrição
FP	Apenas a verificação de impressão digital
	1) PIN+FP (1: 1)
	2) FP (1: N)
	3) RF+FP (1: 1)
PIN	Apenas ID, número de verificação
	Os usuários podem passar a verificação, desde que digitar seus números de identificação por meio de teclado, independentemente de seus modos de inscrição.

Senha	Apenas verificação de senha 1) PIN+“←”+ PW 2) RF+ PW
RF	Apenas a verificação do cartão RF 1) RF
FP/PW	Impressão digital ou senha de verificação 1) PIN + FP (1: 1) 2) FP (1: N) 3) PIN + "←" + PW 4) + RF PW
FP/RF	Impressão digital ou RF verificação 1) PIN+FP(1:1) 2) FP(1:N) 3) RF
PW/RF	Senha ou RF verificação 1) RF 2) PIN+“←”+PW
FP/PW/RF	Impressão digital ou senha ou RF verificação 1) PIN+FP(1:1) 2) FP(1:N) 3) PIN+PW 4) RF
PIN e FP	Número de identificação e verificação de impressões digitais 1) PIN+“←”+FP(1:1) 2) RF+ PIN+“←”+FP(1:1)
FP&PW	Impressão digital e senha de verificação 1) FP(1:N)+PW 2) PIN+FP(1:1)+PW 3) RF+PW + FP(1:1)
FP&RF	Impressão digital e RF verificação 1) RF+FP(1:1) 2) FP(1:N)+RF 3) PIN+FP(1:1)+RF
PW&RF	Senha e RF verificação RF+PW PIN+“←”+PW+RF

10.10 EM Readonly Card, cartão HID, Mifare cartão, cartão iClass

Para acomodar a demanda do mercado para o RF atualmente populares cartões, temos desenvolvido o dispositivo com termômetros builtin RF EM Módulo leitor de cartão. Por meio da integração EM readonly card, esse dispositivo pode ser convenientemente consolidado no telefone já existente, refeitório POS e sistema de controle de acesso. Este dispositivo suporta vários modos de verificação incluindo a verificação de impressões digitais, verificação de senha, verificação do cartão, cartão + verificação de impressão digital e Cartão + verificação de palavra-passe para satisfazer as necessidades de clientes diversificada.

EM Readonly Card

O EM Readonly placa suporta espessa (1,88 mm), fino (0,88 mm) e mediumthickness (1,05 mm) ID/trabalhar com cartões EM frequência de 125 kHz e cartão distância de leitura de 5m.

HID cartão

Para atender à demanda do mercado para o RF atualmente populares cartões, temos desenvolvido o dispositivo com termômetros RF Módulo leitor de cartões HID. Através da integração do cartão HID readonly, este dispositivo pode ser convenientemente consolidado no telefone já existente, refeitório POS e sistema de controle de acesso. Este dispositivo suporta vários modos de verificação incluindo a verificação de impressões digitais, Verificação de senha, verificação do cartão, cartão + verificação de impressão digital e Cartão + verificação de palavra-passe para satisfazer as necessidades de clientes diversificado

O dispositivo suporta cartões HID trabalhar com frequência de 125 kHz e cartão distância de leitura de 2m a 5m.

Cartão Mifare

Para acomodar a demanda do mercado para o RF atualmente populares cartões, temos desenvolvido o dispositivo com termômetros RF Módulo leitor de cartão Mifare. Através da integração do cartão Mifare, o dispositivo pode ser convenientemente consolidado no telefone já existente, refeitório POS e sistema de controle de acesso. Este dispositivo suporta vários modos de verificação incluindo a verificação de impressões digitais, Verificação de senha, verificação do cartão, cartão + verificação de impressão digital e Cartão + verificação de palavra-passe para atender a diversidade às necessidades do cliente.

O dispositivo suporta MIFARE termômetros cartões inteligentes com frequência de 13,56 MHz e placa distância de leitura de 3m a 5m.

Para as operações do Mifare cartões, consultar Cartão Mifare Guia do Usuário.

Cartão iCLASS

Para atender à demanda do mercado para o popular atualmente cartões iClass, temos desenvolvido o dispositivo com termômetros RF Módulo leitor de cartão iClass. Através da integração do cartão iClass, o dispositivo pode ser convenientemente consolidado no telefone já existente, refeitório POS e sistema de controle de acesso. O dispositivo suporta vários modos de verificação incluindo a verificação de impressões digitais, verificação de senha, verificação do cartão, cartão + verificação de impressão digital e Cartão + verificação de palavra-passe para satisfazer as necessidades de clientes diversificada

O dispositivo suporta gravação/leitura iClass termômetros cartões inteligentes com o trabalho frequência de 13,56 MHz e placa distância de leitura de 2m a 5m.

10.11 Função mestre/escravo

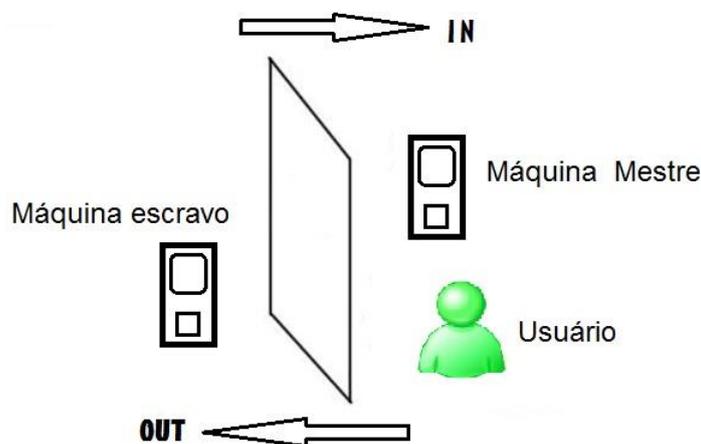
Dois dispositivos, um mestre e um escravo, quer controlar a mesma trava, estão ligados por RS232/RS485/Wiegand.

1. As aplicações do Mestre e o Escravo

1) Armazenamento de registros:

Por padrão, o estado do mestre é saída e a condição de escravo é de entrada. Os registros de entrada e saída são ambas gravadas no mestre.

2) função antipassback:



Se ao executar o antipassback função é determinada pelo último registro da entrada do usuário e sair. Com esta função, a saída registro deve corresponder ao registro de entrada. A função suporta "Para Fora", "no", "dentro e fora", "Nenhum e salvar" ou "Nenhum" antipassback. Por padrão, o status de identificação do mestre é sair e o do escravo é entrada, de modo que se "out antipassback" foi definido e quando o último registro da entrada do usuário não é "entrada", o sistema irá solicitar antipassback recusa" e recusam-se a abrir a porta, se o usuário quer sair. A lógica é a mesma com "out antipassback" e "in & out antipassback".

Por exemplo, agora quer sair.

- ① Se o último registro de UM não é entrada, o dispositivo irá solicitar antipassback recusa e recusam-se a abrir a porta.
- ② Se o último registro para A é entrada, após a identificação de impressões digitais é passado, o dispositivo irá abrir a porta.

3) função de alarme

Se o escravo é equipado com função de alarme (por ex. F10), quando um alarme incidente ocorre, o escravo irá encaminhá-lo para o mestre para o processo. Não existe essa função no aparelho que não é equipado com função de alarme.

2. A ligação do Mestre e do Escravo

Atualmente, três modos—RS232, RS485, Wiegand são aplicáveis para a ligação do mestre e do escravo. Dos três, O RS232 é menos frequentemente utilizado devido a sua deficiência que a sua distância de conexão é curta. Por exemplo, ele pode ser usado quando o mestre e o escravo são apenas instalados, respectivamente, dentro e fora de uma porta. O seu princípio de ligação é semelhante ao da RS485 integrada, que é omitido aqui. A conexão Wiegand é amplamente utilizado a maioria dos seus dispositivos no mercado são aplicáveis para o mestre e o escravo. RS485 integrada, cuja distância de transmissão é grande (no entanto, recomenda-se que a distância não

deve ser superior a 600 metros), aplica-se a maioria das vezes, mas o escravo deve ser equipado com o inBIO leitor (que é usado para coletar impressões digitais ou passando cartão).

Se conexão Wiegand é para ser usado, a conexão e configuração de antipassback são as seguintes:

1) Selecione o modelo:

Mestre máquina: Máquina com Wiegand na função, exceto para F10 Reader.

Escravo da máquina: Máquina com função Wiegand Out.

2) Menu configuração mestre-escravo.

Esta máquina oferece suporte para out, in, no, Não, não e salvo antipassback (entrar no Menu > Definições > Configuração do sistema > Configurações avançadas > antipassback).

3) Modificar o formato de saída Wiegand do dispositivo:

Se os dois aparelhos estão se comunicando, apenas sinais Wiegand sem ID do dispositivo pode ser recebido. Digite dispositivo Menu > comum. Optar por > opção ou digite Wiegand software: configuração básica > gestão > dispositivo Wiegand, para modificar "formato definido como "wiegand26 sem ID de dispositivo".

4) Inscrever usuário:

O usuário deve estar no mestre e escravo máquina ao mesmo tempo, e o usuário deve ser o mesmo. Para isso, é necessário se inscrever no mestre e escravo máquina e máquina ao mesmo tempo.

5) Instruções de conexão:

Comunicação Wiegand é adotado para o mestre e escravo máquina. Consulte os seguintes documentos para ligação:

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

Se conexão RS485 está a ser utilizado, a conexão e configuração de antipassback são as seguintes:

O modo de RS485 é uma nova aplicação no âmbito do mestre e escravo. Neste modo, as informações do usuário, verificação de impressões digitais, verificação de cartão e a autoridade verificação são todas processadas no mestre. E o escravo é usado apenas como um colecionador. Portanto, o software só precisa para gerenciar as informações do usuário e registrar informações sobre o mestre.

Escolher Dispositivos:

O mestre: ele deve ter função 485 de comunicação (atualização de firmware necessários). O escravo: ele deve usar o inBIO leitores (leitor responsável apenas para recolher impressões digitais, como o F11 e o SR 200).

Configurando o menu do mestre:

Definição do mestre:

Acesse Menu> Configurações> Configurações do sistema> Configurações avançadas> Antipassback.

A configuração pode ser "Out", "In", "In Out", "Nada e salvar" ou "Nenhum".

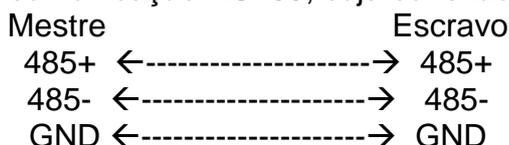
Acesse Menu> Configurações> Opções de acesso> 485 leitores. Se "Sim" é escolhido, a função de mestre e escravo de 485 modos é iniciado e ao mesmo tempo é a função de comunicação com o PC é proibido. Se "Não" é escolhido, a máquina funciona normalmente a função de comunicação de PC.

Definir o escravo:

Defina o número do dispositivo, idêntica à do mestre.

3) Conectando o mestre e o escravo

O mestre e no escravo são para comunicação RS485, cuja conexão é mostrado como na figura:



3. O uso do Mestre e o Escravo

Depois que os aparelhos são iniciados, o mestre funciona da mesma forma que controle de acesso comum. O escravo não pode verificar. Quando uma impressão digital é pressionada ou um cartão é apertada sobre o escravo, o indicador irá piscar e "clique, clique em "som para avisar e o resultado da verificação será exibido no máster.

10.12 Identificação Remota do Servidor (RIS)

Devido à capacidade e velocidade as limitações, é improvável para armazenar uma boa quantidade de impressões digitais (por exemplo, milhares de impressões digitais) off-line sobre o dispositivo. Mesmo se o dispositivo é altamente escalável, o off-line velocidade de funcionamento do dispositivo é muito lento, por oposição ao PC. Portanto, o off-line RFT fica aquém das necessidades levantadas por alguns grandes sistemas de verificação de impressão digital grande capacidade de armazenamento e alta coincide com eficiência.

Princípio de funcionamento do RIS

A RIS solução usa o dispositivo como o leitor de impressões digitais, ao mesmo tempo em que mantém sua função de verificação off-line. Usando a função de rede do dispositivo, que envia os dados, tais como a verificação de impressões digitais e modelos Imagens das impressões digitais para o fundo para a verificação, armazena resultados de verificação em segundo plano banco de dados e exibe-os na tela LCD do aparelho.

A RIS solução é especialmente adequado para grandes bancos de fábricas com um colaborador de 1.000 a 3.000 funcionários, fazendo acompanhamento apontamento altamente eficiente. Além disso, para resolver a questão da mobilidade do pessoal, propomos também a zona e soluções. Dividindo-se logicamente locais de servidor e dinamicamente identificar mobilidade de pessoal, o dispositivo percebe livre mobilidade de pessoal e dispensa configurações manuais. A solução DNS desenvolvido com base no DNS garante estável sistema em execução e até mesmo e alocações de recursos eficientes, mesmo em caso de explosão de tráfego.

RIS Arquitetura

O modo básico do RIS é client/server (c/s) modo, conforme mostrado na figura a seguir. O dispositivo serve apenas como leitor de impressões digitais e envia as impressões digitais para o RIS. A RIS verifica os modelos de impressão digital do dispositivo por tirar proveito da poderosa capacidade de processamento do PC, armazena os resultados de verificação no centro banco de dados e retorna-los para o dispositivo para exibir ao mesmo tempo. Neste momento, a velocidade de verificação do dispositivo é menor do que 2s quando o número total de impressões digitais é 5000.

RIS Operação Descrição

Definição de Menu

Selecione o Menu → Opções → Sistema Opt → Adv RIScapable Opção sobre o dispositivo e você pode ver as duas opções a seguir:

Depois que o dispositivo for conectado com sucesso com o RIS, selecione Menu → Usuário Gerenciar → Matricular Usuário e opção a seguir é exibida:

Matricular Remoto FP: O registro de impressão digital remoto está disponível após esta opção é definida como Y.

Software RIS

O software RIS inclui três partes: registro de impressão digital, verificação de configuração pessoal do servidor e do servidor de verificação de impressões digitais.

10.13 Controle de Acesso do Servidor Web

Visão geral de Software de Controle de Acesso do Servidor Web

O servidor Web sistema de controle de acesso é a coleta de dados/sistema de controle de acesso baseado em servidor Web tecnologia e apoiada pela rede TCP/IP standard estrutura. Ele adota a política solicitações de páginas da Web para processar e gerenciar dados. Ela está livre de restrições geográficas e não requer a instalação de qualquer outro software. Você pode fazer o download do empregado os dados armazenados no terminal biométrico remoto através de vários tipos de navegadores como o IE e o Netscape, e preparar relatórios estatísticos para gestão empresarial e na tomada de decisão. Com o controle de acesso do Web Server software, os clientes podem realmente ter sincronização em tempo real, em qualquer lugar e a qualquer momento.

Papel do Servidor da Web Incorporado
Veja iClock Presenças.

Uso de Software de Controle de Acesso Webserver

Ao usar o software de controle de acesso servidor web, você precisa configurar o endereço IP do dispositivo, por exemplo, 192.168.1.115. Em seguida, digite `http://192.168.1.115` na barra de endereços do IE. O nome de usuário padrão do super-administrador é "admin" e a senha é "admin888".

Para mais informações sobre o servidor web software de controle de acesso, consulte Controle de Acesso Webserver Especificações de Software.

10.14 Coletas automática de endereços IP

É possível que o administrador pode esquecer os endereços IP dos dispositivos quando vários dispositivos são geridos na mesma LAN. Para remover o incômodo da consultando os endereços de IP de dispositivos, um por um, se desenvolve um tipo de software que recolhe automaticamente os endereços IP dos dispositivos da LAN.

Tudo que você precisa é copiar todos os arquivos DLL para o diretório System32 do sistema, e selecione Iniciar → Executar para executar `regsvr32 zkemkeeper.dll`. Depois que o sistema solicita o sucesso de inscrição, clique duas vezes `DeviceSearch.exe` para executar o software.

10.15 Protocolo Wiegand

Wiegand26 é um controle de acesso protocolo estabelecido pelo padrão do Controle de Acesso Standard Subcomissão afiliado ao Setor de Segurança Associativo (IEA). Trata-se de um leitor de cartão IC termômetros interface e protocolo de saída.

Wiegand26 define a interface entre o leitor de cartão e o controlador usados no controle de acesso, segurança e outras áreas industriais. Wiegand26 ajuda a padronizar o trabalho dos designers e leitor de cartão controlador dos fabricantes. O dispositivo também é projetado em conformidade com Wiegand26.

Sinais Digitais

A Figura 1 é um diagrama de sequência em que o leitor de cartão envia sinais digitais no formato bit ao controlador de acessos. Neste diagrama de sequência, segue o PEI Wiegand controle de acesso do protocolo padrão para o 26bit Wiegand leitor de cartão (um pulso intervalos de tempo entre 20 e 100 ° -us, e o pulso saltar intervalos de tempo entre 200 e 20ms).

Dados1 e Dados0 são de alto nível (maior do que V_{oh}) sinais até o leitor de cartão prepara para enviar um fluxo de dados. O baixo nível assíncrono pulso (mais pequeno do que V_{ol}) gerado pelo cartão leitor é enviado ao painel de controle de acesso (O dente de serra onda conforme mostrado na Figura 1) através Dados1 ou Dados0.

Dados1 e DATA0 pulsos vai nem sobrepor-se nem ser gerado de forma síncrona. A Tabela 1 lista o máximo e largura de pulso mínima (um impulso consecutivo) e tempo de pulso salto (tempo entre os pulsos) permitidos pela F séries de impressões digitais terminal de controle de acesso

Tabela 1 Tempo de Pulso

Símbolo	Definição	Valor típico do Reader
T_{pw}	Largura de Pulso	100 μ s
T_{pi}	Intervalo de impulso	1 ms

Formato Wiegand

O formato Wiegand adotado pelo dispositivo é o protocolo de controle de acesso universal.

Formato 26 Bit Wiegand

A composição do abrir de facto Weigand 26 bits padrão da indústria contém 8 bits para o código de instalação e 16 bits para o número de identificação. Matematicamente, este 8º fábrica códigos permite um total de apenas 256 (de 0 a 255) fábrica os códigos, enquanto o número de ID 16 bits permitem um total de apenas 65.536 (de 0 a 65. 536) OU SUPERIOR da identificação individual dentro de cada código de instalação.

26Bit Formato Wiegand é de 26 bits de comprimento, incluindo 2 bits para bits de paridade.

1	2	9 10	25	26
EC	FC	CC	OP	

10.16 Função POE

1. visão global

Power over Ethernet (POE) é uma tecnologia que permite que energia DC junto com os dados a serem fornecidos ao Ethernet base equipamento terminal (como um telefone IP ou um ponto de acesso de rede sem fio) sem quaisquer alterações no cabeamento Ethernet atual arquitetura. Um sistema POE consiste essencialmente de dois grandes componentes; o equipamento de fornecimento de energia (PSE), que fornece energia, e dispositivos de energia (PDS), que receber e usar o poder. POE integra-se energia e dados no mesmo sistema de cabeamento, e fornece dados e alimentação DC através de uma Cat5/5E cabo.

2. Aplicação

Se você conectar um dispositivo com um builtin módulo POE ao sistema POE, o dispositivo pode funcionar corretamente, usando a energia fornecida pelo sistema POE sem qualquer adaptador de energia. Assim, ele não só economiza dinheiro, mas também facilita instalação e cabeamento. A Tabela 1 apresenta as definições de cabos RJ45 do dispositivo após o acesso do módulo POE.

Tabela 1 Pin Definição de RJ45

O pino (soquete entalhe para top; da direita para a esquerda)	Definição
1	TX+
2	TX-
3	RX+
4	Power
5	Power
6	RX-
7	GND
8	GND

10.17 Bateria reserva (Mini-UPS)

UM pré-requisito para um bom trabalho do dispositivo é a fonte de alimentação normal em todos os casos. Para além de adaptadores de energia, nós também fornecemos 5V e 12V MiniUPSs que podem reduzir o impacto da falta de energia como resultado de problemas de fontes de alimentação no funcionamento do dispositivo para a maior medida.

1. princípio de funcionamento

Normalmente, a bateria de backup continua em estado de marcha lenta, e o adaptador de energia converte corrente alternada em corrente contínua fonte de alimentação para o dispositivo. Se a bateria de backup é a transferida insaturada, a bateria será carregada automaticamente. Em caso de falha de energia, a bateria de backup irá mudar automaticamente para o estado de descarga para o fornecimento de energia ao dispositivo.

2. Modelo

5V Mini UPS

Entrada: dc5v-2A

Saída: DC5V-0.8A

Tempo para carregar: ≥ 7.5 H

Tempo de descarga: $3,0 \pm 0,5$ H

Indicador: indicador vermelho está ligado durante a carga. O indicador verde se acende quando a bateria está saturada.

12V Mini UPS

Entrada: DC12V / 2A

Saída: DC7-12V / 0.8A

Tempo para carregar: ≥ 5.0 H

Tempo de descarga: $3,0 \pm 0,5$ H

10.18 9 Dígito Número da inscrição

A IDs de usuário padrão suportado pelo dispositivo para registro do usuário são 5 dígitos (variando entre 1 e 65534). Na prática, os clientes podem requerer que o usuário IDs com dígitos mais de 5 dígitos. Nós podemos personalizar os dispositivos que suportam 9dígitos IDs de usuário para atender às suas necessidades.

10.19 Calibração Automática da Hora

Tendo em conta a enorme carga de trabalho de um em uma calibração em tempo de vários dispositivos em uma rede, você pode especificar um dispositivo ou PC, esta rede, como um servidor de horário, e defina a opção de calibração automática da hora do calibrados dispositivos para o endereço IP do servidor de tempo especificado. Em seguida, outros dispositivos irão conectar-se automaticamente com o servidor para calibração de tempo. Você só precisa garantir que todos os dispositivos podem acessar o servidor de tempo.

Por exemplo, vários dispositivos em um suporte de rede a função de calibração automática da hora. Defina o dispositivo para o servidor de tempo. O tempo de exibição do dispositivo A é 11:00h de 28

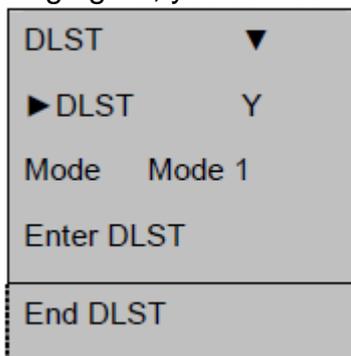
de Outubro de 2006, e seu endereço IP é considerado "192.168.1.100 ". Que você precisa para definir o tempo de todos os dispositivos na quantidade de M nesta rede para estar em sincronia com o dispositivo. Acessar esses dispositivos e selecione **Menu** → **Opções** → **Sistema Opt** → **Adv Opção**. No exibido [Adv Opção] interface, verifique se a opção de calibração automática da hora e ajuste-o para o endereço IP do servidor de horário. Depois de completar essas configurações, reinicie os dispositivos. Esses dispositivos irá procurar automaticamente o servidor de hora depois de um período de tempo, para manter em sincronia com a hora do servidor.

10.20 Horários de Verão (configurações de fuso horário)

O horário de verão (DLST) é um amplamente utilizado sistema de ajustar o horário oficial local frente para poupar energia. O uniforme, tempo adoptou durante a implementação deste sistema é conhecido como o DLST. Normalmente os relógios são ajustados para a frente uma hora no verão para fazer com que as pessoas mais cedo para a cama e cedo para subir, por forma a fazer pleno uso da iluminação recursos e poupar eletricidade. Os relógios são ajustados para trás no Outono. DLST regulamentos específicos variam de acordo com os países. No momento, o sistema é adoptado DLST cada ano por cerca de 110 países em todo o mundo.

Para atender a exigência DLST, o aparelho suporta a função DLST para ajustar a uma hora de x xx (horas): x xx (Minuto) xx (Dia) x x (Mês) e para trás uma hora a xx (horas): xx (Minuto) xx (Dia) x x (Mês).

On the interface as shown in the following figure, you can set the DLST.



Para ativar o DLST, selecione Y e pressione OK; para desativar o DLST, selecione N

Depois de ativar o DLST, você precisa definir os eventos relacionados com o início e final do DLST. Você pode definir dois modos para a DLST formato: Modo 1 e o modo 2.

No Modo Padrão 1, o DLST E Definido não Formato de "Mês Dia Hora: Minuto".

No Modo 2, o DLST E Definido não Formato de "Mês Semana Dia Específico da Semana Hora: Minuto".

O valor da semana passada (WS): 1 - 6. 1, A primeira semana, 2º da segunda semana e assim por diante e assim por diante. O valor do dia (WK): 0 - 6. 0 Meio domingo, 1, segunda-feira, e assim por diante e assim por diante.

Vamos dar 4:00 1 de setembro de 2008 (ou seja, sábado da primeira semana de setembro de 2008) como um exemplo para ilustrar esses dois modos:

MM-DD 24H 9-1 04:00	MM-WS-WK 24H 9-1-6 04:00 WK (0:Sun 6:Sat)
ESC OK	ESC OK
Mode 1	Mode 2

10.21 Reproduzir voz dentro de um prazo determinado segmento (segmento de tempo ou de um grupo)

Quando o usuário aciona o dispositivo, o dispositivo tem comandos de voz. Por exemplo, o dispositivo vozes "Obrigado!" depois que o usuário passa a verificação de impressão digital, e as vozes "tente novamente!" se o usuário não passar a verificação.

Para fazer os dispositivos de uma forma mais acessível, podemos permitir que os dispositivos para reproduzir o especificado prompts de voz em resposta às diferentes operações do utilizador.

Por exemplo, se o empregado sinais durante 6:00h -08:00, o dispositivo será voz "Muito Obrigado!" mas se o empregado sinais durante 8:00h às 10:00h, o prompt irá tornar-se "você está atrasado. Muito Obrigado! ".

Os comandos de voz podem ser definidos de duas formas:

Pelo segmento de tempo: o dispositivo reproduz diversos prompts de voz em resposta à mesma operação realizada dentro de diferentes segmentos.

Pelo grupo (que só está disponível para os dispositivos que suportam as funções de controle de acesso avançado): o dispositivo reproduz diversos prompts de voz em resposta à mesma operação realizada pelos usuários de diferentes grupos

Para configurar comandos de voz para diferentes segmentos de tempo, proceder da seguinte forma: Você pode definir um tempo total de 8º segmento prompts de voz para um dia inteiro. Selecione o Menu → Opções → Sistema Opt → Adv Opção e selecione a opção TZ Voz. Definir o jogo de voz 001 durante 07:00h às 09:00 e voz 002 durante 10:00h às 00:00 como mostrado abaixo:

TZ Voice	
001	07:00-09:00
002	10:00-12:00
003	00:00-00:00
004	00:00-00:00
005	00:00-00:00
006	00:00-00:00
007	00:00-00:00
008	00:00-00:00

Depois de concluir as configurações, pressione OK. Essas configurações terão efeito após a reinicialização do dispositivo.

10.22 Código de Trabalho

[Descrição da Função]

O conceito do código de trabalho é criado para facilitar o software para gerenciar a verificação os registros de acordo com diferentes casos. Por exemplo, podemos definir " 1" para comer, " 2" para ver um médico e " 3" para fumar, e input valor correspondente ao executar uma ação específica. Desta forma, o software pode ser facilmente diferenciado entre os eventos 1, 2 e 3.

[Descrição da operação].

Você pode definir o "Código de Trabalho" selecionando Menu → Opções → Sistema Opt → Adv Opção. O "Código de Trabalho" inclui três opções: Modo 1, o modo 2 e "Nenhum".

Selecione "Modo 1", ou seja, introduza o código de trabalho (um de nove dígitos) mediante a verificação de impressão digital, e pressione OK para salvar os registros em conjunto com a entrada código de trabalho.

10.23 DHCP

O Dynamics Host Configuration Protocol (DHCP) fornece uma estrutura para alocar endereços IP dinâmicos para hosts em uma rede TCP/IP. O DHCP consiste de dois componentes: o servidor e o cliente. O servidor de DHCP executa gestão centralizada de todos os dados de configuração de rede IP e gerencia com as solicitações DHCP do cliente. O cliente utiliza o endereço IP atribuído pelo servidor.

Quando o nosso dispositivo utiliza o DHCP, ele precisa de um servidor DHCP e o nosso dispositivo funciona como um cliente.

Caso selecione "Y", depois de acessar a rede, reinicie o aparelho e o aparelho irá enviar uma mensagem para o servidor DHCP, solicitando um endereço IP dinâmico, e um aviso "Adquirindo endereço IP" será exibido na tela. O servidor DHCP irá fornecer um endereço IP utilizável e uma máscara de sub-rede para o dispositivo com base no endereço configurado. Depois que o aparelho adquirir um endereço IP, você pode selecionar Menu → Opções → Comum optar para consulta do endereço IP, máscara de sub-rede e gateway.

Se você selecionar "N", a função de DHCP não será ativada. Você precisa inserir manualmente um endereço IP, máscara de sub-rede e gateway.

10.24 Agrupamentos de Usuários

Dividir os usuários em grupos diferentes. O usuário precisa para primeira entrada o número do grupo que ele/ela pertence e, em seguida, coloque o seu dedo sobre o dispositivo para o reconhecimento. Você também pode definir o horário de desbloqueio para cada grupo para facilitar a gestão do controle de acessos. O sistema define 5 grupos: Grupo 1, Grupo 2, Grupo 3, Grupo 4 e Grupo 5.

Definição da função "Match pelo Grupo"

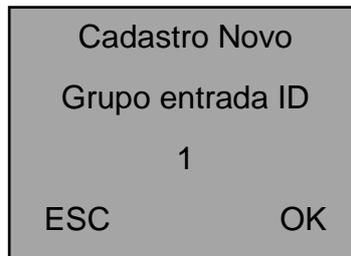
No dispositivo que suporte esta função, selecione Menu → Opções → Sistema Opt → Adv opção e defina a opção que permite que o Grupo do "Adv Opção" interface. Se você selecionar Y, o usuário precisa primeiro inserir o número do grupo que ele/ela pertence e, em seguida, coloque o seu dedo sobre o dispositivo para corresponder. Se você selecionar N, o jogo pelo grupo é desativado durante a verificação do usuário.

You can set and modify the “Default Group” on the “Adv Option” interface by selecting Menu → Options → System Opt → Adv Option.

Cadastro de usuários

Se "Permitir Grupo" está definido para Y, a seguinte caixa de diálogo será exibida durante a inscrição de um novo usuário.

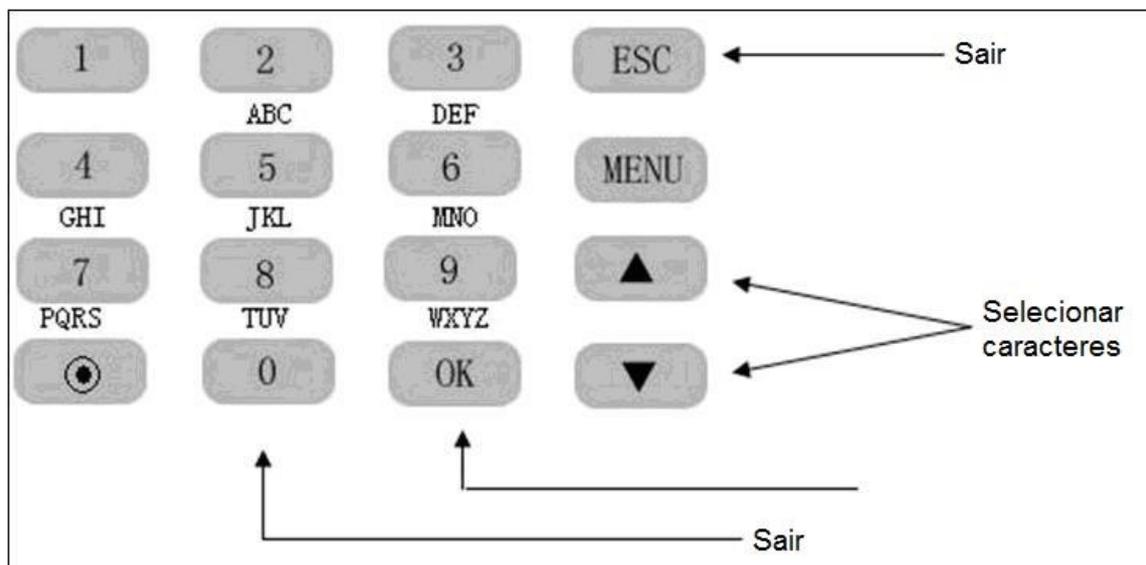
O novo usuário precisa primeiro definir o grupo que ele / ela pertence e, em seguida, inscrever-se no sistema.



10.25 Métodos de Entrada T9

Toda a tecla de números 2-9 é distribuída com 3 ou 4 letras do idioma inglês, por exemplo, a chave 1 tem três letras A, B e C. Você só precisa digitar a tecla a letra desejada uma vez, todos os correspondentes as letras maiúsculas e minúsculas. Você pode pressionar ▲/▼ para escolher a letra desejada. O usuário pode digitar o seu nome, nome do departamento, e turno de trabalho pelo T9 método de entrada.

O layout do teclado de entrada T9 método é a seguinte:



10.26 Função TTS

Através do uso da tecnologia TTS, o dispositivo converte texto normal de linguagem no discurso, que pode ser como saída arquivos WAV. O dispositivo dinamicamente as edições e reproduz o discurso para que os usuários possam desfrutar claro natural da voz. Os usuários podem modificar ou personalizar individualizadas prompts de voz, conforme desejado, utilizando software de PC.

□ **Observação:** O dispositivo suporta 9 dígitos IDs de usuário deve carregar os dados do usuário em primeiro lugar e, em seguida, dados de impressão digital em vez de carregar dados de impressões digitais e de usuário simultaneamente durante a alta velocidade upload de dados de impressões digitais na RS485.