MADIS

MANUAL DE INSTRUÇÕES

MD 5714F

SUMÁRIO

1. APRESENTAÇÃO

MD5714 F É uma versão totalmente atualizada do terminal de medição de temperatura corporal com reconhecimento facial de luz visível, usando algoritmos de reconhecimento facial de engenharia inteligente por imagem térmica e a mais recente tecnologia de visão computacional, ele suporta a verificação facial e da palma da mão com grande capacidade e reconhecimento rápido, além de melhorar o desempenho da segurança em todos os aspectos.

O **MD5714 F** adota a tecnologia de reconhecimento sem toque e novas funções, como medição de temperatura e identificação individual de pessoas com máscara, o que elimina os problemas de higiene de maneira eficaz. Também é equipado com o melhor algoritmo antifalsificação no reconhecimento facial contra quase todos os tipos de ataque de fotos e vídeos falsos. É importante ressaltar que o reconhecimento de palma 3 em 1 (formato da palma, impressão da palma e veia da palma) é realizado em 0,35 s por mão; os dados de palma adquiridos serão comparados com um máximo de 3.000 modelos de palma.

Como mencionado acima, o **MD5714 F** pode ajudar a reduzir o risco de infecção e a propagação de germes durante o recente problema de saúde pública global. Isso permite a medição rápida e precisa da temperatura corporal e a identificação de pessoas com máscara durante a verificação facial e da palma da mão em todos os pontos de acesso especialmente em hospitais, fábricas, escolas, edifícios comerciais, aeroportos, estações e outras áreas públicas.

2. PADRÕES

Confira abaixo os padrões utilizados neste manual:
Padrões GUI:

Software	
Padrão	**Descrição**
Fontes Negritadas	Usadas para identificação de ações no software. Exemplo: **OK**, **Confirmar**, **Cancelar**.
>	Os multiníveis do menu são separados por esses símbolos. Exemplo: **Arquivo>Criar> Pasta**.
Dispositivos	
Padrão	**Descrição**
<>	Os botões ou nomes das teclas no aparelho. Exemplo: **Pressione<OK>**
[ ]	Nome das janelas, itens de menu, tabela de dados e nomes dentro dos colchetes. Exemplo: **[Novo Usuário]**
/	Os multiníveis do Menu são separados por barras. Exemplo: **[Arquivo/Criar/Pasta]**

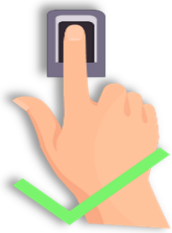
Símbolos:

Padrão	**Descrição**
	Simboliza que existe um aviso.
	Informações gerais que ajudam a operação a ser mais rápida.
	Informação importante.
	Cuidado para evitar perigos ou erros.
	Aviso de que algo alarmante está acontecendo.

3. AVISOS IMPORTANTES

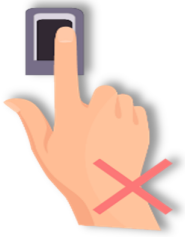
3.1. POSICIONAMENTO dos Dedos

Dedos recomendados: Indicadores, médios ou anelares; evite utilizar o polegar e o mindinho em função das dificuldades para pressionar com precisão o leitor de impressões digitais.



Correto

Muito em baixo



Muito perto da borda

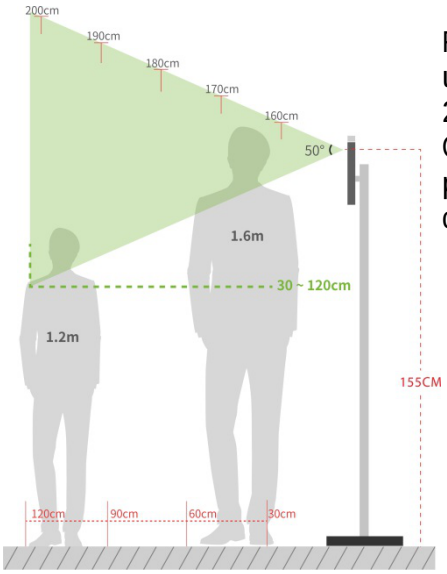
Correto

Muito inclinado

Por favor, garanta a utilização dos métodos corretos para pressionar os dedos no leitor de impressões digitais. A **MADIS** não assumirá nenhuma responsabilidade por problemas decorrentes ao uso incorreto do produto e a empresa, também, se reserva o direito de interpretação final e alterações neste ponto.

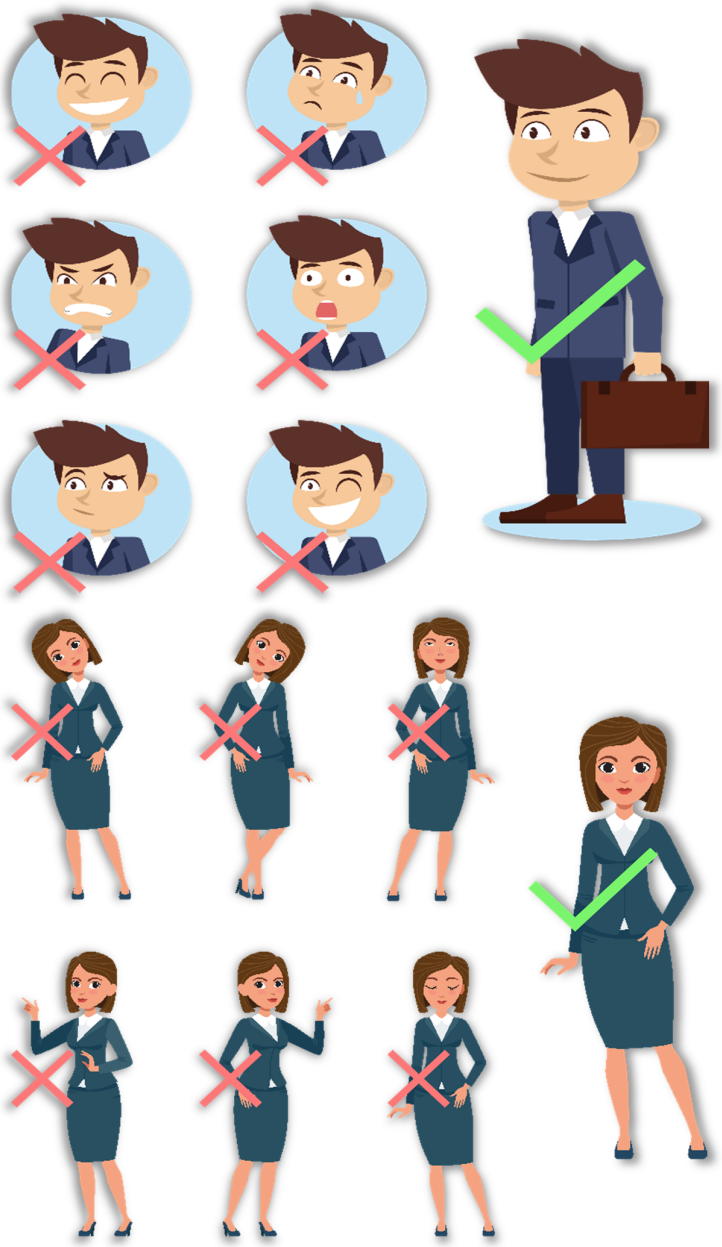
3.2. Posição dos pés, expressões faciais e postura

- **Distância recomendada**



Recomenda-se que a distância entre o dispositivo e um usuário com altura entre 1,55m-1,85m seja de 0,3cm a 2,5m.
Os usuários podem se deslocar ligeiramente para frente e para trás para melhorar a qualidade das imagens faciais capturadas.

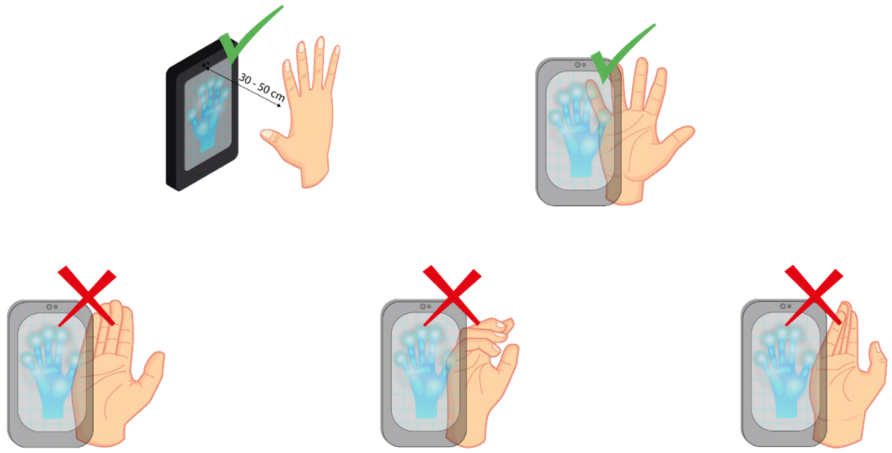
- **Expressões faciais e postura**



Durante o registro e a verificação biométrica, por favor, permaneça com a expressão facial e postura posicionados naturalmente.

3.3. Registro de palma

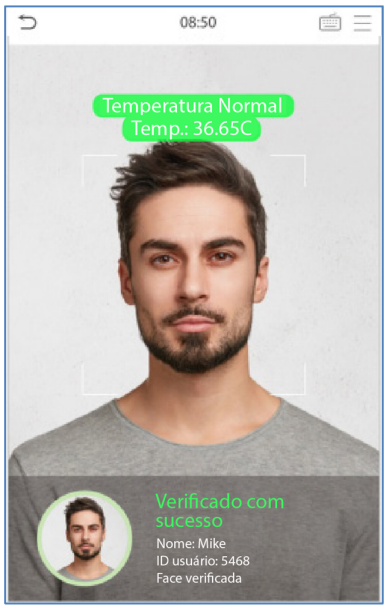
Coloque a palma na área de leitura de forma que a mão seja fique paralela ao dispositivo.
Lembre-se de manter um pequeno espaçamento entre os dedos.



Posicione a palma da mão com a distância de 30-50 cm do aparelho.

3.4. Registro de faces

Mantenha o rosto no centro da imagem de frente para a câmera e mantenha-se imóvel durante todo o registro facial.
A página de registro e verificação possui este aspecto:



Orientações importantes para registro e método de autenticação:

- Ao registrar uma face mantenha a distância de 40 a 80 cm entre o dispositivo e o rosto;
- Seja cuidadoso e natural quanto às expressões faciais. Evite: rosto sorridente ou piscada de olho;
- Se as instruções do **MD5714 F** não forem seguidas, o registro da face poderá demorar ou falhar;
- Fique atento para que os olhos e sobrancelhas não sejam cobertos durante o registro e leitura;
- Não utilize chapéus, máscaras, óculos de sol ou de grau durante o registro e verificação da face;
- É recomendado que os usuários que usam óculos de grau sejam registrados com e sem os óculos;
- Se algum usuário mudar os óculos a autenticação poderá falhar, se o rosto tiver sido registrado sem os óculos valide-o assim. Se apenas o rosto com os óculos tiver sido cadastrado, verifique novamente o rosto com os óculos usados anteriormente;
- Registre uma pessoa de cada vez no **MD5714 F** e certifique-se de não capturar dois rostos ao mesmo tempo para o aparelho;
- Certifique-se que as faces apareçam dentro da linha de orientação apresentada na tela do **MD5714 F**;
- Não é recomendado cobrir parte do rosto e se houver alguma parte coberta com chapéus, máscaras, mancha ocular ou óculos de sol a autenticação poderá falhar.

Interface do dispositivo

Depois que o aparelho for ligado à fonte de alimentação, apresentará a seguinte tela:

1) Clique em para ir até a página de autenticação do usuário no modo

1:1.

2) Quando não houver um administrador definido no dispositivo clique em para acessar o menu e definir um administrador. Para segurança do aparelho realize essa definição na primeira vez que utilizar o **MD5714 F** e sempre que for necessário acessar o menu será necessário que o administrador valide a ação.

3) ★ As alterações nas configurações podem ser feitas usando as teclas de atalho do dispositivo. Clique em qualquer lugar na tela sem ícones, assim aparecerão seis teclas de atalho.

Pressione a tecla do atalho correspondente para selecionar o item que será mostrado em verde.
Lembre-se de consultar o item **7.5 Mapeamento de Atalhos** para entender os detalhes da operação.

3.5. Teclado virtual

- Clique na caixa de entrada para acessar o teclado virtual, e se desejar alterar o teclado para o inglês clique em [En];
- Pressione [123] para mudar para o teclado numérico e para voltar ao alfabético clique em [ABC];
- Em [ESC] você sairá do teclado.

3.6. Métodos de verificação

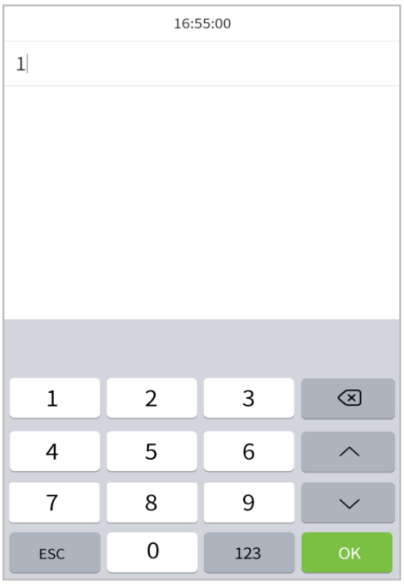
3.6.1. Verificação de Palma

Compara as imagens de palma das mãos lidas pelo coletor com os dados de palma registrados no dispositivo.

O aparelho distinguirá entre o modo de verificação da palma da mão e a verificação facial quando a palma for posicionada no leitor, desta forma o dispositivo detectará o modo de verificação da palma da mão automaticamente.

- **1: 1 Modo de verificação de palma**

Clique em  na tela para entrar na tela de autenticação 1:1, digite o ID seu usuário e pressione [OK].



Caso o usuário tenha registrado a impressão digital, face e senha, além da palma da mão e o método de verificação estiver definido para palma da mão/ impressão digital/ rosto/ senha, a seguinte tela aparecerá:

Selecione o ícone da palma da mão  para entrar no modo verificação de palma.

3.6.2. Verificação de impressão digital

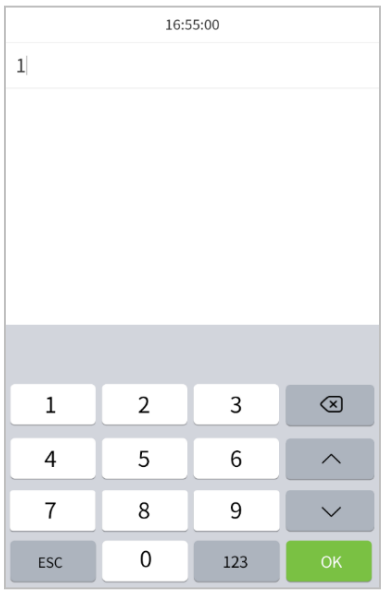
O **MD5714 F** compara a impressão digital que está sendo pressionada no leitor com os dados de digital armazenados no dispositivo.
O aparelho entrará no modo de autenticação da digital quando o usuário pressionar o dedo no leitor de impressões.
Lembre-se de seguir a forma correta para colocar seu dedo no sensor e em caso de dúvidas consulte o item **1.1 Posicionamento dos dedos**. Garantindo assim, uma verificação bem sucedida.

- **1: 1 Verificação de impressão digital**

Compara a impressão digital apresentada no leitor de digitais com os dados ligados a entrada de identificação do usuário por meio do teclado virtual.

Clique em  na tela principal para entrar no modo de verificação de impressões digitais.

1. Digite a identificação do usuário e pressione [OK].



Caso o usuário tenha registrado a impressão digital, leitura de face e senha, além da palma da mão, e o método de verificação estiver definido para: palma da mão/ impressão digital/ rosto/ senha, a seguinte tela aparecerá:

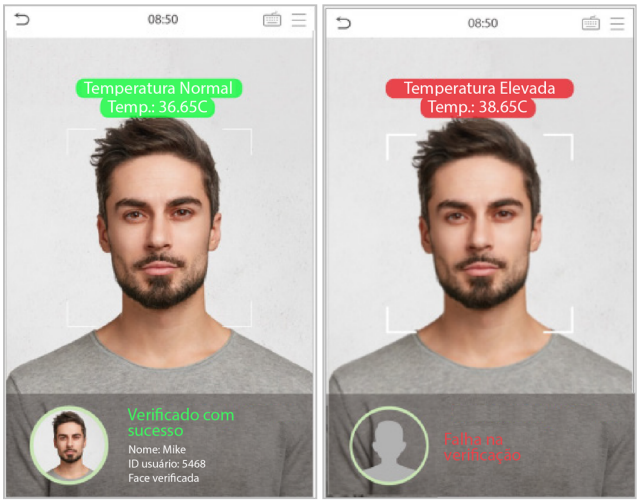
Selecione o ícone  de impressão digital para entrar no modo de verificação da impressão digital.

Pressione a impressão digital que será verificada.

3.6.3. Verificação facial

- **Verificação convencional (1:N)**

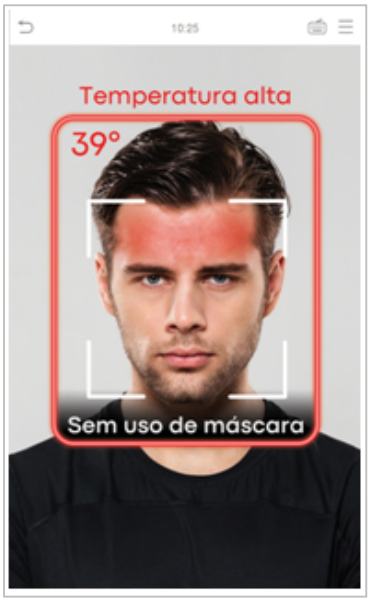
Compara a imagem facial lida com todos os dados faciais registrados no dispositivo, então a seguinte caixa *pop-up* aparecerá com o resultado:



- **Leitura de temperatura com infravermelho**

Quando a função **Ativar detecção de temperatura IR** estiver ligada, além da verificação convencional, a temperatura corporal também será medida.

Para garantir a medição correta, é importante que o usuário esteja com a face alinhada com a área de medição da temperatura corporal.
Lembre-se que essa função é aplicável somente em produtos com o módulo de medição de temperatura.

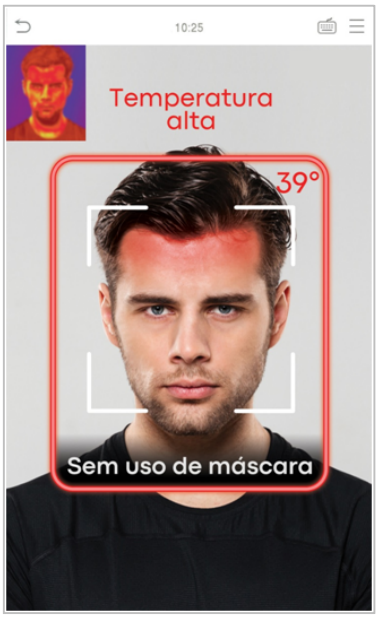


- **Detectando máscara facial**

Se o usuário ligar a função **Ativar detecção de máscara**, o dispositivo identificará se o usuário está utilizando a máscara ou não.
Lembre-se que esta função é aplicável somente em produtos com o módulo de medição da temperatura.

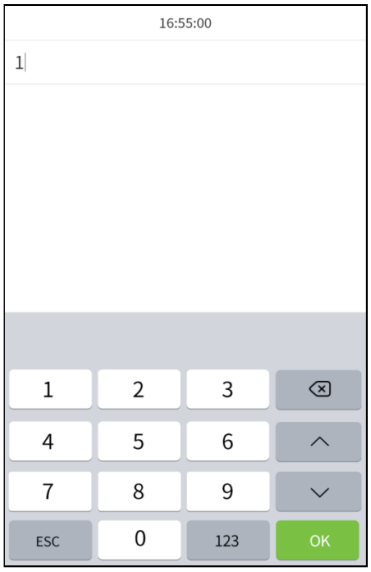
- **Exibir imagem térmica**

Quando a função **Exibir imagem térmica** estiver habilitada, uma imagem do usuário será exibida no canto superior esquerdo da tela do aparelho conforme a imagem abaixo:

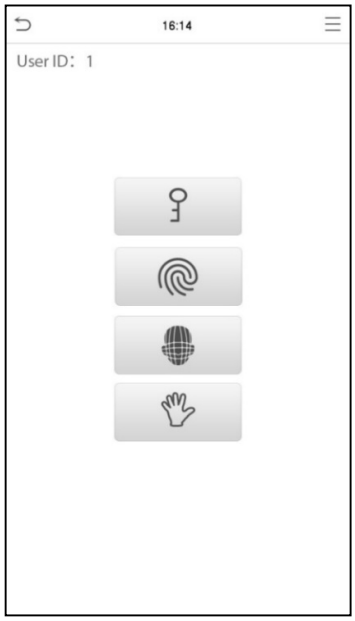


- **1:1 Verificação facial**

Compara o rosto capturado pela câmera com o modelo facial relacionado com o ID do usuário que for apresentado. Pressione na tela principal e acesse o modo de verificação facial e clique em [OK].



Se usuário registrar a leitura da face além da impressão digital, leitura de palma e senha e este método de verificação estiver ativado. A validação será feita na sequência palma da mão/ impressão digital/ rosto/ senha e a tela abaixo aparecerá:



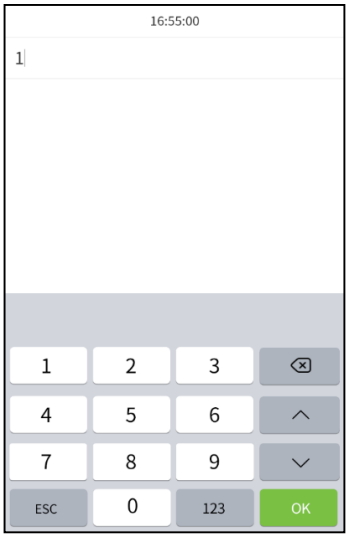
Selecione o ícone  para entrar no modo de validação da face.

3.6.4. Verificação por senha

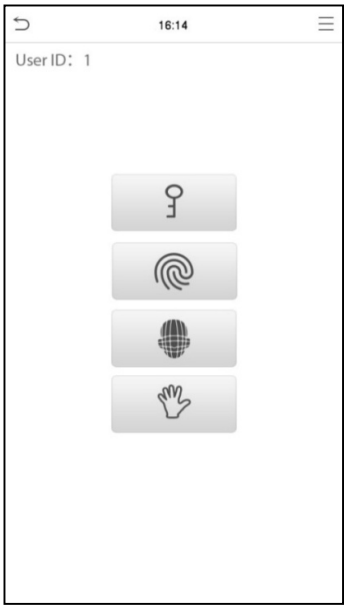
Validará a senha informada pelo usuário com a senha registrada por ele no sistema.

Clique em  na tela principal para acessar o modo de verificação por senha.

1. Entre com o número de identificação do usuário e clique em [OK].



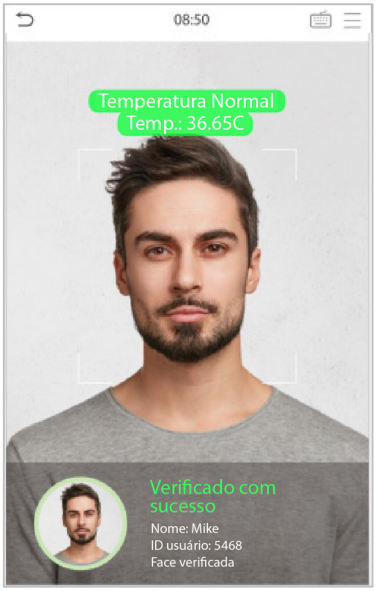
Se além da validação por palma, leitura de face e impressão digital, a função senha estiver ativada, a leitura será feita na seguinte sequência: palma da mão/ impressão digital/ rosto/ senha e a tela abaixo será exibida.



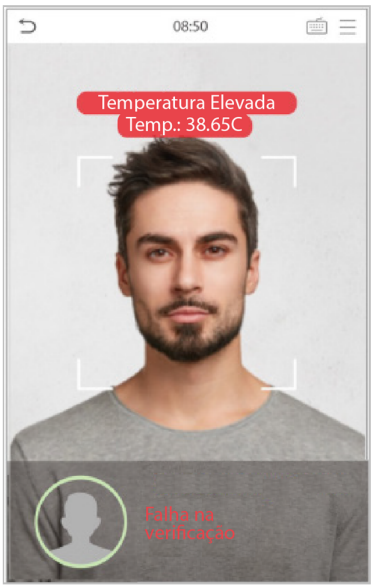
Selecione o ícone  para entrar no modo de validação por senha.

2. Digite a senha e pressione [OK].

Verificação realizada com sucesso:



A verificação falhou:



3.6.5. Verificação combinada

O **MD5714 F** oferece a opção de múltiplas formas de verificação para aumentar ainda mais sua segurança. Existem 15 combinações possíveis de verificação, conforme as orientações abaixo:

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

2) As informações de verificação devem ser registradas antes do modo de verificação combinada, caso aconteça o contrário a verificação poderá falhar.

Exemplo: se um usuário utiliza a leitura do rosto, mas o modo de verificação é Face + Senha este usuário não passará na verificação.

4. Menu principal

Clique em ☰ na página inicial para entrar no menu, conforme a imagem abaixo:

Item	Descrição
Usuário Adm.	Para adicionar, editar, ver e deletar as informações básicas do usuário
Priv. usuário	Para definir as permissões personalizadas e das inscrições, ou seja, direto de alterar o sistema.
Conf. Com.	Para definir os parâmetros de rede, comunicação de serial, conexão com PC, rede sem fio, servidor de nuvem e *wiegand*.
Sistema	Verificar os parâmetros relevantes da rede, comunicação do serial, conexão com o computador, rede *WiFi* e servidores em nuvem.
Personalização	Aqui o usuário encontrará da voz, sinal, definição de a mapeamento de teclas de atalho.
Ger. dados	Para deletar todos os dados importantes do dispositivo.
Controle acesso	Aqui os parâmetros da fechadura e do dispositivo de controle de acesso são alterados. .
Proc. registros	Consulta os registros de acesso especificado, verifique as imagens de presença e de lista de bloqueio.
Autoteste	Testes automáticos para verificar o funcionamento de cada módulo do dispositivo.
Info. sistema	Onde é possível visualizar a capacidade de armazenamento dos dados, informações do dispositivo e *firmware* atual do aparelho.

5. Gestão de usuários

5.1. Adicione usuários

Clique em **Usuário Adm.** no menu principal e vá a **Novo Usr**.

- **Registrando o novo usuário**

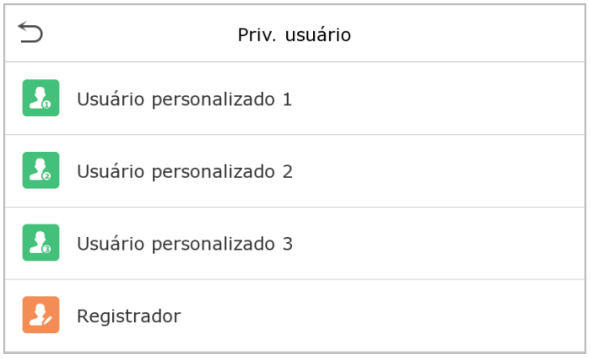
Adicione os dados nos campos nome e identificação do novo usuário.

1) A identificação do usuário poderá conter até 17 caracteres.
2) O nome de usuário, por padrão, pode conter de 1 a 9 dígitos.
3) Durante o registro inicial você poderá modificar o nome de usuário, mas após isso ele não poderá mais ser alterado.
4) Se surgir a mensagem usuário duplicado, você deverá escolher outro nome ou ID.

- **Definindo um Administrador**

No **MD5714 F** existem dois tipos de conta, a de usuário normal e administrador.

Se já houver um administrador registrado, os usuários normais não terão direito de gerenciar o sistema e só poderão fazer autenticação. Já o administrador possui acesso em toda gestão do aparelho, incluindo a seleção de permissões definidas pelo usuário e autenticação.



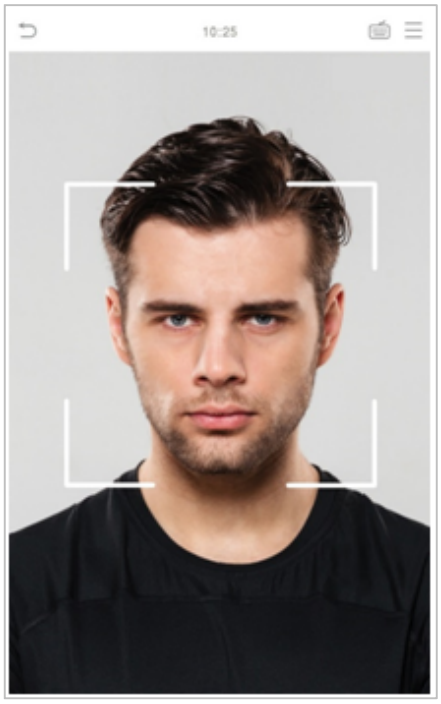
Se o usuário selecionado for um administrador, ele deverá autenticar com algum método pré-cadastrado para acessar o menu principal. É importante ressaltar que a validação é baseada em métodos de autenticação configuradas pelo administrador.

- **Registro de palma**

Clique em **Palma** para cadastrá-la, selecione e aguarde o registro ser finalizado.

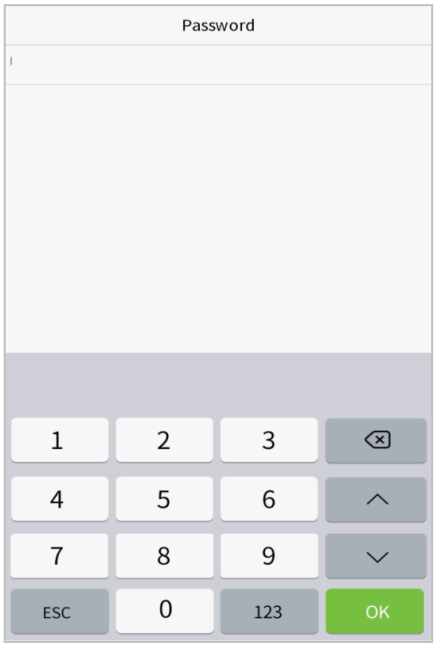
- **Registro de face**

Clique em **Face** para entrar na página de registro, lembre-se de ficar de frente para a câmera durante todo o registro facial, a interface de cadastro é a seguinte:



- **Registro de senha**

Clique em **Senha** para ir até a página de registro, digite novamente a senha e clique OK.



Em caso de divergência nas senhas digitadas a mensagem “Dado não registrado”. Lembre-se que a senha poderá conter no máximo oito dígitos.

- **Registro da foto de usuário**

Quando o usuário for registrado com foto de autenticação ela sempre será exibida, para isso, clique em **Foto Usuário**, vá ao ícone câmera para tirar a foto e então o sistema voltará para a página **Novo Usr**.
Ao registrar um rosto, o sistema captura automaticamente uma foto para imagem do usuário. Caso o usuário não queira registrar a foto, o sistema irá definir a imagem capturada como foto padrão automaticamente.

- **Controle de acesso**

O **controle de acesso** define os direitos de desbloqueio das portas de cada pessoa, incluindo o grupo e o período que o usuário pertence.
Clique na função de Controle de acesso > Grupo de acesso e atribua os usuários registrados a diferentes grupos para uma melhor gestão. Novos usuários sempre são encaminhados, por padrão, para o Grupo 1, eles podem ser reatribuídos para outros grupos e o dispositivo suporta até 99 grupos de controle de acesso.
Clique em **Período**, selecione o período a ser usado.

5.2. Pesquisa por usuários

Clique na barra de pesquisa em **Todos usr** e digite a palavra-chave, pode ser um nome de usuário, nome completo ou sobrenome, assim o sistema irá pesquisar os usuários relacionados com a informação solicitada.

5.3. Editar usuários

Escolha um usuário na lista e clique em **Editar** para entrar na seguinte tela de edição.
Lembre-se que o nome de usuário não poderá ser modificado ao editar um usuário. Verifique mais detalhes sobre o usuário em **3.1 Adicione usuários**.

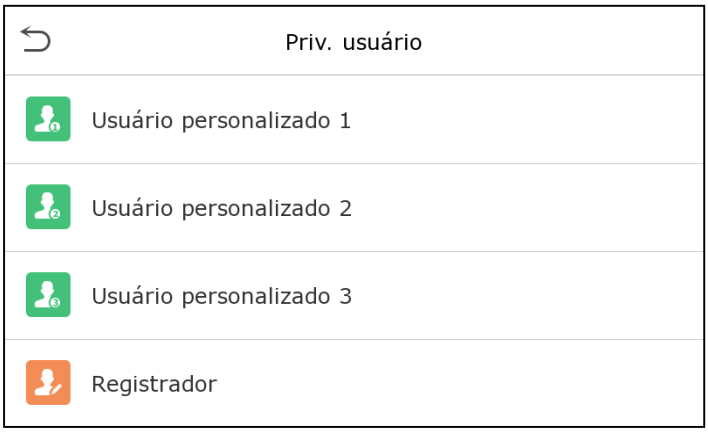
5.4. Apagar usuários

Escolha o usuário na lista e clique em **Apagar**, selecione as informações que serão eliminadas e clique em **[OK]**.

É importante lembrar que quando a exclusão de usuário for selecionada todas as suas informações serão deletadas.

6. Permissões do usuário

Se for necessário atribuir permissões específicas para determinado usuário vá até **Priv. usuário** no menu **Atribuir permissões**, assim será possível definir até três funções para cada um deles.

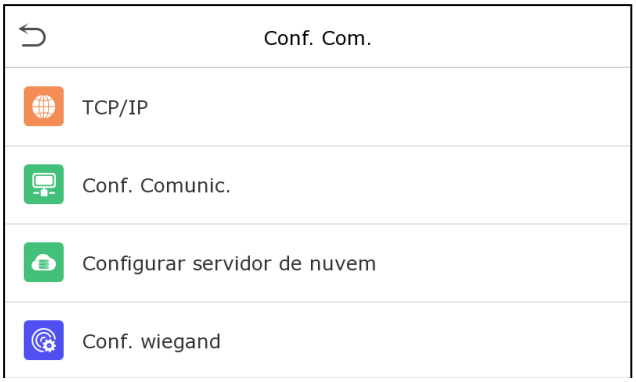


1. Clique no item **Atribuir permissões** clique em **Nome**, digite o nome da função e ative.
2. Clique em **Atribuir permissões** para atribuir os privilégios ao usuário, a ação será concluída e após a operação clique em **Voltar**.

Durante a atribuição de funções, o menu principal estará à esquerda e os submenus ficam à direita.
Selecione as características nos submenus e se houver funções definidas aos usuários, clique em **Usuário Adm.**>**Novo usr**>**Permissões do usuário**.
Se o super administrador não for registrado, o dispositivo solicitará o cadastramento de um responsável.

7. Configurações de rede

Para definir parâmetros de rede, conexão com PC, servidor na nuvem e *Wiegand*, toque em Conf. Com. no menu principal.



7.1. Rede

Quando o **MD5714 F** precisar se comunicar com um computador através do *Ethernet* você deverá ajustar as configurações de rede e garantir que aparelho e o PC estejam conectados à mesma rede.

Clique em *Ethernet* na opção **Conf. Com.** Confira:

Item	Descrição
TCP/IP	O valor de fábrica é 192.168.1.201, é preciso ajustá-lo de acordo com o valor real da rede.
Masc. Rede	O valor de fábrica é 255.255.255.0, é preciso ajustá-lo de acordo com o valor real da rede.
Gateway	O endereço padrão de fábrica é 0.0.0.0, é necessário ajustá-lo de acordo com o valor real de rede.
DNS	O endereço padrão de fábrica é 0.0.0.0, é necessário ajustá-lo de acordo com o valor real da rede.
Porta de comu. TCP	O valor predefinido na fábrica é 4370, é preciso ajustá-lo de acordo a situação de rede.
DHCP	Configuração de *host* dinâmico é utilizada para ajustar dinamicamente os endereços de IP para clientes via servidor.
Mostrar na barra *status*	Para definir se o ícone de rede será exibido na barra de *status*.

7.2. Serial

Para estabelecer a comunicação do aparelho com uma porta *serial* (RS232/RS485) é necessário configurá-la.

Item	Descrição
Porta *Serial*	Selecione a porta serial RS485 para comunicação.
Baudrate	São as taxas de comunicação com o PC, existem quatro opções de taxa: 115200 (padrão), 57600, 38400, e 19200. Quanto maior for a taxa mais rápida é a velocidade da comunicação, mas também menos confiável. Portanto, uma taxa de transmissão mais alta pode ser usada quando a distância de comunicação é curta, já quando a distância de comunicação for longa a escolha de uma taxa de transmissão mais baixa seria mais confiável.

7.3. Conexão com o PC

Para garantir a segurança dos dados defina uma Chave de comunicação entre o dispositivo e o PC. Após definida a senha de conexão, a mesma deverá ser digitada antes que o dispositivo seja conectado ao *software* do PC.

Vá até **Conf. Com.** e clique **Conf. Comunic.** para realizar a configuração.

Item	Descrição
Senha com.	A chave padrão é 0, mas pode ser alterada e deve conter de 1 a 6 dígitos.
ID Equip.	O número de identificação do dispositivo varia entre 1 e 254, se o método de comunicação for RS232/RS485 é necessário introduzir a identificação do dispositivo na tela de comunicação do software.

7.4. Conexão *Wireless*

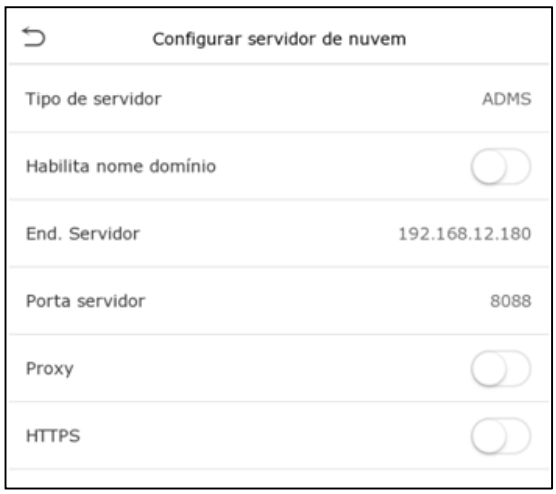
A comunicação de dados sem fio é utilizada como conexão de rede.
Para configurar o *Wireless* vá até **Conf. Com.** e altere as seguintes configurações:
O *WIFI* está sempre ativado, por padrão, no aparelho. Para ligar ou desativá-lo clique no botão .
Após adicionar a rede, encontre o sinal *WIFI* na lista e conecte-se a ele seguindo o mesmo procedimento.

Descrição de funções

Item	Descrição
DHCP	Abreviação de Configuração de Protocolo de *Host* Dinâmico, envolve a alocação dos endereços com IP dinâmicos a clientes de rede.
Endereço de IP	Endereço de IP da rede *WIFI*.
Máscara de sub-rede	Máscaras de sub-rede *WIFI.*
Porta de entrada	Endereço da porta de entrada da rede *WIFI*.

7.5. Configurações do servidor na nuvem

Aqui são configuradas as conexões com o servidor ADMS.
Clique em **Configurar servidor de nuvem** no menu **Conf. Com.**, conforme abaixo:



Item		Descrição
Habilitar nome do domínio	**Endereço do servidor**	Quando esta função estiver ativada será usado o modo de nome do domínio "http://...", como http://www.XYZ.com. Sendo “XYZ” o nome do domínio com este modo ligado.
Desabilitar o nome do domínio	**Endereço do servidor**	Endereço IP do servidor ADMS.
	Porta do servidor	Porta do servidor usada pelo ADMS.
Habilitar servidor *proxy*		Quando você optar por ativar o proxy será necessário definir o endereço do IP e número da porta do servidor proxy.
HTTPS		Um canal HTTP tem a segurança como objetivo. Baseado no HTTP, criptografia de transmissão e autenticação de identidade garantem a segurança do processo de transmissão.

7.6. Configurações *Wiegand*

Para definir os parâmetros de entrada e saída *Wiegand*, clique em **Conf. Wiegand** na opção **Conf. Com.** para abrir a seguinte tela:

Entrada *Wiegand*

Item	Descrição
Formato *Wiegand*	Os valores variam de 26 *bits*, 34 *bits*, 36 *bits*, 37 *bits* e 50 *bits*.
Bits* de *Wiegand	Número de bits de dados por *Wiegand*.
Largura de pulso	O valor da largura do pulso enviado por *Wiegand* é de 100 microssegundos por defeito, poderá ser ajustado dentro do intervalo de 20 a 100 microssegundos.
Intervalo de pulso	O valor por defeito é de 1.000 microssegundos que podem ser ajustados dentro do intervalo de 200 a 20.000 microssegundos.
Tipo de identificação	Selecione entre o usuário ID e número do crachá.

Definições de formatos *Wiegand* comuns:

Formato *Wiegand*	Definições
*Wiegand*26	ECCCCCCCCCCCCCCCCCCCCCCCCC São 26 *bits* de código binário, sendo o 1º *bit* responsável pela paridade par do 2º aos 13º *bits*, enquanto o 26º *bit* é o *bit* de paridade ímpar do 14º aos 25º *bits*. Enquanto do 2º aos 25º *bits* são os números dos cartões.
*Wiegand*26a	ESSSSSSSSCCCCCCCCCCCCCCCC Consiste em 26 *bits* de código binário. Sendo o 1º responsável pela paridade par do 2º aos 13º *bits*, 26º *bit* equivale à paridade ímpar do 14º aos 25º *bits*. Enquanto do 2º aos 9º *bits* são do código do site, já do 10º a 25º *bits* são os números dos cartões.
*Wiegand*34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC São 34 *bits* de código binário, sendo o 1º responsável pela paridade par do 2º aos 17º *bits*, o 34º *bit* é o de paridade ímpar do 18º ao 33º, enquanto do 2º ao 25º são números de cartões.
*Wiegand*34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCC São 34 *bits* de código binário, sendo o 1º responsável pela paridade par do 2º aos 17º *bits*, já o 34º é responsável pela paridade ímpar do 18º aos 33º *bits*. Do 2º aos 9º *bits* são do código do site, já do 10º ao 25º são os números de cartões.

*Wiegand*36	OFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME São 36 *bits* de código binário, sendo o 1º responsável pela paridade ímpar do 2º aos 18º *bits*, o 36º pela paridade par do 19º aos 35º *bits*. O 2º aos 17º *bits* são os *facilitycode*, do 18º aos 33º *bits* são os números dos cartões e os 34º aos 35º *bits* são os códigos do fabricante.
*Wiegand*36a	EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO São 36 *bits* de código binário, sendo o 1º responsável pela paridade par do 2º aos 18º *bits*, o 36º pela paridade ímpar do 19º aos 35º *bits*. Já do 2º aos 19º bits são os *facilitycode* e os 20º ao 35º são números de cartões.
*Wiegand*37	OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE São 37 *bits* de código binário, sendo o 1º responsável pela paridade ímpar do 2º aos 18º *bits*, o 37º *bit* responsável pela paridade par do 19º aos 36º *bits*. Já o 2º aos 4º *bits* são os códigos do fabricante, os 5º ao 16º são *site code* e os 21º ao 36º são os números dos cartões.
*Wiegand*37a	EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO Sendo 37 *bits* de código binário, o 1º é responsável pela paridade par do 2º aos 18º *bits*, enquanto o 37º é o *bit* de paridade ímpar do 19º aos 36º *bits*. Os 2º aos 4º *bits* são os códigos do fabricante, do 5º ao 14º são os *facilitycode*, os 15º aos 20º *bits* são do *site code* e do 21º aos 36º *bits* são os números dos cartões.
*Wiegand*50	ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCO São 50 *bits* de código binário, sendo o 1º responsável pela paridade par do 2º aos 25º, o 50º é o *bit* de paridade ímpar do 26º aos 49º, do 2º aos 17º *bits*são *sitecodes* e do 18º aos 49º são números dos cartões.
"C" denota o número do cartão; "**E"** é o *bit* da paridade par; "**O"** é o *bit* da paridade ímpar; **"F**" é o *facilitycode*; "**M"** o código do fabricante; "**P"** é o *bit* da paridade; e "**S"** é o *site code*.	

Saída *Wiegand*

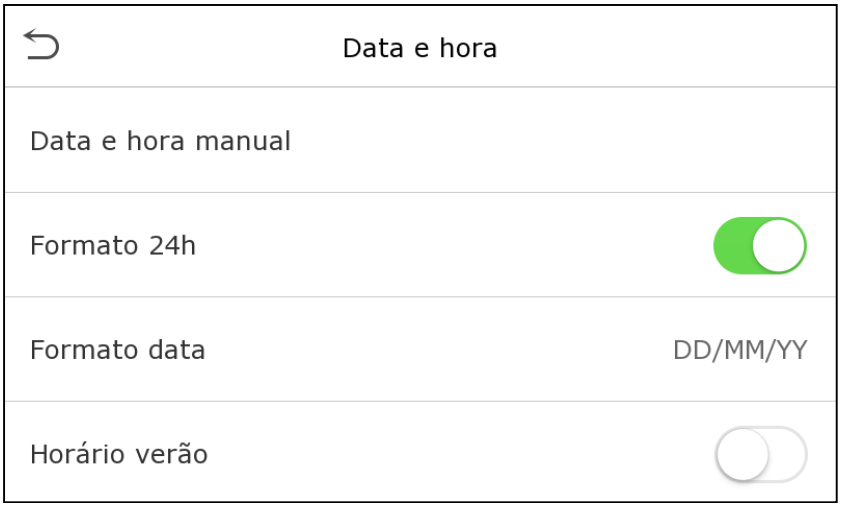
Item	Descrição
SRB	Quando SRB está ativado a fechadura é controlada por ele para evitar que a fechadura seja aberta devido a remoção do dispositivo.
Formato *Wiegand*	Os valores variam de 26 *bits*, 34 *bits*, 36 *bits*, 37 *bits* e 50 *bits*.
Saídas *Wiegand*	Depois de escolher o formato de *Wiegand*, um dos dígitos de saída correspondentes ao formato *Wiegand*.
Identificação falha	Caso a verificação falhe, o sistema enviará a identificação falha para o dispositivo e substituirá o número do cartão ou identificação pessoal pelos novos.
Site Code	É semelhante a identificação do dispositivo, com a diferença que é um *sitecode* pode ser definido manualmente e é repetível em dispositivos diferentes. Seu valor válido varia de 0 a 256 por defeito.
Largura de pulso	A largura de pulso representa as alterações da quantidade de carga elétrica com capacidade de alta frequência regularmente dentro de um tempo específico.
Intervalo de pulso	Intervalo de tempo entre os pulsos.
Tipo de identificação	Selecione para a saída *wiegand* entregar o ID ou número de cartão.

8. Configurações de sistema

Para definir os parâmetros de sistema para otimizar o desempenho do dispositivo, clique em **Sistema** na página do menu principal conforme a imagem abaixo:

8.1. Data e hora

Verifique o item **Data e hora** na página de **Sistema**.



1. Nele é possível alterar manualmente a data e a hora, lembre-se de confirmar a mudança para salvar.
2. Clique em 24 horas para ativar ou desativar este formato e selecione o formato da data.

Ao restaurar as definições de fábrica, o formato da hora e da data podem ser restaurados, mas a data e hora do aparelho não podem ser restauradas.
Por exemplo, o usuário configurou a hora do **MD5714 F** em 18h30 em 1 de janeiro de 2020, após a restauração das configurações de fábrica a hora do aparelho seguirá 18h30 de 1/1/2020.

8.2. Configurações de acesso

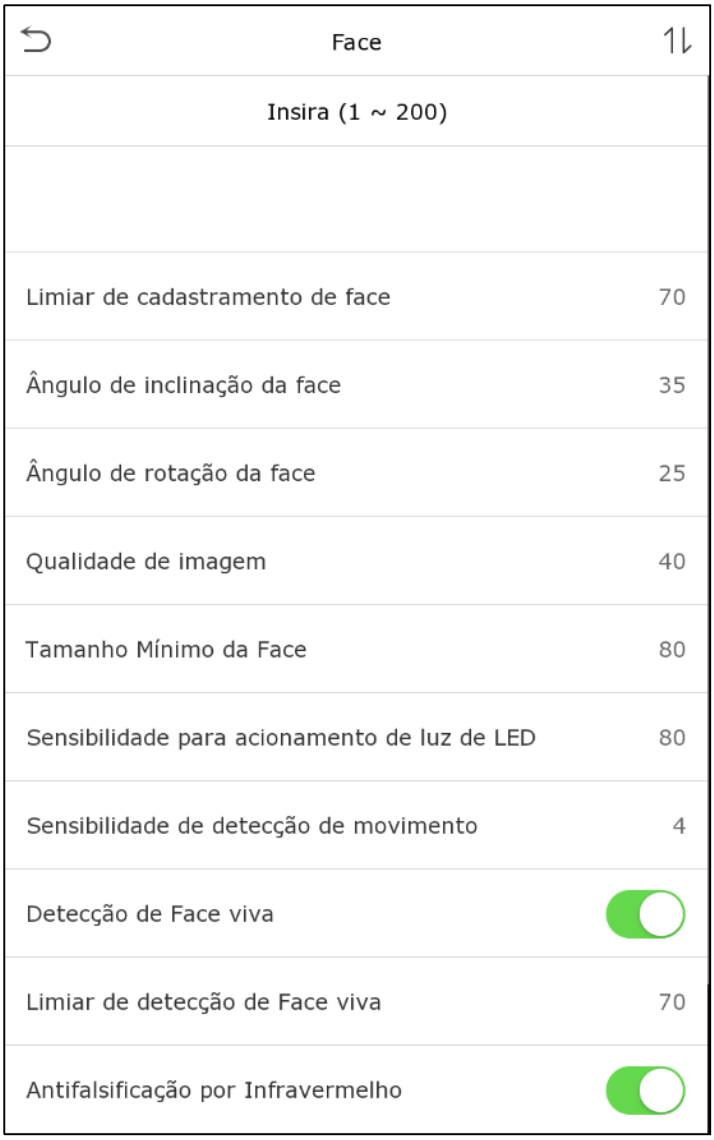
Clique em **Sistema > Conf. Reg. de acesso** para ver a seguinte página:

Item	Descrição
Câmera	Para capturar e guardar a imagem atual durante a verificação existem cinco formas, confira: **Sem foto:** nenhuma foto será tirada durante a verificação. **Tirar foto sem guardá-la**: a foto será tirada, mas não será armazenada durante a verificação. **Tirar a foto e armazená-la:** a foto será feita e guardada durante a validação. **Salvar foto de verificação falha:** a fotografia é feita e armazenada a cada verificação falha.
Mostrar foto de usuário	Mostrará a foto do usuário verificado.
Aviso de memória em registros de acesso	Se o espaço de registros restantes atinge o valor definido o aparelho automaticamente enviará uma notificação de memória dos registros. Os usuários podem desativar a função ou definir um valor de 1 a 9.999.

Apagando registros de acesso	Caso os registros de acesso atingirem sua capacidade total o aparelho automaticamente apagará um valor definido de registros de acesso. É possível desativar essa função ou definir um valor para eliminação de 1 a 999.
Apagando os registros de presença	Quando os registros de presença atingirem a capacidade total o aparelho automaticamente apagará um valor definido de imagens de presença mais antigas. O usuário poderá desativar ou definir um valor para eliminação de 1 a 99.
Apagando fotos da lista de bloqueados	Se as fotos da lista de bloqueados atingirem a capacidade total, o dispositivo apagará automaticamente o valor definido de imagens antigas. O usuário pode desativar a função ou definir um valor válido entre 1 e 99.
Notificação de verificação	A notificação de verificação bem sucedida é exibida pelo tempo de 1~9 segundos.
Intervalo de comparação de faces (s)	Defina o intervalo de tempo entre autenticações faciais, conforme sua necessidade. O valor válido é 0~9 segundos.

8.3. Parâmetros de faces

Clique em **Face** para configurar a função, confira:



Item	Descrição
Parâmetro de verificação 1:N	No modo verificação 1:N a autenticação será bem sucedida somente quando a semelhança entre a imagem da face adquirida e todos os modelos faciais registrados forem maiores do que o valor definido. O valor válido varia de 65 a 120. Quanto mais altos são os parâmetros, mais baixa é a taxa de erro de julgamento, mais alta é a taxa de rejeição e vice-versa. O valor recomendado por defeito é 75.

Parâmetro de verificação 1:1	Em modo de verificação 1:1, a autenticação só será bem sucedida quando a semelhança entre a imagem facial adquirida e os modelos faciais inscritos no dispositivo forem maiores que o valor configurado no parâmetro. A lógica aplicada é a seguinte: quanto mais altos estão os parâmetros, menores serão as taxas de erro no julgamento das imagens e assim maiores serão as taxas de rejeição e vice-versa. Os valores válidos variam entre 55 a 120 e o valor recomendado por defeito é 63.
Parâmetro para cadastro do rosto	A comparação usada em **1:N** durante o registro facial é utilizada para determinar se o usuário já se registrou anteriormente. Se a semelhança entre o rosto e os modelos faciais que já registrados for superior a este parâmetro, conclui-se que o rosto já foi registrado antes.
Ângulo de tolerância para inclinação	Nível de tolerância do ângulo de inclinação do rosto durante o registro e verificação facial. Se o ângulo de inclinação da face exceder o valor definido a imagem será filtrada pelo algoritmo, ignorado pelo terminal e nenhuma imagem de registro ou comparação será acionada.
Ângulo de rotação do rosto	Tolerância do ângulo de rotação da face durante o registro e a comparação dos modelos faciais. Se o ângulo de rotação de uma face exceder esse valor definido, ele será filtrado pelo algoritmo, ou seja, ignorado pelo terminal, portanto, nenhuma interface de registro e comparação será acionada.
Qualidade de imagem	Refere-se a qualidade das imagens faciais registradas e verificadas, lembre-se: quanto mais alto for o valor mais clara será a imagem exigida.
Tamanho mínimo de face	Se o tamanho da face for menor do que o valor definido, o objeto será filtrado e não será reconhecido como um rosto. Esse valor poderá ser entendido como a distância de comparação facial, assim quanto mais distante estiver a pessoa, menor estará seu rosto e menor será o pixel da imagem obtida pelo algoritmo. Sendo assim, o ajuste do parâmetro poderá ser ajustado conforme a distância de comparação de rostos mais distantes. Quando o valor fixado for zero a distância de comparação dos rostos não será limitada.

Sensibilidade da luz de LED	Esse valor liga e desliga a luz LED, sendo assim, quanto maior for o valor fixado, mais frequentemente a luz LED será ligada.
Sensibilidade na detecção de movimentos	Medida da quantidade de mudança no campo de visão da câmera do equipamento, se qualifica como potencial detecção dos movimentos de acordo com o modo de espera e verificação. Quanto maior o valor configurado mais sensível estará o sistema, portanto se for definido um valor maior a interface de autenticação, será muito mais frequentemente acionada.
Detecção de face viva	Utiliza imagens de luz visível para realizar a detecção das tentativas de falsificação, desta forma é determinando se as fontes das amostras biométricas são seres humanos vivos ou apenas uma representação falsa.
Parâmetro para detecção ao vivo	Garante se a detecção da imagem visível vem de um ser vivo. Quanto maior for o valor configurado, melhor será o desempenho da proteção de antifalsificação da luz visível.
Antifalsificação com NIR	Previne ataques com fotos ou vídeos falsos utilizando imagens de espectros infravermelhos.
WDR	O *WideDynamic Range (WDR)*, é responsável por equilibrar a luz e ampliar a visibilidade das imagens em vídeos de vigilância sob cenas de iluminação com alto contraste, além de melhorar a identificação de objetos em ambientes claros ou escuros.
Modo *anti-flicker*	Ajuda a reduzir as oscilações de luz na tela do aparelho quando o WDR estiver desligado.
Algoritmos de rostos	Informações relacionadas com algoritmos de face e atualização dos modelos em pausa.
Importante	Lembre-se de ajustar os parâmetros de exposição e qualidade de acordo com as orientações da **MADIS**, ajustes inadequados podem afetar gravemente o desempenho do aparelho.

8.4. Parâmetros de impressões digitais

Clique em Impressão digital no **MD5714 F** e confira:

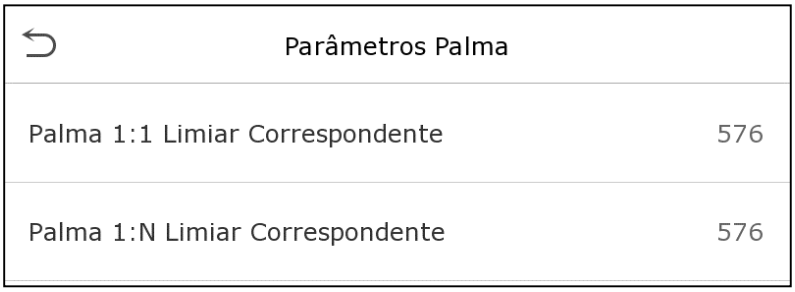
FRR	**FAR**	**Limiar de comparação recomendado**	
		1:N	1:1
Alto	Baixo	45	25
Médio	Médio	35	15
Baixo	Alto	25	10

Item	Descrição
Parâmetro de comparação:1:1	No método de verificação 1: 1, a verificação só será bem-sucedida quando a semelhança entre os dados de impressão digital cadastrada e o modelo de impressão digital cadastrado ao ID do usuário no dispositivo for maior que o valor definido.
Parâmetro de comparação 1:N	No método de verificação 1: N, a verificação só será bem-sucedida quando a semelhança entre os dados de impressão digital cadastrados e os modelos de impressão digital registrados no dispositivo for maior que o valor definido.
Sensibilidade do sensor de impressão digital	É recomendável usar o nível padrão "Médio". Quando o ambiente está seco, pode resultar em lentidão na detecção de impressão digital, você pode definir o nível como "Alto" para aumentar a sensibilidade; quando o ambiente está úmido, dificultando a identificação da impressão digital, você pode definir o nível como "Baixo".
Número de tentativas 1:1	Na verificação 1: 1, os usuários podem esquecer a impressão digital registrada ou pressionar o dedo incorretamente. Para reduzir o processo de inserir novamente ou o ID do usuário, é permitida novas tentativas

Imagem das impressões digitais	Para definir se a imagem da impressão digital deve ser exibida na tela durante o registro ou a verificação da impressão digital. Quatro opções estão disponíveis: **Exibir no cadastro**: Exibe a imagem da impressão digital na tela apenas durante o cadastro. **Exibir na autenticação:** Exibe a imagem da impressão digital na tela apenas durante a autenticação. Sempre mostrar: Exibe a imagem da impressão digital na tela durante o cadastro e autenticação Nenhuma: Não exibe a imagem da impressão digital.

8.5. Parâmetros de Palma

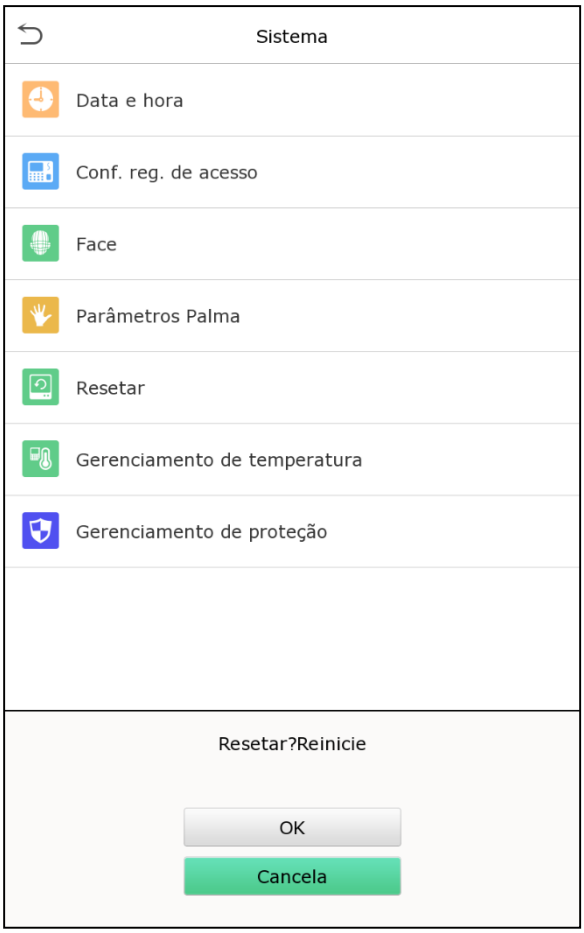
Confira a opção **Parâmetros de Palma** no **MD5714 F**:



Item	Descrição
Parâmetro de comparação:1:1	No método de verificação 1:1 somente quando a semelhança entre a palma da verificação e a palma registrada do usuário for maior que esse valor a verificação poderá ser bem-sucedida.
Parâmetro de comparação: 1:N	No método de verificação 1:N somente quando a semelhança entre a palma da verificação e toda a palma registrada for maior que esse valor a verificação poderá ser bem-sucedida.

8.6. Resetando o dispositivo

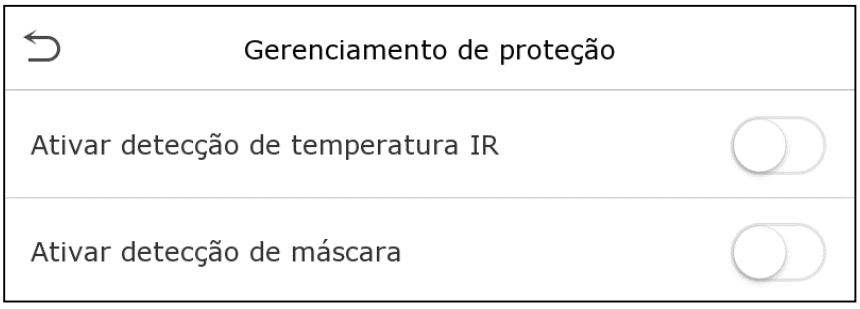
Para restaurar as definições de fábrica do dispositivo sem apagar os dados registrados pelos usuários, clique em *Resetar* no sistema do **MD5714 F**, conforme a imagem abaixo:



Clique em **OK** para resetar o aparelho.

8.7. Gerenciamento de Proteção

Vá até **Gerenciamento de Proteção** e verifique:

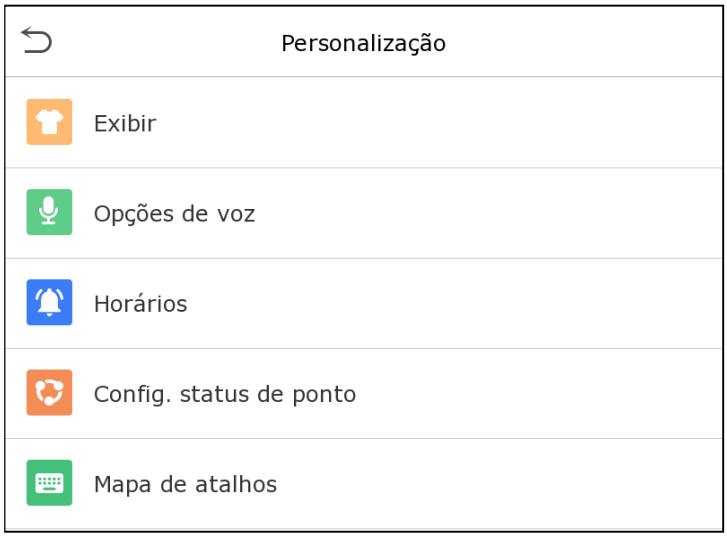


Item	Descrição
Permitir medição da temperatura com infravermelho	Quando ativada, essa função permite que além da verificação de identidade, também, seja realizada a medição da temperatura corporal do usuário. É importante que o rosto do usuário esteja alinhado com a área de medição de temperatura para que ela seja bem sucedida.
Alarme de alta temperatura	Aqui é possível definir o valor em que o alarme de alta temperatura será ativado. O equipamento possui o nível predefinido de 37,30ºC, caso a temperatura medida durante a verificação seja superior a este valor o dispositivo emitirá um alarme sonoro imediatamente.
Acesso negado por alta temperatura	Quando ativada essa função, bloqueará o acesso dos usuários que estiverem com a temperatura superior ou inferior aos parâmetros configurados no dispositivo. Se a função estiver desativada os usuários terão acesso às áreas restritas somente com a verificação de identidade, independente da temperatura corporal.
Correção no desvio de temperatura	As variáveis do ambiente, temperatura e umidade, podem afetar o módulo de medida da temperatura que por sua vez, admite uma pequena possibilidade de erros nos valores coletados em diferentes ambientes. Por este motivo os usuários devem definir nesta opção o valor do desvio de temperatura.
Unidade de medida da temperatura	A unidade de medida da temperatura pode ser alterada entre Celsius (ºC) e Fahrenheit (ºF).
Distância adequada para medida de temperatura	Para medir a temperatura durante a leitura existem três modos: muito perto, perto e longe.
Imagem térmica	Ative essa função para visualizar a imagem térmica do usuário. Após a ativação, a imagem térmica do usuário será exibida no canto superior esquerdo do aparelho durante a autenticação.

Temperatura corporal	Quando ativada a função, exibirá o valor da temperatura do usuário durante o processo de autenticação.
Permitir detecção de máscaras	Se essa função estiver ativada o dispositivo identificará se o usuário está ou não utilizando uma máscara no momento da autenticação.
Permitir acesso de pessoas não registradas	Ative essa função quando desejar que o aparelho permita que pessoas que não registradas tenham acesso às áreas restritas passando pela detecção.
Permitir captura de imagem das pessoas não registradas	Se ativada essa função permite que o **MD5713 MT** capture automaticamente imagens de pessoas não registradas.
Acionar alarme externo	Caso a opção esteja ativada e o usuário apresentar temperatura superior ao valor fixado nas configurações do dispositivo, o alarme externo será ativado.
Apagar alarme externo	Desliga o alarme externo que foi acionado.
Atraso no alarme externo	O tempo autodesligamento de acionamento do alarme externo poderá ser definido pelo usuário com um valor entre 1 e 255. O dispositivo permita que a função seja desativada
Atualização de *Firmware*	Neste menu, é possível atualizar a versão do software do módulo de medição de temperatura por imagem térmica.

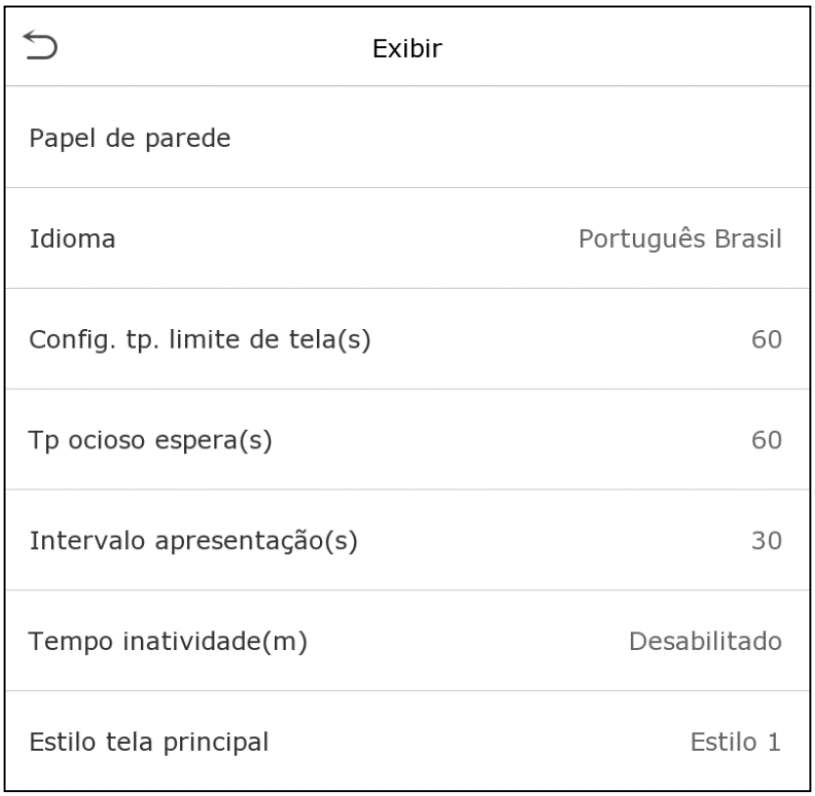
9. Personalização das configurações

Clique em **Personalizar** no menu principal e atualize as configurações de tela, áudio e alarme.



9.1. Configurações de interface

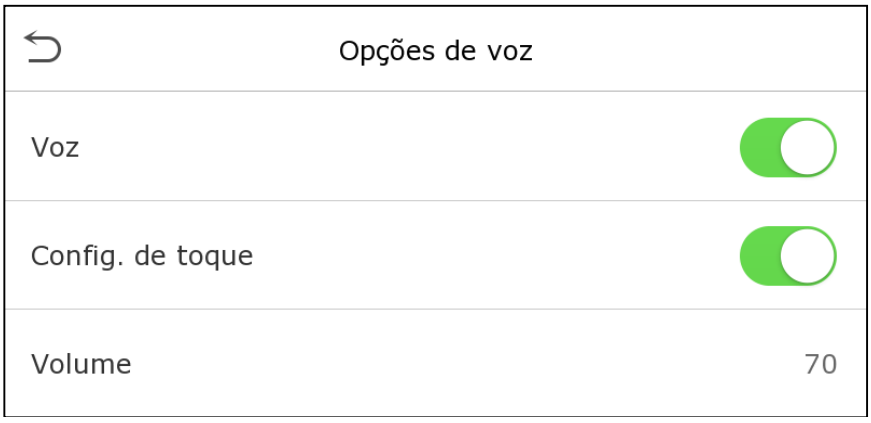
Clique em **Interface** para personalizar as configurações.



Item	Descrição
Papel de parede	Selecione um papel de parede desejado para tela principal.
Idioma	Selecione o idioma para operação do dispositivo.
Tempo de espera do menu na tela	Quando não houver operação e o tempo exceder o valor definido o aparelho voltará automaticamente para a tela inicial. É possível que a função seja desativada ou que o usuário defina o tempo entre 60 e 99.999 segundos.
Apresentação durante o ócio	Quando não houver nenhuma operação sendo realizada e tempo de espera exceder o valor estabelecido será reproduzida uma apresentação. Essa função também poderá ser desativada ou ter seu tempo definido com um valor entre 3 e 999 segundos.
Intervalo de apresentação dos slides	Refere-se ao intervalo de tempo para troca de imagens no dispositivo. A função poderá ser desativada ou que o usuário defina com um valor entre 3 e 999 segundos.
Tempo de inatividade para repouso	Se a opção estiver ativada e não houver um tempo de inatividade, o aparelho entrará em modo de repouso. Quando o usuário pressionar qualquer tecla o dispositivo voltará para o trabalho normal. Essa função também poderá ser desativada ou que o usuário defina com um valor entre 1 e 999 minutos.
Estilo de tela inicial	Selecione o estilo de tela principal de acordo com sua preferência.

9.2. Configurações de voz

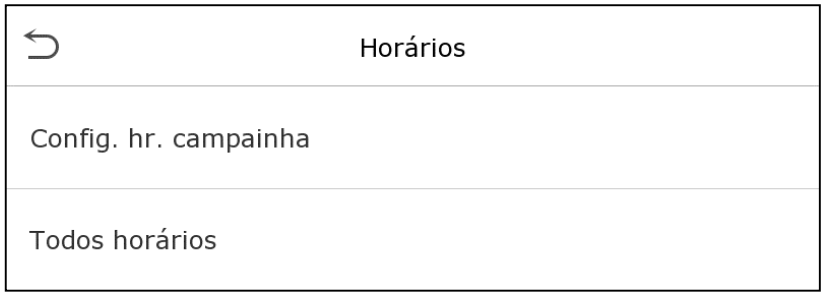
Clique em Voz e personalize as informações, confira:



Item	Descrição
Comandos por voz	Ative ou desative a função Comandos por voz.
Sons do teclado	Ative ou desative a função de som do teclado.
Volume	Ajuste o volume do dispositivo, entre 0-100.

9.3. Alarmes

Vá a **Personalização** e ajuste o item **Horários**, conforme a imagem abaixo:



- **Adicionando um alarme**

Clique em **Config. hr. campainha** para adicionar um novo horário.

tem	Descrição
***Status* do alarme**	Aqui é possível alterar o *status* dos alarmes.
Horário do alarme	Defina do horário em que o alarme soará.
Repetir	Defina o ciclo de repetição do alarme.
Toque	Configuração do som do alarme.
Intervalo campainha (s)	Ajuste a duração do alarme interno, os valores válidos são de 1 a 999 segundos.

Volte à página **Horários** e clique em **Todos horários** para ver o novo sinal adicionado.

- **Editar alarme**

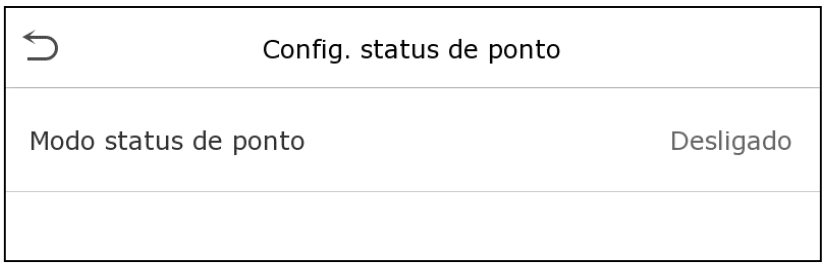
Na página **Todos horários**, clique no item que desejar editar, selecione **Editar** e siga o mesmo método utilizado para adicionar um novo alarme para realizar as alterações.

- **Apagar alarme**

Na página **Todos horários** clique no item desejado, selecione **Apagar** e selecione **[Sim]** para realizar a ação.

9.4. Configurações de ponto

Em **Config. *status* de ponto** é possível configurar os dados da melhor forma.



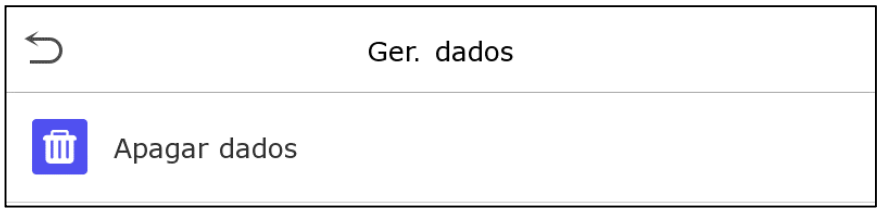
Item	Descrição
Modo do status de ponto	Selecione um modo de estado do ponto, podendo ser: **Desligado:** para desativar a função da tecla *status* de ponto. A chave de estado do ponto definida no menu Mapa de atalhos se tornará inválida. **Modo Manual:** para alternar manualmente a tecla de estado do ponto, e a tecla de estado do ponto desaparecerá após o Tempo limite do estado do ponto. **Modo Automático:** após esse modo ser escolhido, defina o tempo de comutação da tecla de estado do ponto em Mapa de atalhos; quando o tempo de comutação é atingido, a tecla de estado do ponto é comutada automaticamente**.** **Modo Manual e Automático:** nesse modo, a interface principal exibirá a chave de estado do ponto de comutação automática, mas também pode ser feita manualmente a troca de status. Após o tempo limite, a chave de estado do ponto de comutação manual se tornará a chave de estado do ponto de comutação automática. **Modo fixo manual**: depois que a chave do estado do ponto é alternada manualmente, a chave do estado do ponto permanece inalterada até ser trocada manualmente na próxima vez. **Modo fixo:** somente a tecla de estado do ponto fixo será exibida e não poderá ser alterada.

9.5. Atalhos

Os usuários podem configurar os atalhos para o *status* de ponto ou teclas funcionais para que sejam exibidos na tela principal.
Em **Personalização** clique em **Mapa de atalhos**, conforme a imagem abaixo:

10. Gerenciar dados

Para alterar os dados do **MD5714 F** clique em **Ger. dados** no menu principal.



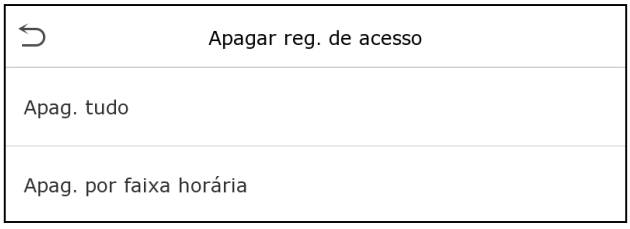
10.1. Apagar dados

Clique em **Apagar** dados na página **Ger. dados**.

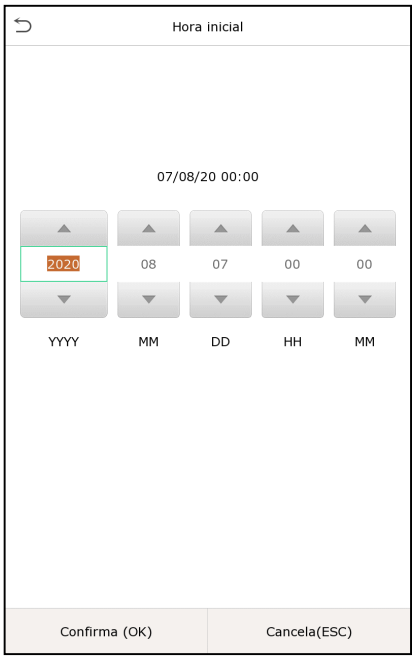
Item	Descrição
Apagar registros de acesso	Selecione para apagar os registros de acesso.
Excluir imagens dos registros de acesso	Exclua as fotos de registros das pessoas autenticadas.
Apagar fotos de validações com falha	Para apagar todos as fotos de autenticações falhas.

Apagar todos as informações	Aqui é possível excluir todos os registros de acesso dos usuários.
Apagar o administrador	Para remover o administrador.
Limpar os dados do controle de acesso	Apague todos os dados do controle de acesso.
Apagar as fotos dos usuários	Elimine todas as fotos de usuários.
Apagar o papel de parede	Apague todos os papéis de parede do aparelho.
Excluir os protetores de tela	Exclua todos os protetores de tela.

Importante: em caso de exclusão dos registros de acesso, fotos de presença ou fotos da lista de bloqueio, você poderá selecionar **Apagar tudo** ou **Apagar por período**, onde existe a possibilidade de determinar os dados que deseja excluir por um intervalo de tempo.



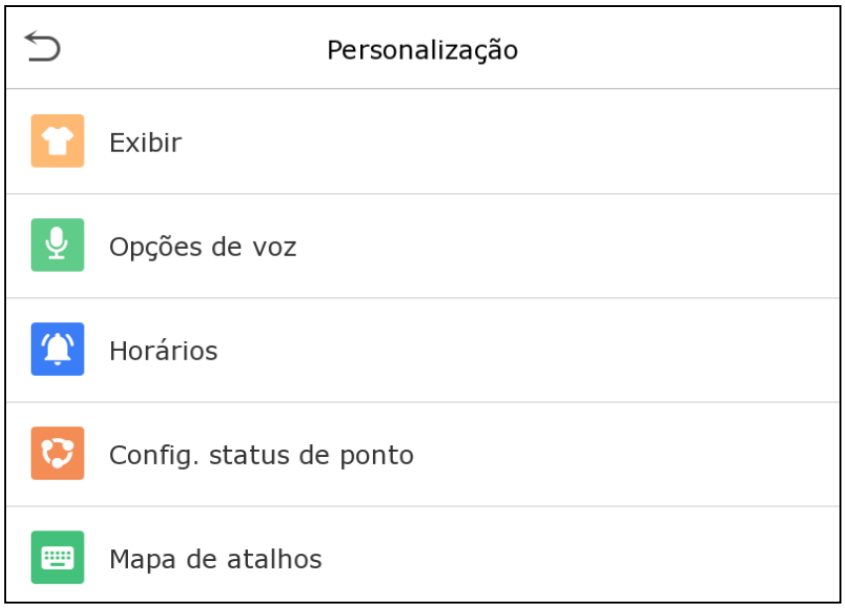
Selecione **Apagar período** e clique OK.



Defina o período a ser excluído e clique em OK.

11. Controle de acesso

O controle de acesso é usado para definir o horário de abertura das portas, controle das fechaduras e os demais parâmetros que controlam o acesso às áreas restritas.
Clique em **Controle Acesso** no menu principal.

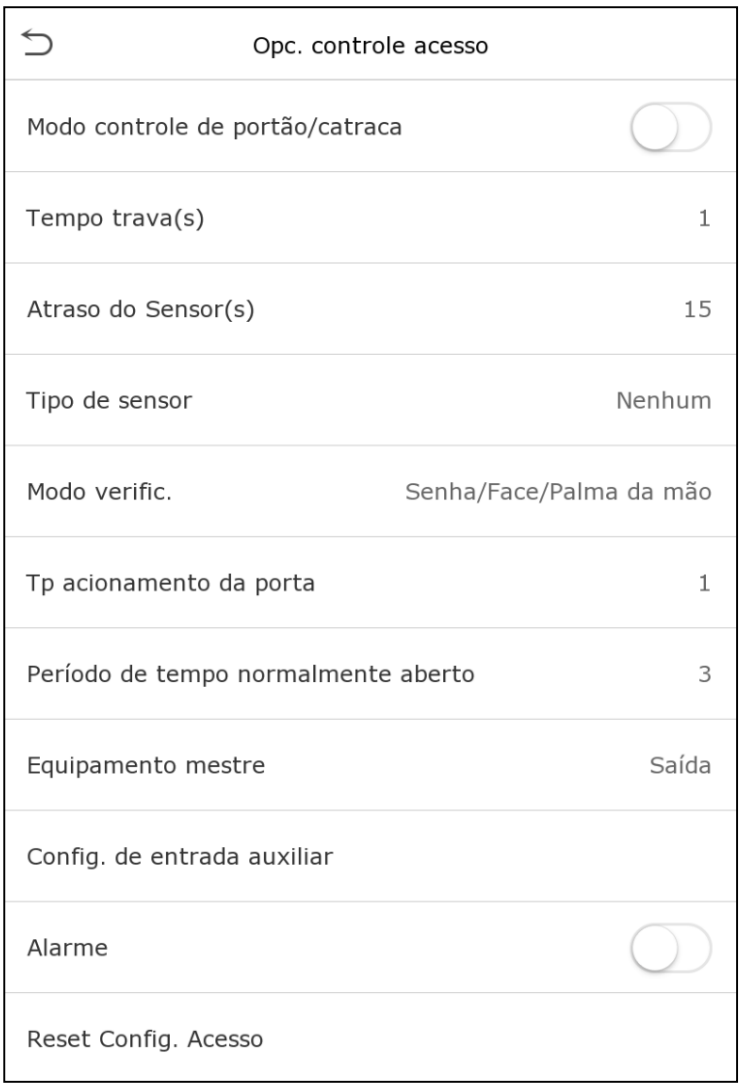


Para ter o acesso permitido é necessário que o usuário atenda às seguintes requisitos:

1. O faixa de horário para abertura da porta, deve estar dentro de qualquer faixa horária válida na regra de acesso do usuário.
2. O grupo do usuário deve estar na combinação de abertura da porta (quando houver outros grupos na mesma combinação de acesso, a verificação dos membros desses grupos também será necessária para abrir a porta).

11.1. Opções no controle de acesso

Neste item é possível definir os parâmetros de tempo de trava de controle do terminal e dos equipamentos relacionados.
Selecione **Controle Acesso** no menu do **MD5714 F** para alterar as definições.



Item	Descrição
Modo catraca	Caso o modo catraca esteja ativado, as configurações de relés de porta e sensor de porta serão desativadas.
Tempo para desbloqueio	Período em que a porta se manterá aberta após a autenticação válida do usuário. O valor varia entre 1 e 10 segundos. Zero segundos representam desligado e não fecha a saída a relé.
Tempo do sensor de porta	Se a porta não for trancada após o período de sua abertura um alarme será acionado. O tempo até a porta ser trancada varia de 1 a 255 segundos.

possíveis

Tipo de sensor da porta	Existem três modos para configuração de sensor: nenhum, normalmente aberto e normalmente fechado. No modo **Nenhum**, significa que o sensor da porta não será usado, sendo que **Normalmente aberto** significa que no estado de porta fechada, o sensor estará aberto. **Normalmente fechado** significa que no estado de porta fechada, o sensor estará fechado.
Modo de verificação	O método de verificação possui os modos senha/face, somente a identificação do usuário, senha ou somente a verificação da face.
Tempo disponível na porta	Aqui é possível definir o período de disponibilidade da porta.
Aberta em tempo normal	Tempo programado para o modo Normalmente Aberto para que a porta esteja destrancada.
Dispositivo mestre	Quando configurar os dispositivos mestre e auxiliar, somente o mestre poderá definir as entradas e saídas. **Saída:** o registro verificado será gravado como saída. **Entrada:** o registro verificado será gravado como entrada.
Configuração de entrada auxiliar	Defina o tempo de desbloqueio para a porta e o tipo de saída do dispositivo auxiliar. Os tipos de saída auxiliar são: Nenhum, Porta do gatilho aberta, alarme do gatilho, Porta do gatilho aberta e Alarme.
Modo de verificação RS485	No modo de verificação RS485 selecione: cartão/impressão digital, somente impressão digital, cartão, impressão digital + senha, cartão + senha, cartão + impressão digital ou cartão + impressão digital +senha.
Alarme sonoro	Utilizado para tocar um alarme sonoro em caso de campainha. Caso a porta seja fechada ou a verificação seja bem sucedida, o alarme será cancelado.

Resetar as configurações de acesso	Os parâmetros do controle de acesso incluem o tempo de abertura da porta, sensor da porta, o tipo de sensor da porta, o modo de verificação, o período normal de abertura, dispositivos mestre e alarmes. É importante lembrar que os dados de controle do acesso são apagados somente em **Gerenciar dados**.

11.2. Regras de tempo

Nos equipamentos, podem ser definidos até 50 regras de horários. Cada regra de horário pode conter até dez faixas horárias, ou seja, uma semana e três feriados, e cada faixa horária tem um período válido dentro de 24 horas por dia. Você pode definir no máximo 3 períodos para cada faixa horária. A relação entre esses períodos é "ou". Quando o horário de verificação cai em qualquer um desses períodos, a verificação é válida. O formato do período da faixa horária: HH MM-HH MM, tem a precisão de minutos de acordo com o relógio de 24 horas.
Para definir vá até **Config. regra de tempo** no menu **Controle acesso**.

1. Para inserir uma faixa horária para ser pesquisada, clique na caixa cinza de pesquisa e lembre-se que o número máximo de faixas horárias é 50.

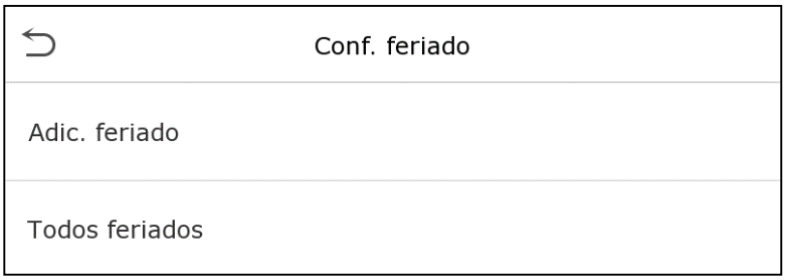
2. Clique na data em que as configurações de faixa horária são necessárias, digite a hora inicial, final e clique **OK**.

Importante:

- Caso a hora final seja anterior à hora inicial, como 23h57min a 23h56min, indica que o acesso é proibido durante o dia. Já quando a hora final é posterior à hora inicial, como 00h00min a 23h59min, estabelece que o intervalo é válido.
- Os períodos do dia em que o sistema deverá abrir a porta: aberto todos os dias, 00h00min a 23h59min, ou quando a hora final for após a inicial, como 08h00min a 23h59min.
- A faixa horária padrão 01 indica que a porta estará aberta durante todo o dia.

11.3. Configurações de férias

Sempre que houver alguém de férias será necessário que seja configurado um acesso especial, mas o mais indicado é que o método de acesso às áreas restritas seja aplicável a todos os funcionários e o usuário poderá ter acesso mesmo durante as férias.
No menu **Controle Acesso** clique em **Conf. feriado**, conforme abaixo:



- **Adicione uma nova configuração de férias**

Em **Conf. feriado** insira os parâmetros das férias que serão adicionadas.

- **Edite as férias**

No menu **Conf. feriado** selecione o item que será modificado, clique em **Editar** e altere as configurações desejadas.

- **Apagar período de Férias**

Na página **Conf. feriado** selecione o item que deverá ser eliminado e clique em **Apagar**, confirme em **OK**. Após essa ação o item não será exibido na página Férias.

11.4. Configurações de acesso combinado

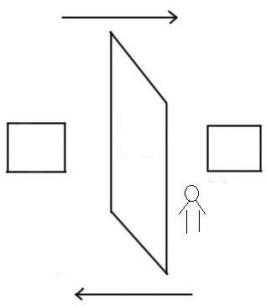
Os grupos de acesso são organizados em diferentes combinações de desbloqueio das portas para que a segurança esteja sempre reforçada.
Nas combinações de desbloqueio das portas, o intervalo do número combinado X é 0 ≤ X ≤ 5, sendo o total de membros X que podem pertencer a um grupo de acesso ou poderá pertencer a cinco grupos de acesso diferentes.
Em **Controle acesso** vá até **Acesso Combinado**, conforme abaixo:
Clique na combinação de desbloqueio de porta que será configurada, altere o número de combinações nas setas para cima e para baixo e, em seguida, confirme em **OK**.

Exemplos:
A verificação combinada para que a porta 1 se abra é definida com 01 03 05 06 08, o que indica que o conjunto de desbloqueio 1 consiste em cinco pessoas e que cada uma delas pertence a um grupo de controle de acesso diferente.
No acesso combinado da porta 2 a definição é 02 02 02 04 04 07, indicando que a combinação do desbloqueio 2 possui cinco pessoas e que os dois primeiros são do grupo 2, os seguintes do grupo 4 e somente o último do grupo 7.

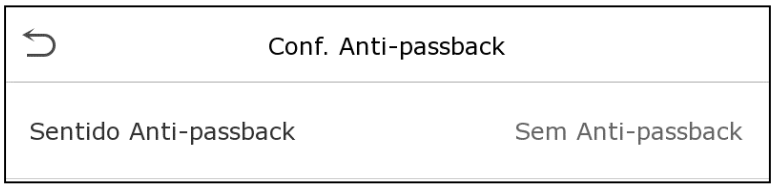
Apague um aceso combinado
Defina o número do grupo de acesso para zero, assim a combinação será apagada.

11.5. Configurações a*nti-passback*

Existe a possibilidade de um usuário ser seguido por outras pessoas ao entrar pela porta sem verificação, o que leva a um problema de segurança. Pensando nisso, o *anti-passback* é idealizado para evitar esse tipo de situação. Quando ativado os registros de entrada deverá coincidir com os registros de saída para abrir a porta.
Essa função requer dois dispositivos, um é instado dentro da porta (aparelho mestre) e o outro fora da porta (aparelho auxiliar), eles se comunicam por sinal *Wiegand*. A saída *Wiegand* pode ser configurada para entregar o ID do usuário ou o número do cartão



Em **Controle Acesso** encontre a opção ***anti-passback***, conforme abaixo:



Item	Descrição
Sentido *anti-passback*	**Sem *anti-passback*:** aqui o *anti-passback* está desativado, o que significa que a verificação será realizada com sucesso por meio do dispositivo mestre e auxiliar. Nesta opção o estado do atendimento não é salvo. ***Anti-passback* saída:** se o último registro do usuário for a saída, ele poderá registrar sua entrada, mas não poderá sair novamente. Caso ele tente o alarme será acionado. **Entrada e saída com *anti-passback*:** após a entrada o usuário ele poderá registrar, somente, sua saída. Caso o contrário seja tentado o alarme será acionado.

11.6. Configurações de coação

Se um usuário ativar a função coação durante uma verificação específica, o aparelho abrirá a porta normalmente e ao mesmo tempo será enviado um comando para acionar o alarme.
Em **Controle acesso** e clique em **Opc. de coação**, conforme abaixo:

Item	Descrição
Alarme na senha	Se o usuário utilizar a validação por senha o alarme será acionado, caso o contrário aconteça não soará nenhum sinal.
Alarme em impressão digital	Caso o usuário utilize uma impressão digital para realizar a verificação um alarme soará, se a digital não for usada não haverá nenhum sinal.
Acionamento do alarme	O alarme não soará enquanto seu tempo de acionamento não terminar. Esse tempo varia entre 1 e 999 segundos.
Senha de coação	Configure uma senha de coação com seis dígitos, assim quando algum usuário a digitar o alarme soará.

12. Pesquisa de acessos

Quando a identidade de alguém é verificada este registro fica salvo no **MD5714 F**, graças a esta função é possível verificar todos os acessos.
No menu principal clique em **Proc. registros**, conforme as imagens abaixo:

A busca por registros de ponto e fotos registradas é semelhante ao de busca pelos registros de acesso. Na página **Proc. registros**, clique em **Reg. acesso** para ter acesso aos dados, veja os detalhes no exemplo a seguir:
1.Digite o usuário que será pesquisado e clique em **OK**, caso seja necessário pesquisar todos os registros de usuários, clique em **OK** sem digitar nenhum usuário;
2.Selecione o período que deseja obter os registros;
3.Quando a pesquisa for completada, clique no item que estiver em verde para obter mais detalhes.

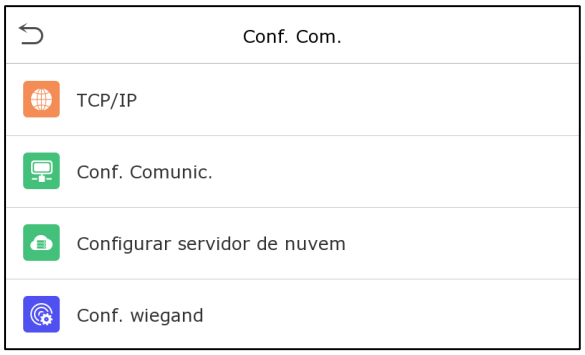
13. Autoteste

Teste automaticamente se todos os módulos do aparelho estão funcionando corretamente, incluindo a tela de LCD, áudio, impressões digitais, câmera e o relógio em tempo real.

Item	Descrição
Testar todos	Para testar automaticamente a tela de LCD, áudio, câmera e o RTC.
Testar LCD	Aqui é possível testar automaticamente o efeito exibido na tela LCD, incluindo as cores branco e preto puro para garantir que a tela está as exibindo normalmente.
Testar áudio	Testa automaticamente se os arquivos de áudio que foram armazenados no aparelho estão completos e se a qualidade está boa.
Testar impressões digitais	Para testar o sensor de impressão digital pressione um dedo no leitor e verifique se a imagem adquirida está clara.
Testar face	Realize o teste da câmera verificando se as fotos tiradas estão com a qualidade correta.
Testar relógio	O dispositivo testa se o relógio está funcionando corretamente com um cronômetro, é necessário um toque na tela para iniciar a contagem e outro toque para pará-lo.

14. Informações do sistema

Na opção **Info. sistema** você poderá visualizar os detalhes de armazenamento, versão do dispositivo e demais itens, conforme abaixo:



Item	Descrição
Capacidade	Exibe o armazenamento atual do aparelho incluindo os dados de palma da mão, impressão digital, senhas, rostos, administradores, registros de acesso, imagens de presença, fotos dos usuários e lista de bloqueio.
Info dispositivo	Informa o nome do aparelho, seu número de série, endereço MAC, palma da mão, versão de impressão digital, algoritmo facial, informações da plataforma e do fabricante.
Info *firmware*	Exibe as informações do *firmware* atual e outros detalhes do aparelho.

15. Conectando o Speed Face ao *software* ZKBioAccess

O **ZKBioAccess MTD** é uma plataforma leve, segura e desenvolvida pela **MADIS** em ambiente *web*, compatível com a maioria dos hardwares **MADIS**.
Especialmente pensado a linha *Visible Light* sem toque, e para a série de **MADIS** de produtos com temperatura corporal e detecção de máscara. O sistema possui soluções de gerenciamento para pequenas e médias empresas: gerenciando pessoas, controle de acesso, vigilância por vídeo, além da gestão de sistema, presença e temperatura em tempo real.

15.1. Configure o servidor

- **No aparelho**

1. Clique em **Conf. Com.**>***Ethernet*** no menu principal para definir o endereço de IP e a porta do aparelho. É importante que o endereço de IP seja capaz de se comunicar com o servidor **ZKBioAccess** e de preferência no mesmo segmento de rede e endereço do servidor.
2. Em **Conf. Com.**>**Conf. Comunic.** do servidor na nuvem para definir o endereço de IP e a porta de entrada no servidor.

Endereço do servidor: Definido como o endereço de IP do servidor **ZKBioAccess MTD**.
Porta do servidor: É definida como a porta de serviço do **ZKBioAccess**, seu padrão é 8088.

- **No *software***

Acesse o *software* **ZKBioAccess MTD**, clique em **Sistema**>**Comunicação**>**Comunicação com aparelho** e defina a porta de serviço, conforme as imagens abaixo:

15.2. Adicione o dispositivo ao *software*

Inicie o processo de busca da seguinte forma para adicionar um dispositivo:

1) Acesse os itens **Controle de Acesso** >**Dispositivo** >**Pesquisar**;
2) Clique em **Pesquisar**;
3) Após a busca, será exibida uma lista com o número total de controladores de acesso encontrados;
4) Clique em **Adicionar** e aguarde até que o dispositivo inserido.

15.3. Adicione as pessoas no *software*

1. Vá a **Pessoal** >**Novo**;
2. Preencha todos os parâmetros e clique em **OK**.

15.4. Monitore o *software* em tempo real

1. Clique em **Detecção de temperatura > Ger. Temperatura > Monitoramento em tempo real** para verificar todos os eventos, incluindo os dados de usuários com altas temperaturas.
   Quando o alarme de temperatura estiver configurado as temperaturas anormais serão sinalizadas em vermelho.
2. Em **Detecção de temperatura > Ger. Temperatura >Estatísticas** é possível analisar os dados das temperaturas colhidas.

*Para realizar operações específicas, por favor, confira o Manual de Usuário do software **ZKBioAccess MTD**.*

APÊNDICE 1

Requisitos de leitura das faces em tempo real através de luz visível

1. É recomendado que o registro em um ambiente interno com uma fonte de luz apropriada, sem sub e superexposição;
2. Não direcione o aparelho para luzes externas como: portas, janelas ou outras fontes de luzes fortes;
3. É recomendado que para uma leitura qualificada utilize-se roupas escuras nas autenticações, de forma que o fundo da imagem tenha outra coloração de contraste;
4. Garanta que todo o rosto esteja sendo capturado sem que a testa e as sobrancelhas estejam cobertas pelos cabelos;
5. Exiba uma expressão facial simples e natural, não feche os olhos, nem incline a cabeça para qualquer direção. Quem usa óculos deverá ter duas imagens registradas sendo uma com e outra sem o acessório (dois cadastros);
6. Não utilize lenços ou máscaras que cubram a boca e o queixo durante a captura.
7. Mantenha a face posicionada na área de captura conforme exemplificado na Imagem 1 e olhe diretamente para a câmera do aparelho;
8. Não posicione mais de uma pessoa por vez na área de captura;
9. A distância recomendada entre o usuário e o aparelho é de 50 cm - 80 cm.

Requisitos para coleta de imagens faciais pela luz visível

A foto deve ser colorida, conter apenas um usuário e ele não deve estar uniformizado. Lembrando que usuários que usam óculos devem ser registrados com e sem o acessório.

- **Distância dos olhos**

É recomendado que a distância tenha 200 *pixels* ou mais e nunca menos de 115 *pixels*;

- **Expressão facial**

É necessário estar com a expressão natural.

- **Gestos e ângulo**

Os ângulos de rotação horizontal, elevação e depressão não devem exceder ±10°.

- **Acessórios**

Máscaras e óculos coloridos não são permitidos.

- **Rosto**

Deve aparecer o rosto completo com contorno claro em escala real, luz uniformemente distribuída e sem sobra.

- **Formato das imagens**

As fotos são geradas em BMP, JPG ou JPEG.

- **Requisitos dos dados:**

Devem ser cumpridos os seguintes itens:

1) Quando a roupa do usuário for escura, mantenha o fundo da imagem claro;
2) Método de cor em 24 *bit*;
3) Imagens em formato JPG com tamanho máximo de 20kb;
4) Taxas de definição entre 358 x 441 para 1080 x 1920;
5) A imagem deve conter os ombros do usuário capturados no mesmo nível horizontal;
6) O usuário precisa estar com os olhos abertos, as írises claramente a vista e não poderá sorrir mostrando os dentes no momento da captura;
7) O usuário deve ser visto claramente na imagem com sua cor natural, sem mancha de luz, reflexo no rosto ou no fundo e nenhuma distorção óbvia na imagem. É importante que os níveis de contraste e leveza estejam calibrados devidamente;
8) Taxa de definição entre 358 x 441 a 1080 x 1920.

APÊNDICE 2

Direitos de privacidade

Prezado (a) cliente, .
Obrigado por escolher um produto de reconhecimento biométrico projetado e fabricado pela **MADIS**. Como um fornecedor de renome mundial das principais tecnologias de reconhecimento biométrico, estamos pesquisando e desenvolvendo constantemente novos produtos e novas tecnologias. Nos esforçamos para seguir todas as leis de privacidade de cada país em que nossos produtos são comercializados.
Declaramos que:

1. Todos os nossos dispositivos civis de reconhecimento de impressões faciais capturam apenas características, não imagens digitais, assim não envolvem proteção de privacidade;
2. Nenhuma das características das impressões digitais que capturamos pode ser utilizada para reconstrução de uma imagem da digital original e não envolve proteção de privacidade;
3. Enquanto fornecedor deste dispositivo não assumiremos nenhuma responsabilidade direta ou indireta por quaisquer consequências que possuam resultantes do uso deste dispositivo;
4. Caso seja necessário contestar os direitos humanos ou questões de privacidade relativas ao uso dos nossos produtos, por favor, entre em contato com seu fornecedor.

Os produtos ou ferramentas **MADIS** de desenvolvimento de impressões digitais podem capturar as imagens originais dos usuários. Para obter mais detalhes sobre as leis de direito à privacidade, por favor, entre em contato com seu Governo ou fornecedor do dispositivo. Enquanto fabricante dos dispositivos não assumiremos nenhuma responsabilidade legal.
Importante:
As leis chinesas incluem as seguintes determinações sobre a Liberdade individual de seus cidadãos:

1. Não deve haver prisão, detenção, busca ou violação ilegal das pessoas;
2. A dignidade pessoal está diretamente relacionada a liberdade individual e não deve ser violada;
3. A residência de nenhum cidadão pode ser violada;
4. O direito de todo cidadão a comunicação e confidencialidade dessas informações dessas informações são protegidos por lei.

Gostaríamos de enfatizar ainda mais que o reconhecimento biométrico é uma tecnologia avançada que certamente será usada no comércio eletrônico, bancos, seguros, judiciais e em outros setores no futuro. Todos os anos o mundo inteiro está sujeito a grandes perdas em função da natureza insegura das senhas, sendo assim os produtos biométricos são usados para proteger sua identidade em ambientes de alta segurança.

Período ecologicamente correto

O período de operação ecologicamente correta refere-se ao tempo que o produto não descarrega nenhuma substância tóxica ou perigosa quando utilizado de acordo com os pré-requisitos do Manual.
Este período ecologicamente correto não inclui baterias ou outros componentes que são desgastados com facilidade e precisam ser substituídos periodicamente. A bateria do produto, por exemplo, possui o período ecologicamente correto de cinco anos.

Substâncias tóxicas ou perigosas e suas quantidades

Nome do componente	Substância tóxica					
	Chumbo (Pb)	Mercúrio (Hg)	Cádimio (Cd)	*Hexavalentchromium* (Cr6+)	*PolybrominatedBiphenyls* (PBB)	*PolybrominatedDiphenylEthers* (PBDE)
Resistência do chip	×	○	○	○	○	○
Capacitor do chip	×	○	○	○	○	○
Introdutor de chip	×	○	○	○	○	○
Diodo	×	○	○	○	○	○
Componentes ESD	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adaptador	×	○	○	○	○	○
Parafusos	○	○	○	×	○	○

○ indica que a quantidade total de conteúdo tóxico em todos os materiais homogêneos está abaixo do limite, conforme especificado no SJ/T 11363—2006.
× indica que a quantidade total de conteúdo tóxico em todos os materiais homogêneos excede o limite, conforme especificado no SJ/T 11363—2006.
Observação: 80% dos componentes desde produto são fabricados utilizando materiais ecologicamente corretos e que não são tóxicos. Os componentes que contêm toxinas ou elementos nocivos são incluídos devido às atuais limitações econômicas ou técnicas que impedem sua substituição por materiais não tóxicos.

Revisão – 00– Agosto de 2022
Neo-Tagus Industrial Ltda.
Av. Diógenes Ribeiro de Lima, 2346 - Alto de Pinheiros - São Paulo – SP - Brasil
Fone: 55 11 3026-3000
www.madis.com.br / madis@madis.com.br

Manual produzido por:
Neo-Tagus Industrial Ltda.
Imagens meramente ilustrativas.
As especificações aqui mencionadas têm caráter informativo e podem sofrer alterações sem aviso prévio.