Manual de usuário ProFaceX [TI]

Data: fevereiro de 2021

Obrigado por escolher nosso produto. Por favor, leia as instruções cuidadosamente antes da operação. Siga estas instruções para garantir que o produto esteja funcionando corretamente. As imagens mostradas neste manual são apenas para fins ilustrativos.

Para mais detalhes, acesse o site **www.zkteco.com.br**

Copyright © 2021 ZKTECO CO., LTD. Todos os direitos são reservados.
Não é permitida a cópia, alteração ou encaminhamento de nenhuma parte deste manual sem a autorização prévia da **ZKTeco**. Todo o conteúdo nele publicado pertence à **ZKTeco** e suas filiais.

Marca registrada

ZKTeco é uma marca registrada **ZKTeco**.

Outras marcas registradas envolvidas neste manual pertencem a seus respectivos proprietários.

Informações importantes

O conteúdo deste manual, incluindo todas as informações e imagens, é referente a operação e instalação dos produtos **ZKTeco** e pode ser divulgado somente com ordens expressas da empresa.

O manual deve ser lido por completo antes da operação ser iniciada e se houver dúvidas com relação às informações descritas nele, por favor, entre em contato com a **ZKTeco** antes de utilizá-lo.

É um pré-requisito para operação correta dos produtos que os usuários que irão operá-lo tenham recebido treinamento adequado, conheçam e tenham compreendido todas as informações contidas no manual.

ZKTeco Co., Ltd (ZKTeco) não oferece garantia com relação às informações apresentadas neste manual e as alterações nele incluídas. A empresa não estende garantia de qualquer natureza, englobando o *design* ou sua comercialização para outros fins.

O fabricante não assume responsabilidade por quaisquer erros ou omissões nas informações e documentos que são referenciados neste manual. O risco quanto aos resultados e desempenho obtidos com a utilização da informação é de completa responsabilidade do usuário.

A **ZKTeco** não é responsável por qualquer dano acidental, consequencial, indireto ou especial, incluindo perda de negócios, lucros, interrupção de negócios, perda de informações comerciais ou qualquer outro tipo de perda decorrente, relacionada ou não com a utilização ou referenciada neste manual, mesmo que a **ZKTeco** tenha sido avisada da possibilidade de tais danos.

A **ZKTeco** detém o direito de acrescentar ou alterar as informações publicadas no manual de tempos em tempos em formato de circulares, cartas ou notas etc. afim de aprimorar o funcionamento e segurança dos equipamentos. Este tipo de alteração destina-se à melhoria do funcionamento dos equipamentos e para essas alterações não conferem qualquer direito de reclamação, dano ou indenização em quaisquer circunstâncias.
Sendo assim, este produto receberá atualizações sem aviso prévio. Para verificar os procedimentos operacionais mais recentes, acesse o site http://www.zkteco.com.br
A **ZKTeco** não se responsabiliza (i) em casos de mau funcionamento do equipamento devido a qualquer não cumprimento das instruções contidas neste manual (ii), em casos de funcionamento do equipamento além de seus limites (iii) ou de equipamentos em condições diferentes das descritas neste manual.

Lembramos que este manual introduz as operações do **ProFaceX [TI]**.

Todas as imagens exibidas no manual são apenas para fins ilustrativos e podem não ser exatamente consistentes com os produtos reais.

Características sinalizadas com ★ não estão disponíveis em todos os aparelhos.

Se ocorrer algum problema com relação ao produto, por favor, entre em contato conosco.

Suporte Técnico ZKTeco do Brasil

Site: zkteco.com.br

E-mail: suporte.brasil@zkteco.com

A empresa

A **ZKTeco Co., Ltd (ZKTeco)** é uma multinacional especialista em verificação biométrica, fabricante de produtos de três grandes segmentos: equipamentos de verificação biométrica; tecnologia inteligente de controle de entrada e saída de pessoas + veículos + objetos, e a plataforma de escritório inteligente baseada em nuvem. Oferecemos serviços para empresas públicas e privadas, e produtos para consumidores finais instalarem em suas residências.

A **ZKTeco** possui aproximadamente 3.500 funcionários, sendo cerca de 1.000 atuando em equipes de P&D e 600 em escritórios ao redor do mundo. Temos 45 filiais na China e 48 escritórios espalhados em diversos países.

Contamos com vários centros de desenvolvimento, design e inovações no Vale do Silício, Europa, Índia, Dongguan, Xiamen e Dalian. Hoje, as técnicas e terminais inteligentes da **ZKTeco** já são utilizados pela maioria das 500 principais empresas mundiais e estamos presentes em mais de 100 países e regiões.

Buscamos integrar técnicas de verificação biométrica híbrida e técnicas de visão computacional à *Internet*, *IoT*, *big data* e computação em nuvem por meio de softwares, como o **ZKBioSecurity**.

Nossas soluções podem ser aplicadas em empresas, escolas, residências, aeroportos, entre vários outros segmentos.

Nosso portfólio contempla mais de 400 produtos e é utilizado no Brasil em grandes empresas. Entre os equipamentos que fabricamos estão terminais e câmeras de reconhecimento facial, raio-x, detectores de metais, catracas, cancelas, fechaduras digitais, entre outros produtos de controle de acesso, segurança de inspeção, controle de entrada de pessoas + veículos + objetos e *smart home*.

Em 2020, a empresa mudou sua sede brasileira para Vespasiano, região metropolitana de Belo Horizonte/MG, com instalações de 3.000m², em um terreno de 22.000 m², e passou a fabricar equipamentos no Brasil. Além disso, possuímos uma equipe de P&D para o desenvolvimento de soluções especificamente para as demandas brasileiras.

Índice

1. Visão geral 7
2. Instruções de uso 7
2.1 Posição dos pés, expressão facial e postura corporal 7
2.2 Registro de palma 9
2.3 Registro de faces 10
2.4 Interface do dispositivo 11
2.5 Teclado virtual 12
2.7 Métodos de verificação 12
2.7.1 Verificação de palma 12
2.7.2 Verificação de senha 15
2.7.3 Verificação facial 18
2.7.6 Verificação combinada 22
3. Menu principal 22
4. Gestão de usuários 24
4.1 Adicione usuários 24
Registro de palma 27
Registro de face 28
Registro de senha 29
Registro de foto do usuário 29
Controle de acesso 29
4.2 Pesquisa por usuários 30
4.3 Editar usuários 30
4.4 Apagar usuários 30
5. Permissões do usuário 31
6. Configurações de rede 33
6.1 Rede 34
6.2 Conexão com o PC 35
6.3 Rede sem fio 35
6.4 Configurações do servidor na nuvem 36
6.5 Configurações *Wiegand* 37
Saída *Wiegand* 39
7. Configurações de sistema 40
7.1 Data e hora 41
7.2 Configurações de acesso 42
7.3 Parâmetros de faces 43
7.4 Parâmetros de palma 46

7.5 Resetando o dispositivo 47
7.6 Gestão de temperatura 47
7.7 Gestão de Detecção 48
8. Personalização configurações.... 50
8.1 Configurações de interface 51
8.2 Configurações de voz 52
8.3 Alarmes 52
Adicionando um alarme 52
Editar alarme 53
Apagar alarme 53
8.4 Configurações de ponto 53
8.5 Mapeamento de teclas de atalho.... 54
9. Gerenciar dados.... 54
9.1 Apagar dados 54
10. Controle de acesso....57
10.1 Opções no controle de acesso....57
10.2 Regras de tempo 59
10.3 Configurações de férias 61
Adicione uma nova configuração de férias 61
Edite as férias 61
Apagar período de Férias.... 61
10.4 Configurações de acesso combinado 61
Apague um acesso combinado 62
10.5 Configurações *anti-passback*....62
10.6 Configurações de coação....63
11. Pesquisa de acessos.... 64
12. Autoteste 65
13. Informações do sistema 66
14. Conectando o SpeedFace [P] ao *software*.... 66
14.1 Configure o servidor 67
14.2 Adicione o dispositivo ao *software* 67
Adicione as pessoas no *software*....67
14.3 Monitore o *software* em tempo real 67
Apêndice 1.... 68
Apêndice 2.... 70
Período ecologicamente correto.... 71

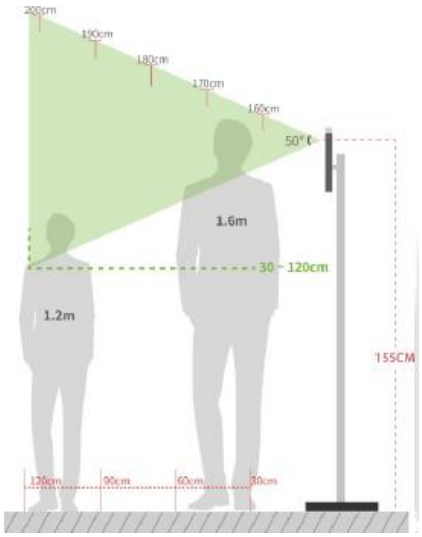
1. Visão geral

Este documento descreve o procedimento operacional do dispositivo **ProFace X [TI]**. Os módulos operacionais do dispositivo incluem gerenciamento do usuário, atribuição de função do usuário, comunicação do dispositivo, detecção de temperatura, controle de acesso e assim por diante. O dispositivo oferece suporte ao acesso descomplicado dos usuários às instalações, sem comprometer nenhum aspecto de segurança, garantindo assim a proteção.

2. Instruções de uso

2.1 Posição dos pés, expressão facial e postura corporal

- **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 a frente e para trás para melhorar a qualidade das imagens faciais capturadas.

- **Expressões faciais e postura**

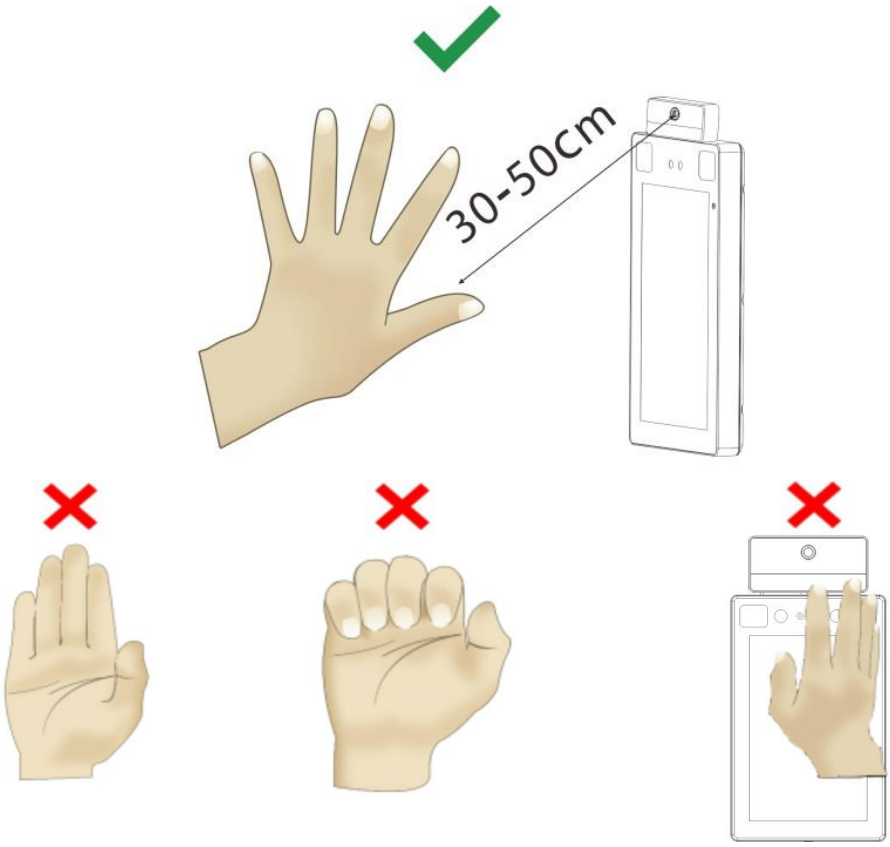
Durante o registro e a verificação biométrica, por favor, permaneça com a expressão facial e postura posicionadas naturalmente.

Importante: Durante a inscrição e verificação, mantenha as expressões faciais e postura corporal naturais.

2.2 Registro de palma

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

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



2.3 Registro de faces

Mantenha o face 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 esta configuração:

Métodos de autenticação e registro facial:

Instruções para registrar um rosto

- Ao registrar um rosto, mantenha uma distância de 40 a 80 cm entre o dispositivo e o rosto.
- Tenha cuidado para não alterar a expressão facial – rosto sorridente, rosto maquiado ou piscando.
- Se você não seguir as instruções na tela, o registro do rosto poderá demorar ou falhar.
- Tenha cuidado para não cobrir os olhos ou sobrancelhas.
- Não use chapéus, máscaras ou óculos escuros.
- Tenha cuidado para não mostrar duas faces na tela, registre somente uma pessoa de cada vez.
- Recomenda-se a um usuário que usar óculos de grau registre o rosto com e sem óculos.

Instruções para autenticar um rosto

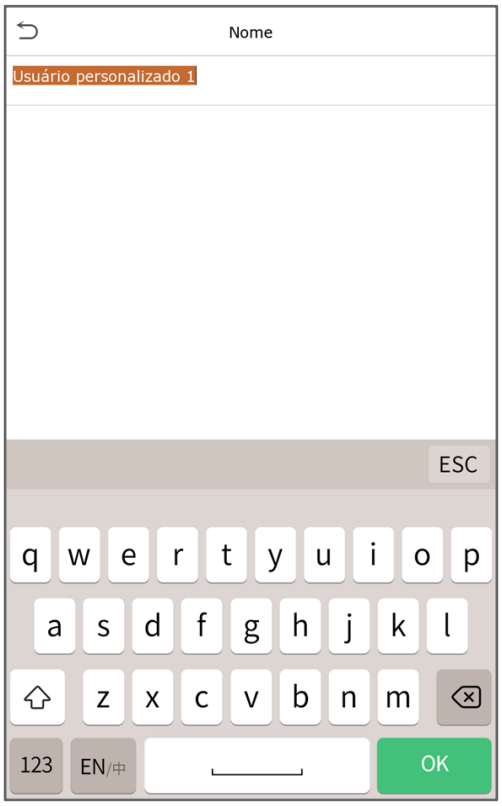
- Certifique-se de que o rosto está posicionado dentro da área de detecção exibida na tela do dispositivo.
- Se os óculos de grau forem trocados, a autenticação pode falhar. Se o rosto sem óculos foi registrado, autentique o rosto sem óculos. Caso apenas o rosto com óculos foi registrado, autentique o rosto com os óculos usados anteriormente.
- Se uma parte do rosto estiver coberta por um chapéu, máscara, tapa-olho ou óculos de sol, a autenticação poderá falhar. Não cubra o rosto, permita que o dispositivo reconheça as sobrancelhas e o rosto.

2.4 Interface do dispositivo

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

- Clique em para ir até a página de autenticação do usuário no modo 1:1.
- 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 **ProFaceX [TI]** e sempre que for necessário acessar o menu será necessário que o administrador valide a ação.

2.5 Teclado virtual



- O **ProFace X [TI]** possui a entrada de caracteres, números, símbolos chineses e ingleses.

Clique em [**En**] para mudar para o teclado inglês

- Pressione [**123**] para mudar para o teclado numérico e para voltar ao alfabético clique em [**ABC**];
- Em [**ESC**] você sairá do teclado.

2.7 Métodos de verificação

2.7.1 Verificação de palma

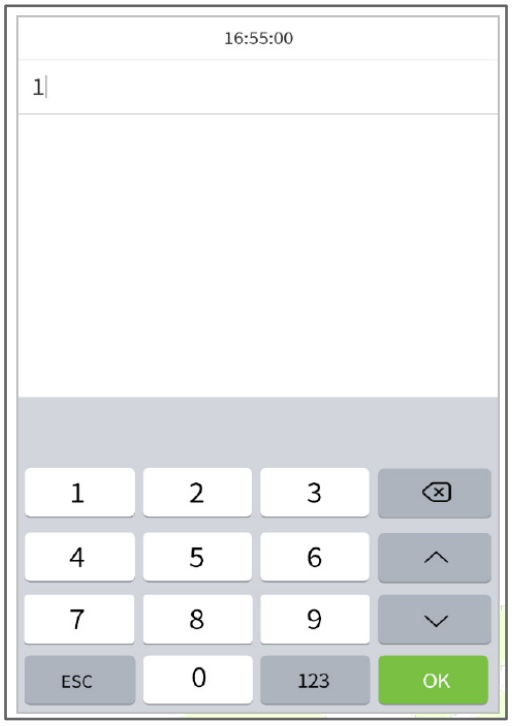
O **modo 1:N (um para muitos)** de verificação da palma compara a imagem da mão coletada pelo **ProFaceX [TI]** com todos os registros de palma salva no aparelho.

Posicione a mão na área de leitura, assim o **ProFaceX [TI]** automaticamente realiza a distinção entre o modo de verificação de palma e o modo de verificação da face.

- **Modo 1:1 (um para um) de verificação de palma**

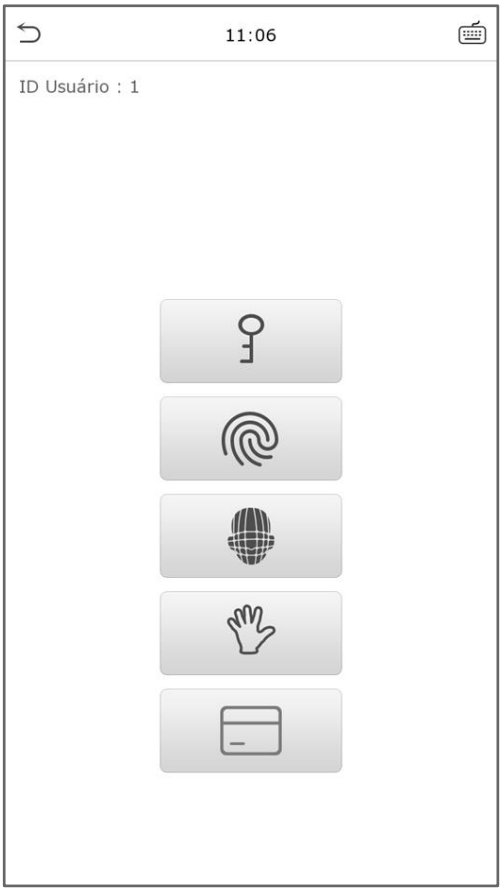
Clique em e acesse a tela de autenticação 1:1, digite o ID do seu usuário e pressione [**OK**].

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



Se o usuário tiver registrado a impressão digital, face, senha, palma da mão, e o método de verificação estiver definido como Senha/Imp. Dig. /Cartão/Face/Palma da mão, a seguinte tela será exibida.

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

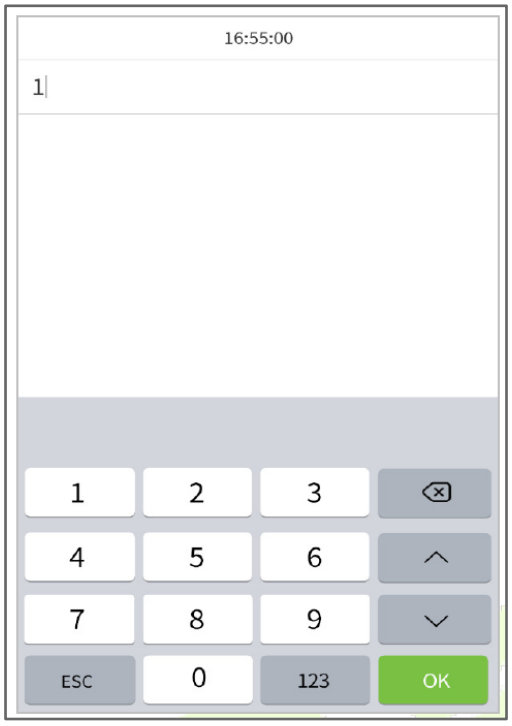


2.7.2 Verificação de senha

A verificação de senha compara a senha inserida com a senha cadastrada dentro do ID de usuário registrado.

- Acesse no menu principal para abrir o modo de verificação 1:1 (um para um) de senha.

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

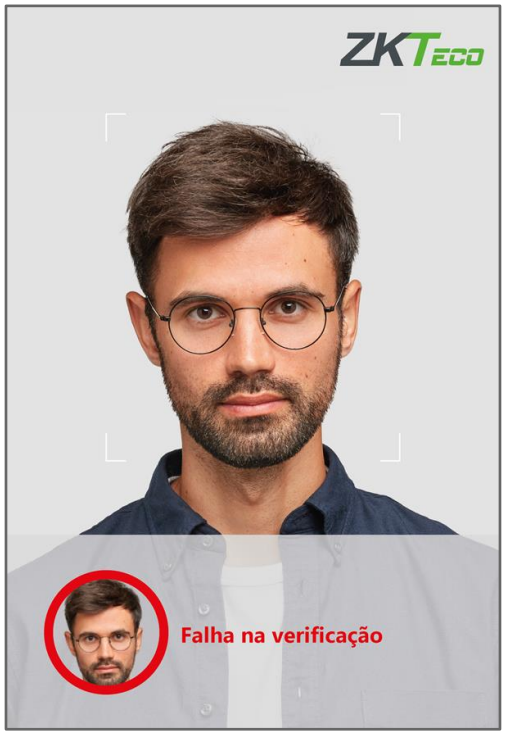


Caso o usuário registre a palma da mão, impressão digital e a face, além da senha. A tela abaixo será exibida, em seguida selecione para acessar o modo de verificação por senha.

2. Insira a senha e clique em [**OK**].

Verificação realizada com sucesso:

A verificação falhou:



2.7.3 Verificação facial

1. Verificação 1:N (um para muitos) facial

A verificação convencional compara faces adquiridas com todos os dados faciais registrados no **ProFace X [TI]**. Confira abaixo a caixa *pop-up* com o resultado da comparação.

2. Medição de temperatura com infravermelho

Quando a opção de triagem de temperatura com função infravermelha estiver habilitada, durante a verificação do usuário, além do método de verificação convencional, o rosto do usuário deve estar alinhado com a área de detecção de temperatura para detectar a temperatura corporal antes que a verificação convencional seja realizada.

3. Detecção de máscara

Quando o usuário habilita a função de detecção de máscara, o dispositivo identifica se o usuário está usando máscara ou não. A seguir está a interface de verificação.

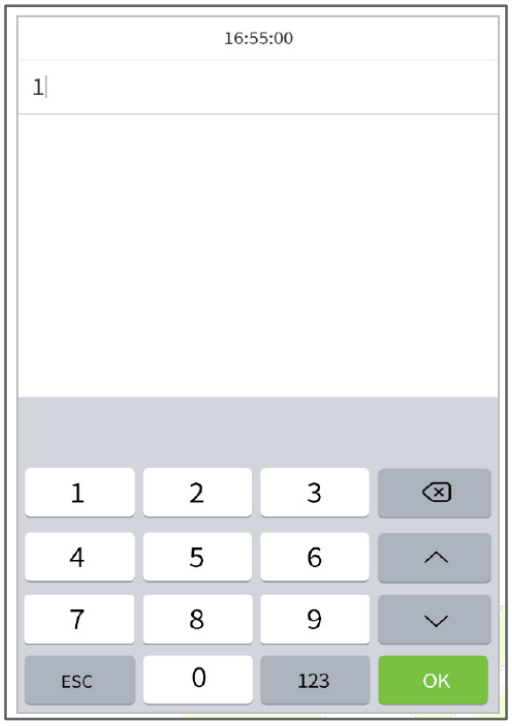
4. Exibir Figura Termodinâmica

Quando o usuário habilitou a função **Exibir Figura Termodinâmica**, durante o processo de detecção, a imagem térmica da pessoa será exibida no canto superior esquerdo do **ProFace X [TI]**.

- **Verificação 1:1 (um para um) facial**

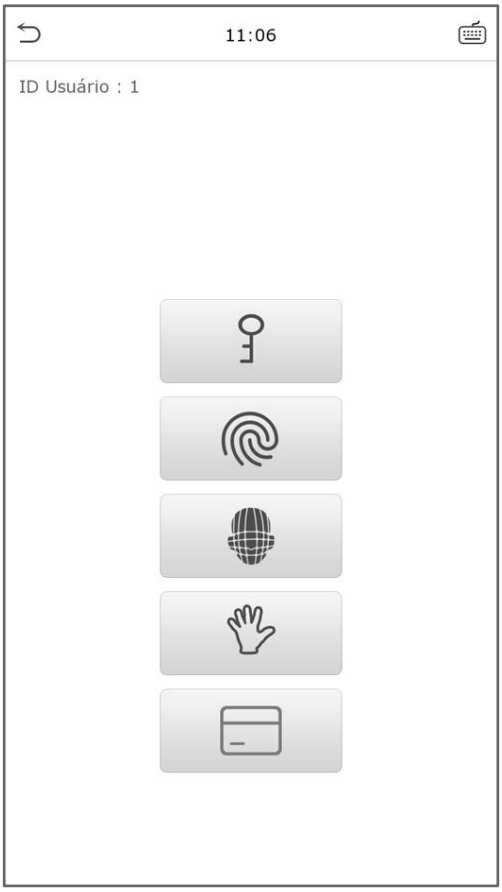
Neste modo de identificação o **ProFace X [TI]** compara a face capturada pela câmera com o modelo facial cadastrado no dispositivo.

1. Selecione no menu principal e acesse o modo de verificação 1:1 (um para um).
2. Insira o ID do usuário cadastrado e clique em [**OK**].



Caso o usuário registre a palma da mão, impressão digital e senha, além da face, e o método de verificação estiver definido como Senha/Imp. Dig. /Cartão/Face/Palma da mão a tela abaixo será exibida.

Selecione para acessar a verificação de face.



2.7.6 Verificação combinada

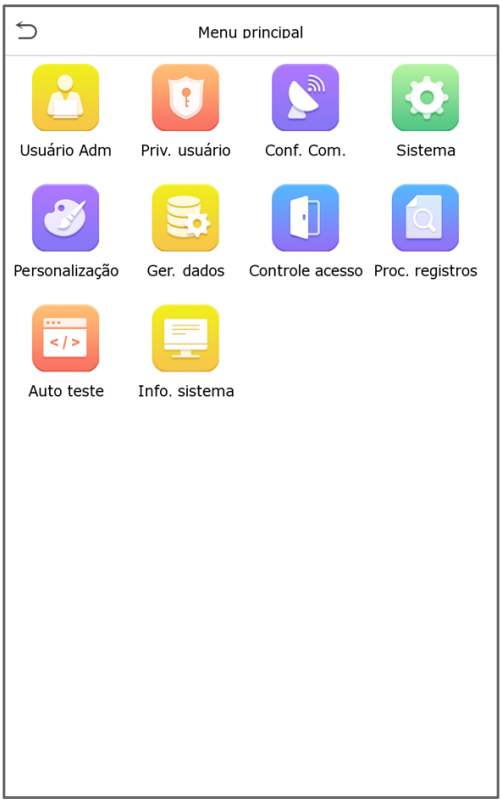
O **ProFace X [TI]** oferece a opção de múltiplas formas de verificação para aumentar ainda mais sua segurança. Existem 15 combinações de verificação possíveis, conforme as orientações abaixo:

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 da face, mas o modo de verificação é Face + Senha este usuário não passará na verificação.

3. Menu principal

Clique em ☰ na página inicial para acessar o menu, conforme a imagem abaixo:



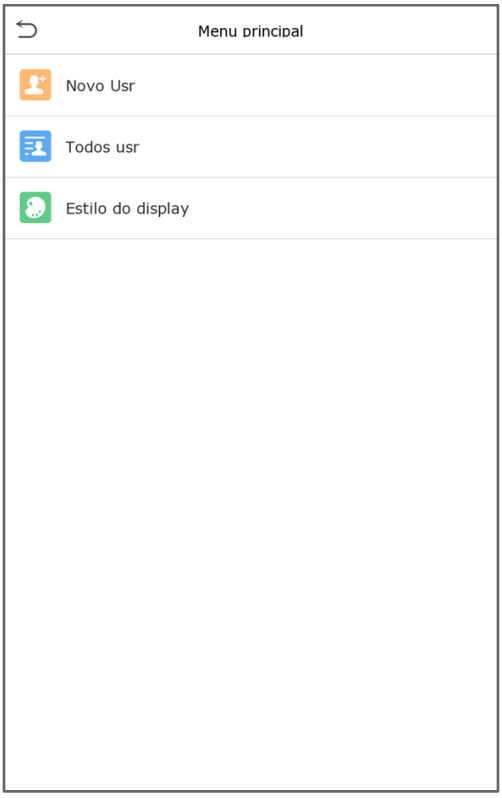
Item	Descrição
Usuário Adm.	Para adicionar, editar, ver e deletar as informações básicas do usuário;
Priv. usuário	Para definir as permissões personalizadas e das inscrições, ou seja, direito de alterar o sistema;
Conf. Com.	Para definir os parâmetros de rede, comunicação de serial, conexão com PC, rede sem fio, servidor de nuvem e *Wiegand*;
Sistema	Verificar os parâmetros relevantes da rede, comunicação do serial, conexão com o computador, rede *Wi-Fi* e servidores em nuvem;
Personalização	Aqui o usuário encontrará da voz, sinal, definição de 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 especificados, verifique as imagens de presença e a 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.

4. Gestão de usuários

4.1 Adicione usuários

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



Clique em **Novo Usr**, registre o ID e o nome do usuário.

Novo Usr	
ID Usuário	5
Nome	
Regra Usr	Usuário
Palma	0
Imp. Dig.	0
Face	0
No. Cartão	
Senha	
Foto usuário	0
Priv. controle acesso	

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", assim você deverá escolher outro nome ou ID.

Definição do papel do usuário

O **ProFace X [TI]** conta com dois tipos de contas de usuário: Usuário normal e Super admin. Caso já exista um usuário registrado como administrador, os usuários normais não têm direitos para gerenciar o sistema e podem acessar somente as verificações de identidades.

O administrador possui todos os privilégios de gestão do sistema, caso uma função personalizada seja definida, selecione as permissões de função definidas pelo usuário. Selecione uma opção entre **Usuário Normal** ou **Super Admin**.

Importante: Se a função de usuário selecionada for **Super Admin**, o usuário deve passar na autenticação de identidade para acessar o menu principal. A autenticação é baseada nos métodos de autenticação que o **Super Admin** registrou.

- **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 de foto do usuário**

Quando um usuário registrado com uma foto passa pela autenticação, a foto registrada será exibida.

Acesse a opção **Foto Usr.**, clique no ícone da câmera para registrar uma nova imagem, em seguida o sistema voltará para a interface **Novo Usuário** após tirar uma foto.

Assim que registrar a foto do usuário, o sistema captura automaticamente uma foto que será usada como foto do usuário. Caso uma imagem não seja capturada para foto do usuário, o sistema definirá automaticamente a foto capturada durante o registro do utilizador como foto padrão.

- **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

atribuídos a outros grupos e o dispositivo suporta até 99 grupos de controle de acesso. Clique em Período, selecione o período a ser usado.

4.2 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.

4.3 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 no item **Adicionar usuários**.

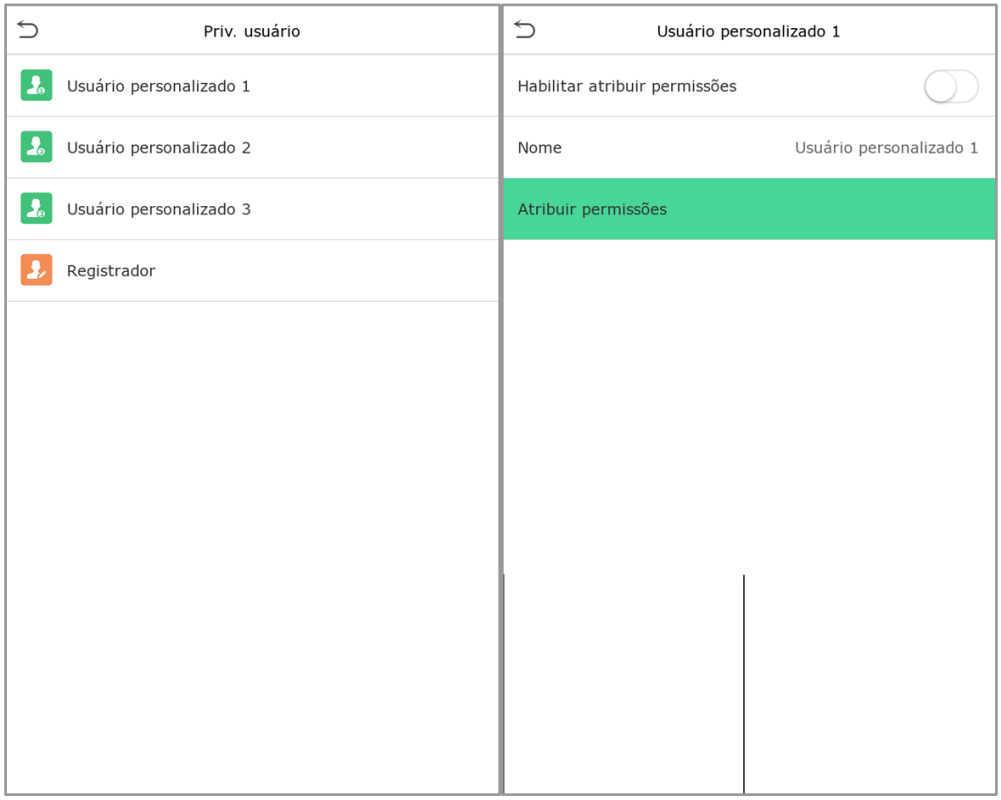
4.4 Apagar usuários

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.

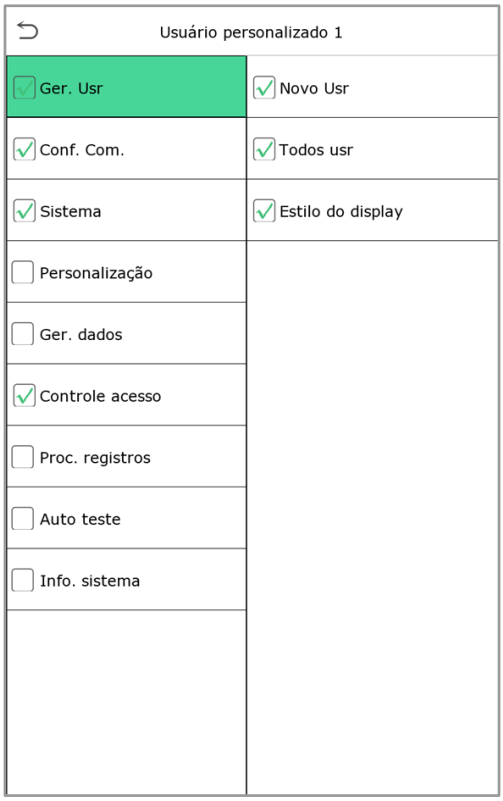
5. Permissões do usuário

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

Se você precisar atribuir algumas permissões específicas a certos usuários, você pode editar a **Função definida pelo usuário** no item Função do Usuário. É possível definir até 3 funções e atribuir para cada usuário, acesse Priv. usuário no menu principal.



1. Clique no item Atribuir permissões, clique em **Nome**, digite o nome da função e ative.



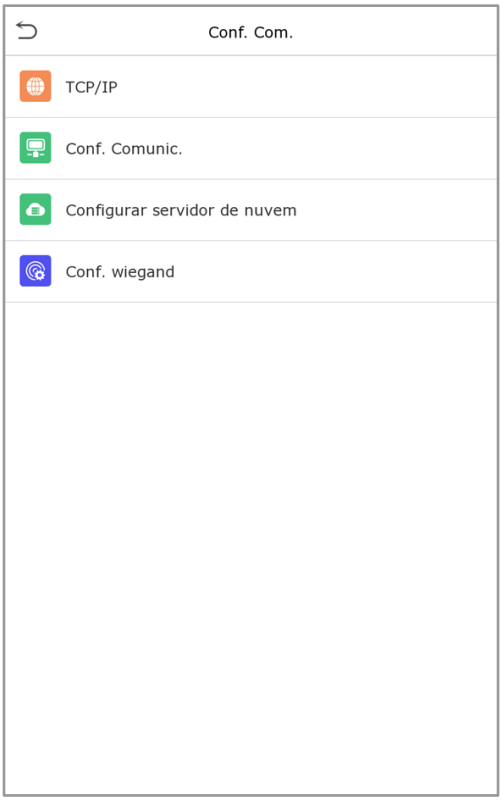
2. Clique em **Atribuir permissões** para atribuir os privilégios ao usuário, a ação será concluída e após a operação clique em **Voltar**.

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.

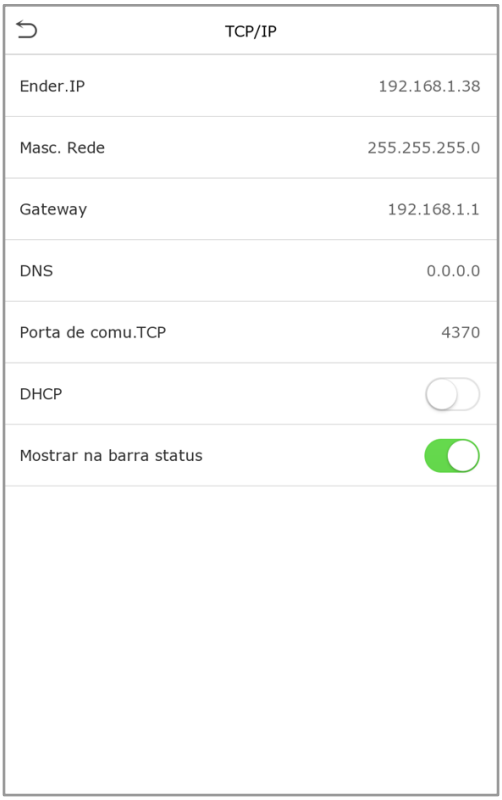
6. Configurações de rede

As configurações de rede são usadas para definir os parâmetros da Rede, conexão de PC, servidor de nuvens, e *Wiegand*. Acesse **Conf. Com.** no menu principal.



6.1 Rede

Para que o **ProFace X [TI]** seja conectado com um PC através da *Ethernet* é necessário configurar a rede e garantir que os dois equipamentos estejam conectados ao mesmo segmento de rede. Acesse o item *Ethernet* em **Conf. Com.** e confira a seguinte página:



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 da 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 com a situação da 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*.

6.2 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.

Acesse o item 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*.

6.3 Rede sem fio

É usado para conexão de rede, transmissão de dados sem fio e comunicação.

O *Wi-Fi* está habilitado no dispositivo por padrão. Ative o botão para ativar ou desativar o *Wi-Fi*. Quando o *Wi-Fi* está habilitado, toque na rede necessária na lista de redes pesquisadas.

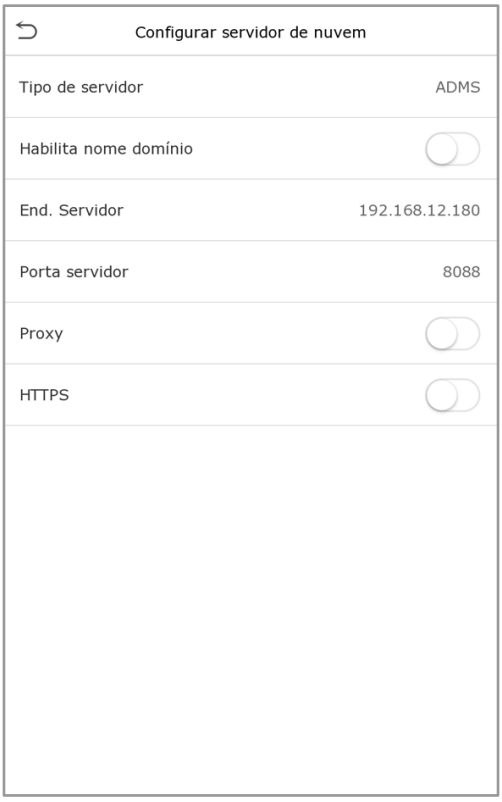
- ***Wi-Fi* habilitado:** Acesse a rede necessária na lista de pesquisa de rede, insira a senha para inserir a senha e, em seguida, toque em **[Conectar]** ao *Wi-Fi* **[OK]**.
- **Adicionar rede Wi-Fi manualmente:** Acesse em **Adicionar rede *Wi-Fi*** para adicionar o *Wi-Fi* manualmente. Nesta tela, insira os parâmetros da rede *Wi-Fi*.

Depois de adicionada, encontre a rede *Wi-Fi* adicionada na lista e conecte-se à rede seguindo o mesmo procedimento.

Item	Descrição
DHCP	Configuração de host dinâmico é utilizada para ajustar dinamicamente os endereços de IP para clientes via servidor;
Endereço de IP	O endereço IP da rede *Wi-Fi*;
Máscara de sub-rede	A máscara de sub-rede da rede *Wi-Fi*;
Gateway	Porta de entrada.

6.4 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.

6.5 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, podendo 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 o número do crachá.

- **Definições de formatos *Wiegand* comuns:**

Formato *Wiegand*	Definições
Wiegand26	ECCCCCCCCCCCCCCCCCCCCCCCCO 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 ao 25º *bits* são os números dos cartões;
Wiegand26a	ESSSSSSSSCCCCCCCCCCCCCCCCO 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 ao 9º *bits* são do código do site, já do 10º a 25º *bits* são os números dos cartões;
Wiegand34	ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO 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;

Wiegand34a	ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO 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 ao 9º *bits* são do código do site, já do 10º ao 25º são os números de cartões;
Wiegand36	OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME 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 *facility code*, do 18º aos 33º *bits* são os números dos cartões e os 34º aos 35º *bits* são os códigos do fabricante;
Wiegand36a	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 ao 19º *bits* são os *facility code* e os 20º ao 35º são números de cartões;
Wiegand37	OMMMMSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE 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;
Wiegand37a	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 *facility code*, os 15º aos 20º *bits* são do *site code* e do 21º aos 36º bits são os números dos cartões;
Wiegand50	ESSSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO São 50 *bits* de código binário, sendo o 1º responsável pela paridade par do 2º ao 25º, o 50º é o *bit* de paridade ímpar do 26º aos 49º, do 2º aos 17º *bits* são *site codes* e do 18º ao 49º são números dos cartões;

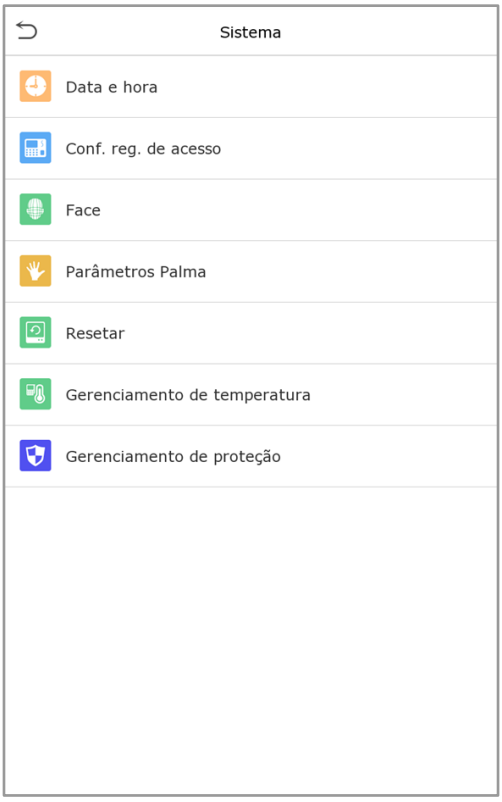
- **C** denota o número do cartão;
- **E** é o *bit* de paridade par;
- **O** é o *bit* de paridade ímpar;
- **F** é o *facility code*;
- **M** é o código do fabricante;
- **P** é o *bit* de paridade;
- **S** é o *site code*.

- **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 site code 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.

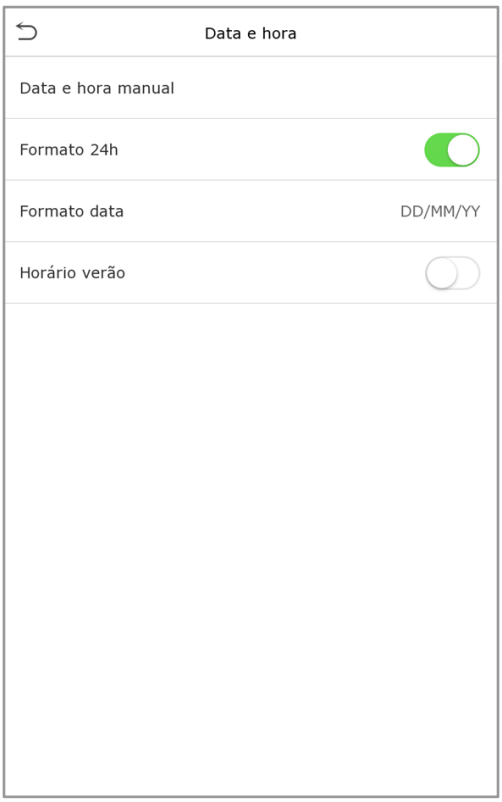
7. Configurações de sistema

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



7.1 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 **ProFace X [TI]** em 18h30 em 1 de janeiro de 2020, após a restauração das configurações de fábrica a hora do aparelho seguirá às 18h30 de 1/1/2020.

7.2 Configurações de acesso

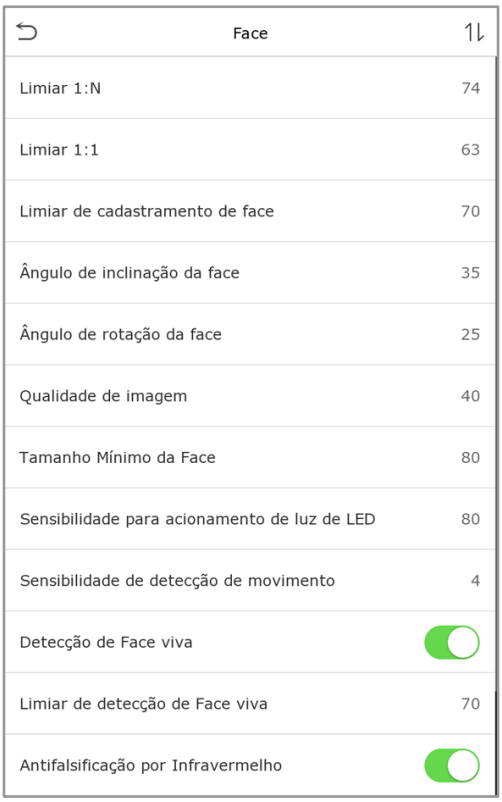
Clique em **Sistema** > **Conf. Reg. de acesso** para configurar a seguinte página:

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	A foto do usuário verificado será exibida;
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.

7.3 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 face	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 face e os modelos faciais que já registrados for superior a este parâmetro, conclui-se que o face já foi registrado antes;
Ângulo de tolerância para inclinação	Nível de tolerância do ângulo de inclinação do face 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 face	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, mas 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 face. Esse valor poderá ser entendido como a distância de comparação facial, quanto mais distante estiver a pessoa, menor estará seu face 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 faces mais distantes. Quando o valor fixado for zero a distância de comparação dos faces 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 *Wide Dynamic 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 faces	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 **ZKTeco**, ajustes inadequados podem afetar gravemente o desempenho do aparelho.

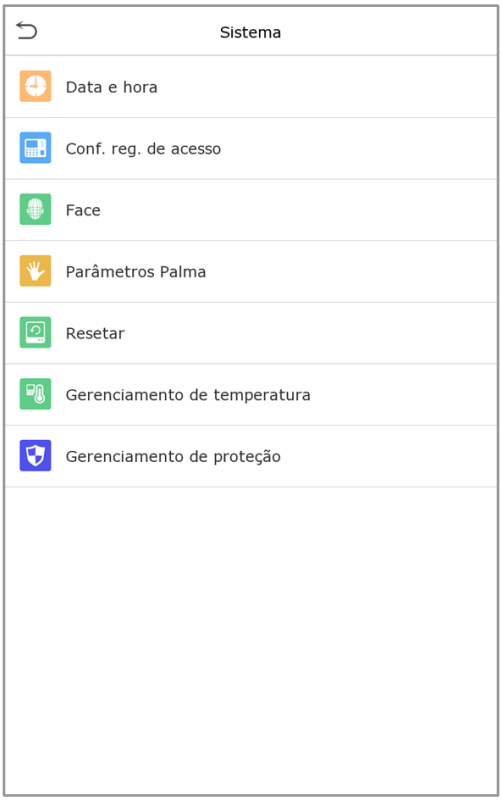
7.4 Parâmetros de palma

Clique em **Palma** no **ProFace X [TI]**. Confira:

Item	Descrição
Limite de correspondência Palma 1: 1	No Método de Verificação 1: 1, somente quando a similaridade entre a palma de verificação e a palma registrada do usuário é maior que este valor a verificação pode ter sucesso;
Limite de correspondência Palma 1: N	No Método de Verificação 1: N, somente quando a similaridade entre a palma verificadora e toda a palma registrada é maior que este valor a verificação é bem-sucedida.

7.5 Resetando o dispositivo

Para restaurar as definições de fábrica do dispositivo sem apagar os dados registrados pelos usuários, clique em Resetar no sistema do **ProFace X [TI]**, conforme a imagem abaixo:



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

7.6 Gestão de temperatura

O **ProFace X [TI]** possui um sensor de temperatura embutido e quando a temperatura ambiente estiver muito baixa ou muito alta, ele irá desligar.

Clique em **Gestão de temperatura** na tela do sistema.

Item	Descrição
Temperatura atual do dispositivo	Esta coluna mostra a temperatura em tempo real do dispositivo;
Baixa temperatura/aquecer	Assim que a temperatura do dispositivo for inferior ao valor definido, o dispositivo iniciará o autoaquecimento, a faixa é de 0 a 10 (° C);
Alta temperatura/reiniciar	Quando a temperatura do dispositivo for superior ao valor definido, ele desligará automaticamente para proteger o *hardware*, a faixa é de 30° a 60° C.

7.7 Gestão de Detecção

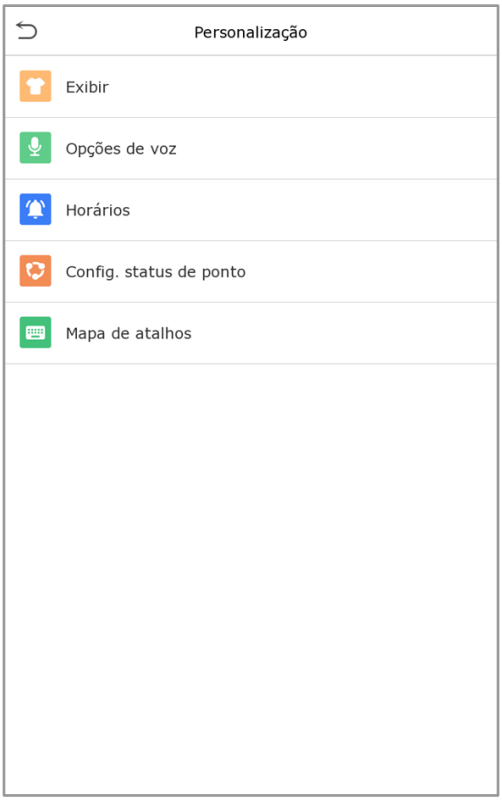
Acesse **Gerenciamento de detecção** na interface do sistema.

Item	Descrição
Ativar medição de temperatura com infravermelho	Para ativar ou desativar a função de medição de temperatura por infravermelho. Quando esta função é habilitada, antes do acesso concedido, o usuário deve passar pela triagem de temperatura além da verificação de identidade. Para medir a temperatura corporal, os rostos dos usuários devem estar alinhados com a área de detecção de temperatura.
Limite de alarme de alta temperatura	Configurar o valor do limite de alarme de alta temperatura corporal. Quando a temperatura detectada durante a verificação for superior ao valor definido, o dispositivo dará um aviso e um alarme sonoro. O limite de alarme padrão é 37,30 ° C;
Temperatura acima da faixa/ acesso negado	Quando ativado, se a temperatura corporal detectada pelo usuário estiver acima (ou abaixo) do limite do alarme, o usuário não terá acesso, mesmo que sua identidade seja verificada. Caso esteja desabilitado, o usuário tem permissão para acessar a área restrita quando sua identidade for verificada, independentemente de sua temperatura corporal;
Correção de desvio de temperatura	Como o módulo de medição de temperatura permite uma pequena faixa de erros (perturbação) de um valor observado em diferentes ambientes (umidade, temperatura ambiente e outros), os usuários podem definir o valor de desvio aqui;
Temp. Unidade	A unidade de temperatura corporal pode ser alternada entre Celsius (° C) e Fahrenheit (° F).
Distância de medição de temperatura	Ao detectar a temperatura durante o processo de verificação, existem três modos: **Perto, Fechar e Longe**.

Exibir figura termodinâmica	Para habilitar ou desabilitar a função da figura termodinâmica do display. Quando ativado, durante o processo de detecção, a imagem térmica da pessoa será exibida no canto superior esquerdo do dispositivo;
Exibir temperatura corporal	Para ativar ou desativar a função de exibição de temperatura corporal. Quando habilitado, o dispositivo exibirá o valor de temperatura específico do usuário durante o processo de verificação;
Habilitar detecção de máscara	Para ativar ou desativar a função de detecção de máscara. Quando ativado, o dispositivo identificará se o usuário está usando uma máscara ou não durante a verificação;
Permitir o acesso de pessoas não registradas	Para habilitar ou desabilitar as pessoas não registradas para acessar a função. Quando ativado, o dispositivo permite que a pessoa entre sem registro;
Permitir captura de pessoa não registrada	Para habilitar ou desabilitar a captura de função de pessoa não registrada. Quando ativado, o dispositivo irá capturar automaticamente a foto da pessoa não registrada, a ativação deste recurso requer permitir que pessoas não registradas acessem;
Acionar alarme externo	Quando ativada, se a temperatura do usuário for superior ao valor definido ou a detecção da máscara estiver ativada, mas a máscara não estiver sendo usada, ela acionará um alarme;
Limpar alarme externo	Limpe os registros de alarme disparado do dispositivo;
Atraso (s) de alarme externo	O (s) tempo (s) de atraso para acionar um alarme externo pode ser definido em segundos, os usuários podem desabilitar a função ou definir um valor válido entre 1 e 255;
Atualização de *firmware*	Escolha se deseja atualizar a versão do *software* do módulo de detecção de temperatura de imagem térmica.

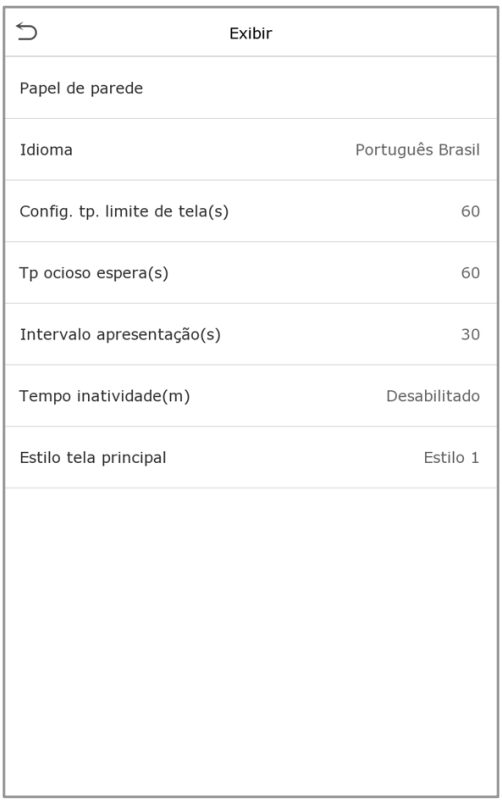
8. Personalização configurações

É possível personalizar as configurações de tela, áudio e alarmes do **ProFace X [TI]**. Acesse Personalização no menu principal, conforme a imagem abaixo:



8.1 Configurações de interface

Clique em **Exibir** 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 o 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.

8.2 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.

8.3 Alarmes

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

- **Adicionando um alarme**

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

Item	Descrição
Status do alarme	Aqui é possível alterar o status dos alarmes;
Horário do alarme	Defina o 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.

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

Editar alarme

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

Apagar alarme

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

8.4 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, que pode ser: • **Desligado:** Para desativar a função da tecla status de ponto. A chave de estado do ponto definida no menu Mapa de atalhos de atalho 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:** Neste 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.

8.5 Mapeamento de teclas de atalho

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:

9. Gerenciar dados

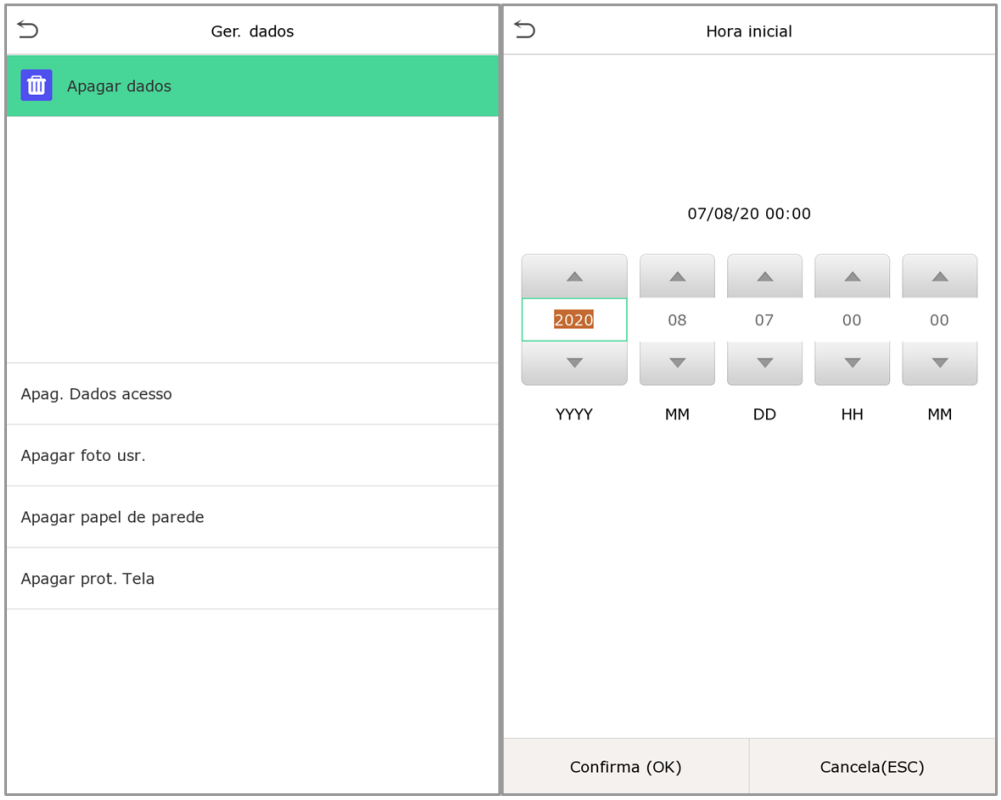
Para alterar os dados do **ProFace X [TI]** clique em **Ger. dados** no menu principal.

9.1 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 todas 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.

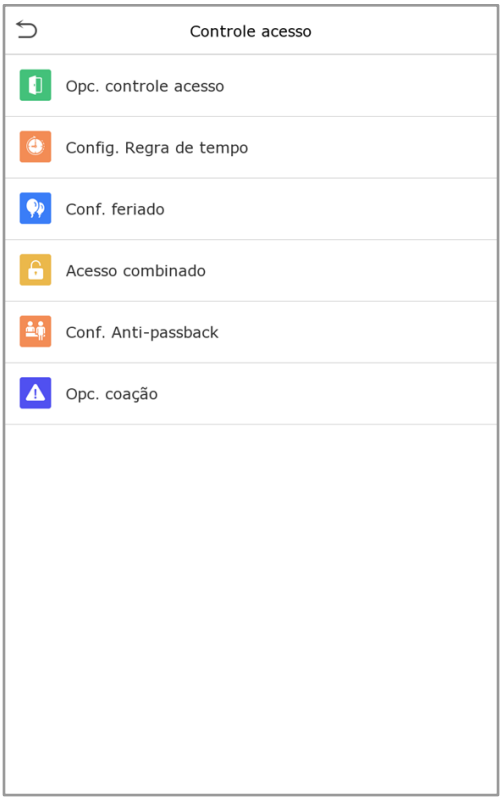
Importante: Em caso de exclusão dos registros de acesso, fotos de presença ou fotos da lista de bloqueio, você poderá selecionar **Apagar tudo** ou **Apagar por período**, onde existe a possibilidade de determinar os dados que deseja excluir por um intervalo de tempo.



1. Selecione **Apagar período** e clique [**OK**].
2. Defina o período a ser excluído e clique em [**OK**].

10. 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 aos seguintes requisitos:

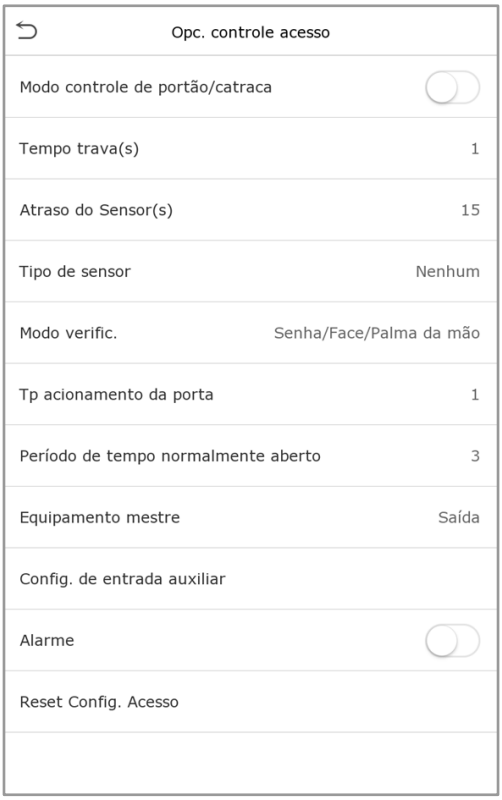
1. A faixa de horário para abertura da porta, deve estar dentro de qualquer faixa horária válida na regra de acesso do usuário.

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).

Nas configurações padrão, novos usuários são alocados no primeiro grupo com o fuso horário padrão e combinação de acesso como "1".

10.1 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 **ProFace X [TI]** 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 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;
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;

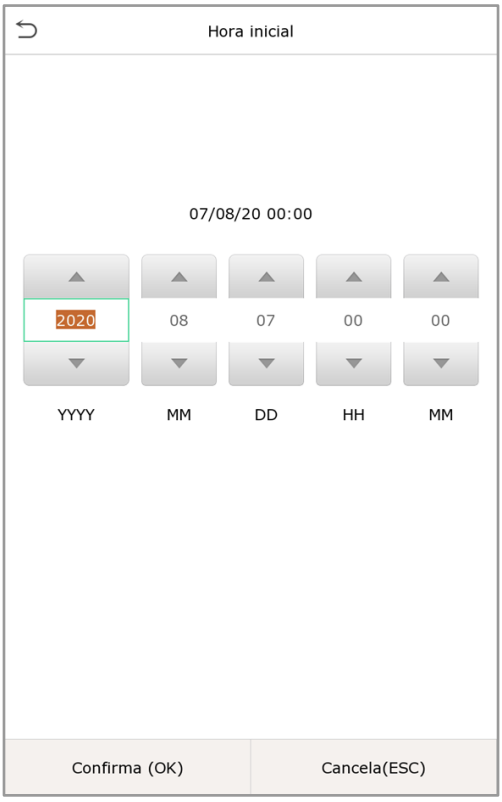
Tempo disponível na porta	Aqui é possível definir o período de disponibilidade da porta;
Aberta em tempo normal	Tempo programado para o modo **Normalmente Aberto** para que a porta esteja destrancada;
Dispositivo mestre	Quando configurar os dispositivos mestre e auxiliar, somente o mestre poderá definir 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.

10.2 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 23:57 a 23:56, indica que o acesso é proibido durante o dia. Já quando a hora final é posterior à hora inicial, como 00:00 a 23:59, estabelece que o intervalo é válido.
- Os períodos do dia em que o sistema deverá abrir a porta: aberto todos os dias, 00:00 a 23:59, ou quando a hora final for após a inicial, como 08:00 a 23:59.
- A faixa horária padrão 01 indica que a porta estará aberta durante todo o dia.

10.3 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** e clique em **Conf. feriado**.

- **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**.

10.4 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 $0 \leq X \leq 5$, 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.

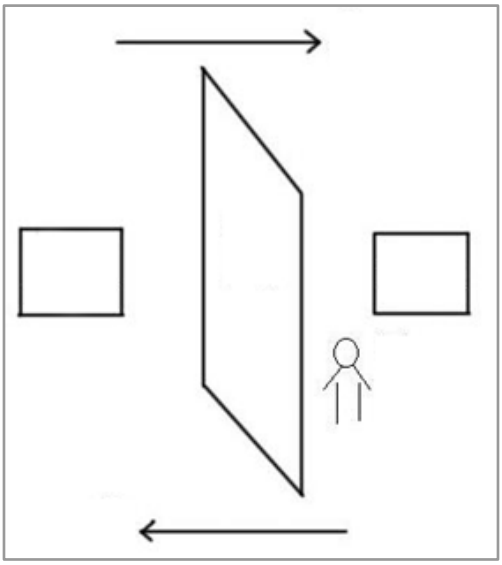
No acesso combinado da porta 2 a definição é 02 02 02 04 04 07, indicando que a combinação do desbloqueio 2 possui cinco pessoas e que os dois primeiros são do grupo 2, os seguintes do grupo 4 e somente o último do grupo 7.

- **Apague um acesso combinado**

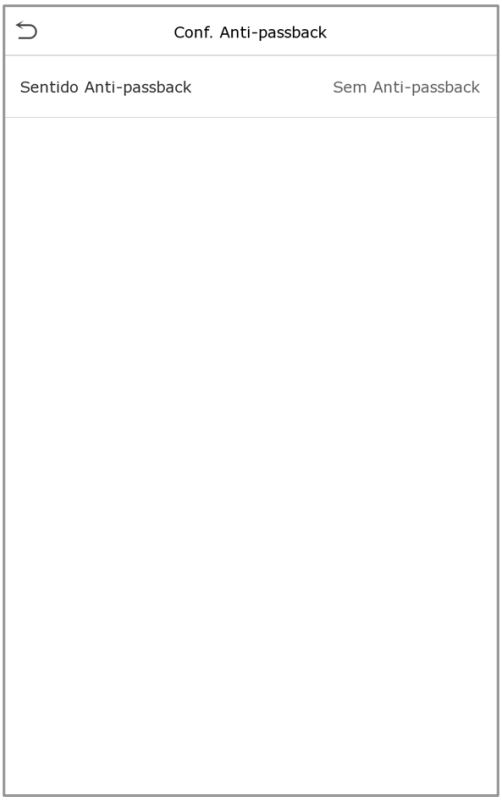
Defina o número do grupo de acesso para zero, assim a combinação será apagada.

10.5 Configurações *anti-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 deverão coincidir com os registros de saída para abrir a porta. Essa função requer dois dispositivos, um é instalado 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 **Conf. *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; • **Saída *anti-passback*:** 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 ativado; • **Entrada e saída com *anti-passback*:** Após a entrada o usuário poderá registrar, somente, sua saída. Caso o contrário seja tentado o alarme será acionado.

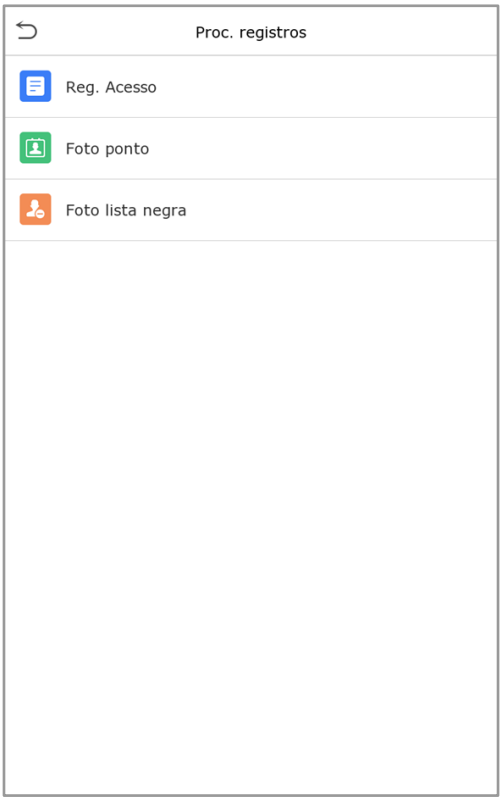
10.6 Configurações de coação

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;
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 digitar o alarme soará.

11. Pesquisa de acessos

Quando a identidade de alguém é verificada este registro fica salvo no **ProFace X [TI]**, 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 à 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.

12. 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 às 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.

13. Informações do sistema

Com a opção de informações do sistema, você pode visualizar o *status* de armazenamento, a versão do dispositivo e as demais informações sobre o dispositivo. Clique em Info Sistema Info no menu principal.

Item	Descrição
Capacidade	Exibe o armazenamento atual do aparelho incluindo os dados de palma da mão, impressão digital, senhas, faces, 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.

14. Conectando o SpeedFace [P] ao *software*

Os softwares **ZKTeco** contam com plataformas leves, seguras e desenvolvidas em ambiente *web*, compatível com a maioria dos *hardwares* **ZKTeco**. Especialmente pensado a linha *Visible Light* sem toque, e para a série de ZKTeco 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.

14.1 Configure o servidor

No aparelho

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 do *software*, de preferência no mesmo segmento de rede e endereço do servidor.

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 do *software*.
- **Porta do servidor:** é definida como a porta de serviço do *software*, seu padrão é 8088.

No *software*

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

14.2 Adicione o dispositivo ao *software*

1. Inicie o processo de busca da seguinte forma para adicionar um dispositivo:
2. Acesse os itens **Controle de acesso** > **Dispositivo** > **Pesquisar**;
3. Clique em **Pesquisar**;
4. Após a busca, será exibida uma lista com o número total de controladores de acesso encontrados;
5. Clique em **Adicionar** e aguarde até que o dispositivo seja inserido.

- **Adicione as pessoas no *software***

1. Clique em **Pessoal** > **Novo**;
2. Preencha todos os parâmetros e clique em [**OK**].

14.3 Monitore o *software* em tempo real

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.

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*.

Apêndice 1

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

- O cadastramento da face deve ser realizado em um ambiente interno, com boa iluminação, sem sub ou superexposição, ou seja, excesso ou falta de luz.
- Não é recomendado que o equipamento esteja voltado para locais de entrada de luz externa, como portas, janelas ou outras fontes de luzes fortes.
- Para facilitar a identificação do usuário, é aconselhável que o cadastro seja feito vestindo uma blusa de cor escura. Assim, o contraste entre a roupa e o ambiente de fundo facilita a identificação do usuário.
- O face deve estar bem exposto no momento do cadastro, sem que a testa e as sobrancelhas estejam cobertas pelos cabelos. Isso é importante para o mapeamento dos pontos da face, o que permite o reconhecimento do usuário.
- O usuário deve estar com a face bem natural. Nunca deve-se fechar os olhos, nem inclinar a cabeça para qualquer direção. Quem utiliza óculos deve registrar duas imagens, ou seja, realizar dois cadastros, sendo um com e outro sem os óculos.
- Durante a pandemia, o uso de máscara de proteção está sendo exigido em todos os ambientes. No entanto, a máscara cobre alguns pontos importantes da face, podendo dificultar o reconhecimento facial. Sendo assim, o cadastro deve ser feito sem a máscara e, caso o equipamento tenha dificuldade em reconhecer o usuário quando ele estiver a utilizando, recomenda-se abaixar um pouco a máscara e fazer nova verificação.
- Mantenha a face posicionada na área de captura, conforme exemplificado na imagem abaixo, e olhe diretamente para a câmera do aparelho.
- O registro deve ser feito individualmente, sem que haja mais pessoas na área de captura.
- A distância recomendada entre o usuário e o aparelho é de 50 a 80cm.

Requisitos para o uso de fotos no cadastro de usuários na linha *Visible Light*

O cadastramento dos usuários pode ser realizado diretamente no equipamento, por meio de upload de fotos ou, ainda, pela captura de uma selfie na opção de autocadastro. Para as duas últimas opções, é necessário que o equipamento esteja conectado a um *software* da **ZKTeco** ou de parceiros.

Para as opções de upload de fotos e captura de selfie, alguns requisitos são necessários para que o reconhecimento seja feito com agilidade e segurança:

- A foto deve ser colorida, apresentar um bom contraste entre o usuário e o cenário de fundo e conter apenas uma pessoa. É importante reforçar que pessoas que utilizam óculos devem ser cadastradas 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: a pessoa deve estar com a expressão natural, portanto recomenda-se não sorrir, fazer careta ou outras expressões faciais.

- Gestos e ângulo da cabeça: a cabeça deve estar reta, direcionada para a câmera. Nunca tire a foto com a cabeça angulada ou fazendo gestos com as mãos próximas ao face.
- Acessórios: as fotos devem ser feitas sem o uso de máscara de proteção ou óculos de sol.
- Face: a foto deve ser feita em local com boa iluminação, ou seja, sem sombra ou superexposição de luz, e com o face totalmente descoberto, ou seja, sem franja ou cabelo cobrindo os olhos e sobrancelhas.
- Formato da foto: as fotos devem ser cadastradas nas extensões BMP, JPG ou JPEG. O método de cor deve ser de 24 bits. A proporção em pixels deve ser 358 x 441 ou 1080 x 1920. A cabeça deve ocupar 2/3 da foto.
- A imagem deve conter os ombros do usuário.

Apêndice 2

Direitos de privacidade

Prezado (a) cliente,

Obrigado por escolher um produto de reconhecimento biométrico projetado e fabricado pela **ZKTeco**. 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 assumimos nenhuma responsabilidade direta ou indireta por quaisquer consequências que possam resultar 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 **ZKTeco** 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 assumimos nenhuma responsabilidade legal

Importante: As leis chinesas incluem as seguintes determinações sobre a Liberdade individual de seus cidadãos:

- Não deve haver prisão, detenção, busca ou violação ilegal das pessoas;
- A dignidade pessoal está diretamente relacionada à liberdade individual e não deve ser violada;
- A residência de nenhum cidadão pode ser violada;
- O direito de todo cidadão a comunicação e confidencialidade 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 período em 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)	*Hexavalent chromium* (Cr6+)	*Polybrominated Biphenyls* (PBB)	*Polybrominated Diphenyl Ethers* (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 deste produto são fabricados utilizando materiais que não são tóxicos e ecologicamente corretos. Os componentes que contêm toxinas ou elementos nocivos são incluídos devido às atuais limitações econômicas ou técnicas que impedem sua substituição por materiais não tóxicos.

Este produto pode conter um ou mais módulos listados abaixo, de acordo com o modelo adquirido por você.

ANATEL 01094-23-12720

Módulo: IC11
"Incorpora produto homologado pela ANATEL sob número 01094-23-12720"

ANATEL 07935-23-12720

Módulo: MTR11
"Incorpora produto homologado pela ANATEL sob número 07935-23-12720"

ANATEL 07937-23-12720

Módulo: MTR10
"Incorpora produto homologado pela ANATEL sob número 07937-23-12720"

ANATEL 12509-20-12720

Módulo: IC01 (M330-L_V3.4)
"Incorpora produto homologado pela ANATEL sob número 12509-20-12720"

ANATEL 14815-21-12720

Módulo: EM05 (V2.01)
"Incorpora produto homologado pela ANATEL sob número 14815-21-12720"

ANATEL 11891-22-11470

Módulo: L287B-SR
"Incorpora produto homologado pela ANATEL sob número 11891-22-11470"

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.