Manual do Usuário

TERMINAL DE RECONHECIMENTO FACIAL ACESSUS 3000 F

Parabéns,
Você acaba de adquirir um produto com a qualidade JFL Alarmes, produzido no Brasil com a mais alta tecnologia de fabricação. Este manual mostra todas as funções do equipamento.

Índice

1 Produto....4
2 Especificações Técnicas....5
3 Instalação....6
3.1 Parte externa....6
3.2 Escolha do local de instalação....7
3.3 Instalação caixa 4x2....7
3.4 Montagem no suporte de base....10
3.5 Fiação....11
3.5.1 Descrição da fiação....11
3.6 Diagrama de ligação da fiação....13
4 Ativação....14
4.1 Ativação via produto....14
4.2 Ativação via SADP....15
4.3 Ativação via Navegador Web....16
5 Operação inicial....17
6 Operação....18
6.1 Login por Administrador....18
6.2 Usuário....19
6.2.1 Adicionar usuário....19
6.3 Acesso....21
6.3.1 Configurações de Autenticação....21
6.4 Presença na plataforma....22
6.4.1 Desabilitado....22
6.4.2 Manual....22
6.4.3 Automático....22
6.4.4 Manual e automático....23
6.5 Comunicação....24
6.5.1 Rede com Fio....24
6.5.2 Wi-Fi....24
6.5.3 RS-485....25
6.5.4 Wiegand....25
6.6 Configuração básica....26
6.7 Biometria....27
6.8 Dados....29
6.9 Sistema....30
7 Precauções....31
8 Regulamentação e informações legais....32
8.1 Direitos autorais....32
8.2 Política de atualização de software....32
8.3 LGPD – lei geral de proteção de dados....32
8.4 Marcas registradas e código aberto....33
9 Certificação anatel....34

1 PRODUTO

O sistema de controle de acesso facial, Acessus 3000 F, tem o objetivo de conceder a entrada e/ou saída de uma área de segurança controlada e negar tal entrada e/ou saída a indivíduos não autorizados. Tais como condomínios, aeroportos, campus universitários, empresas e residências, etc.
O Acessus 3000 F contém a tecnologia reconhecimento facial e de RFID (Identificação por Rádio Frequência), na frequência de 13,56 MHz e trabalha com a tecnologia Mifare (de acordo com a ISO 14443A).

2 ESPECIFICAÇÕES TÉCNICAS

- Tela de toque LCD de 4,3 polegadas;
- Lente dupla grande angular de 2 MP;
- Distância de reconhecimento facial: 0,3 m a 1,5 m;
- Face anti-spoofing;
- Suporte remoto a visualização ao vivo;
- Incorporado com sensor de imagem de luz estelar. O efeito de reconhecimento facial não será afetado em ambiente de luz fraca ou sem luz de suplemento branco;
- Algoritmo de aprendizagem profunda;
- Altura sugerida para reconhecimento facial: entre 1,4 m e 1,9 m;
- Capacidade de 1.500 faces, 3.000 cartões;
- Apenas o dispositivo com módulo de impressão digital periférico suporta a função de impressão digital;
- Vários modos de autenticação;
- Duração do reconhecimento facial ≤ 0,2 s/Usuário; taxa de precisão de reconhecimento facial ≥ 99%;
- O módulo leitor de cartão embutido adota o design de passar o cartão sob a tela para apoiar a identificação do cartão Mifare (cartão IC) em locais com altos níveis de segurança como segurança pública ou local judicial;
- Vários tipos de cartão de autenticação;
- Suporte a detecção de uso de máscara;
- Suporte a vários modos de exibição, incluindo modo normal, modo de anúncio e modo simples;
- Comando de áudio;
- Exibição do resultado da autenticação de suporte;
- Conecta-se à unidade de controle de porta segura via protocolo RS-485 para evitar a abertura da porta quando o terminal é destruído;
- Conecta-se ao controlador de acesso externo ou leitor de cartão Wiegand via protocolo Wiegand;
- Visualização remota ao vivo via protocolo RTSP;
- Modo de codificação: H.264;
- NTP, sincronização de tempo manual e sincronização automática;
- Gerenciamento de parâmetros, pesquisa e configurações do dispositivo;
- Capturar links e salvar imagens capturadas;
- Importar dados para o dispositivo a partir do software cliente;
- Gerencie, pesquise e defina dados do dispositivo depois de fazer login no dispositivo localmente;
- Áudio bidirecional com software cliente, estação de porta, estação interna e estação principal;

3 INSTALAÇÃO

3.1 PARTE EXTERNA

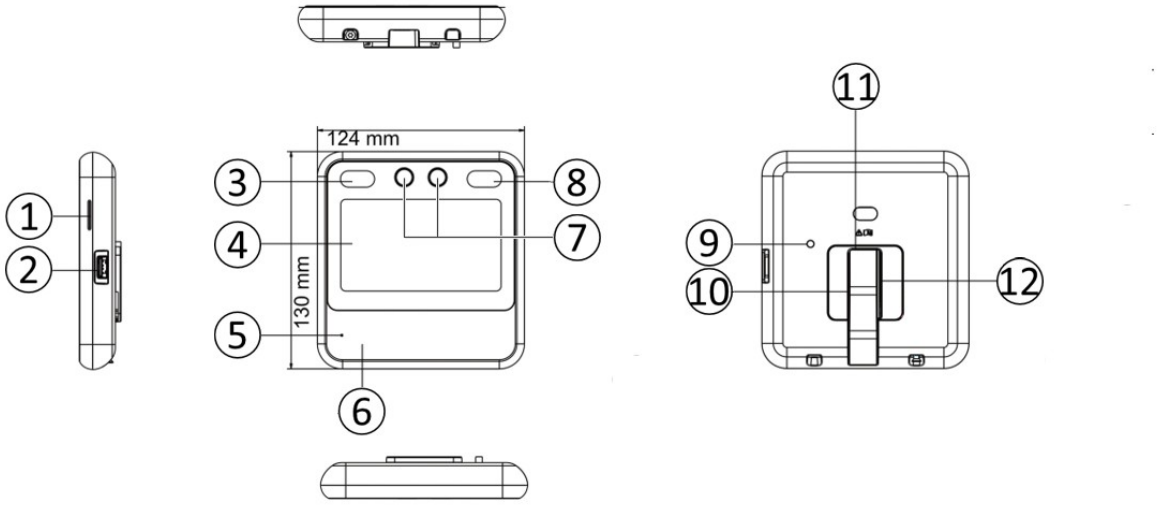

Figura 3.1: Terminal de Reconhecimento Facial Acessus 3000 F

Nº	Nome
1	Alto Falante
2	Interface
3	LED Infravermelho
4	Tela Touch Screen
5	Microfone
6	Leitor de Cartão
7	Camera
8	LED Infravermelho
9	Tamper
10	Terminal de Cabos
11	Interface de Rede
12	Interface reservada

3.2 ESCOLHA DO LOCAL DE INSTALAÇÃO

- Escolha um local que não tenha luz de fundo, luz solar diretamente e indiretamente;
- Par obter o melhor reconhecimento facial, é necessário ter uma fonte de luz no ambiente ou próximo a ele;
- Se for instalado em ambiente externo, deve-se instalar uma proteção para o dispositivo.

NOTA A proteção não acompanha o produto.

3.3 INSTALAÇÃO CAIXA 4X2

Passo:

1. Remova a tampa da caixa 4x2;

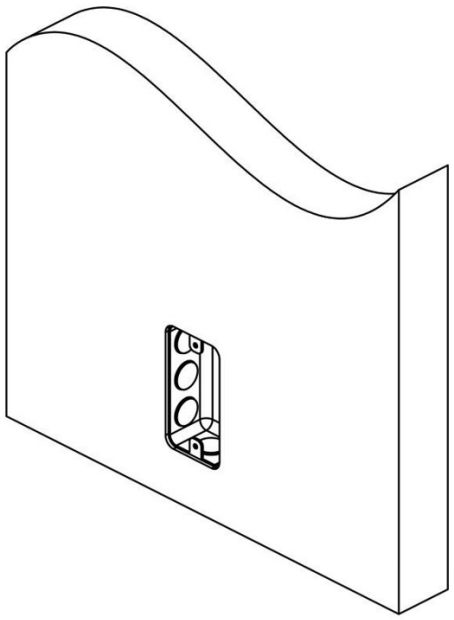

Figura 3.2: Caixa 4x2

2. Fixe a placa de montagem na caixa 4x2;

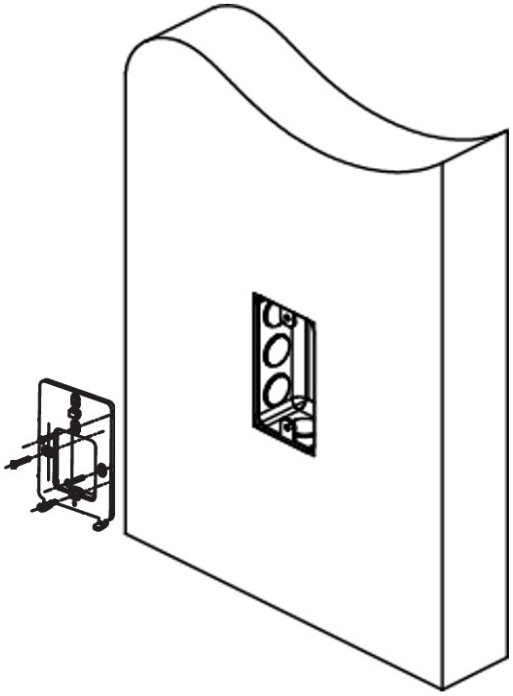

Figura 3.3: Placa de montagem caixa 4x2

3. Encaixe os cabos no produto e encaixe o mesmo na placa de montagem;

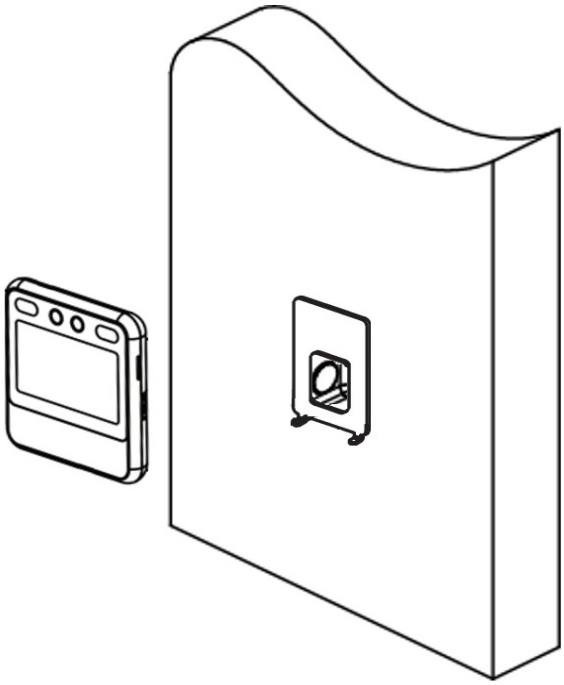

Figura 3.4: Encaixe na placa de montagem

4. **Alinhe o produto com a placa de fixação e fixe o dispositivo com o parafuso;**

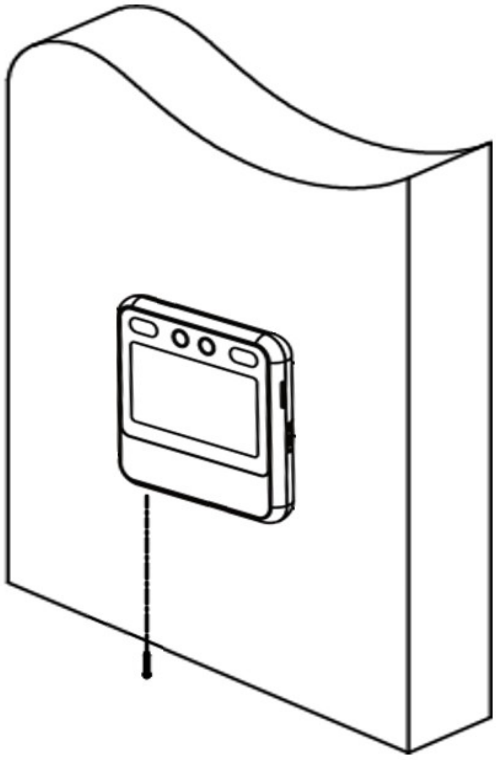

Figura 3.5: Fixação dispositivo

3.4 MONTAGEM NO SUPORTE DE BASE

O suporte de base tem como finalizada a instalação do equipamento em uma plataforma de entrada de locais com controle facial.

Passos:

1. **Passe o cabeamento pelo abertura do suporte e conecte no dispositivo;**

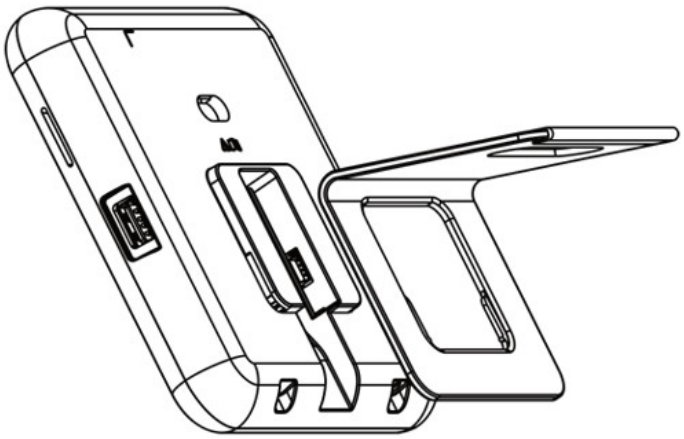

Figura 3.6: Suporte de base

2. **Encaixe o suporte na parte de trás do produto, com as duas mão pressione o suporte e deslize para cima o suporte;**

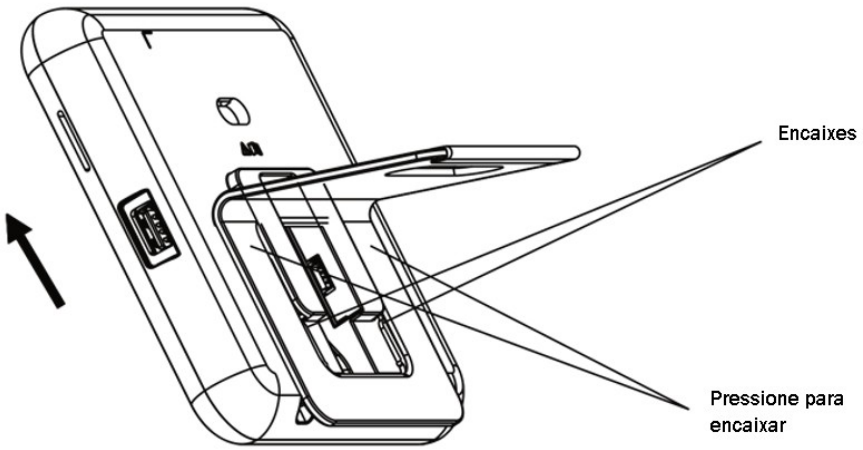

Figura 3.7: Encaixe suporte

3. **Encaixe o suporte até o final para finalizar a instalação.**

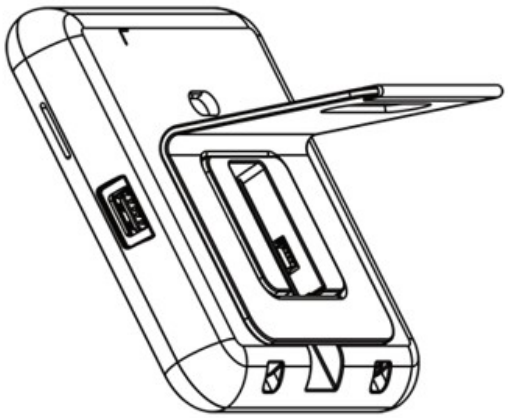

Figura 3.8: Instalação finalizada

3.5 FIAÇÃO

O Acessus 3000 F possui conexão RS-485, trava de porta, botão de saída, leitor de cartão Wiegand, controlador de acesso e fonte de alimentação.

Se conectar o leitor de cartão Wiegand com o controlador de acesso, o terminal de reconhecimento facial pode transmitir as informações de autenticação para o controlador de acesso e o controlador de acesso pode julgar se deve abrir a porta ou não.

3.5.1 DESCRIÇÃO DA FIAÇÃO

Diagrama da fiação:

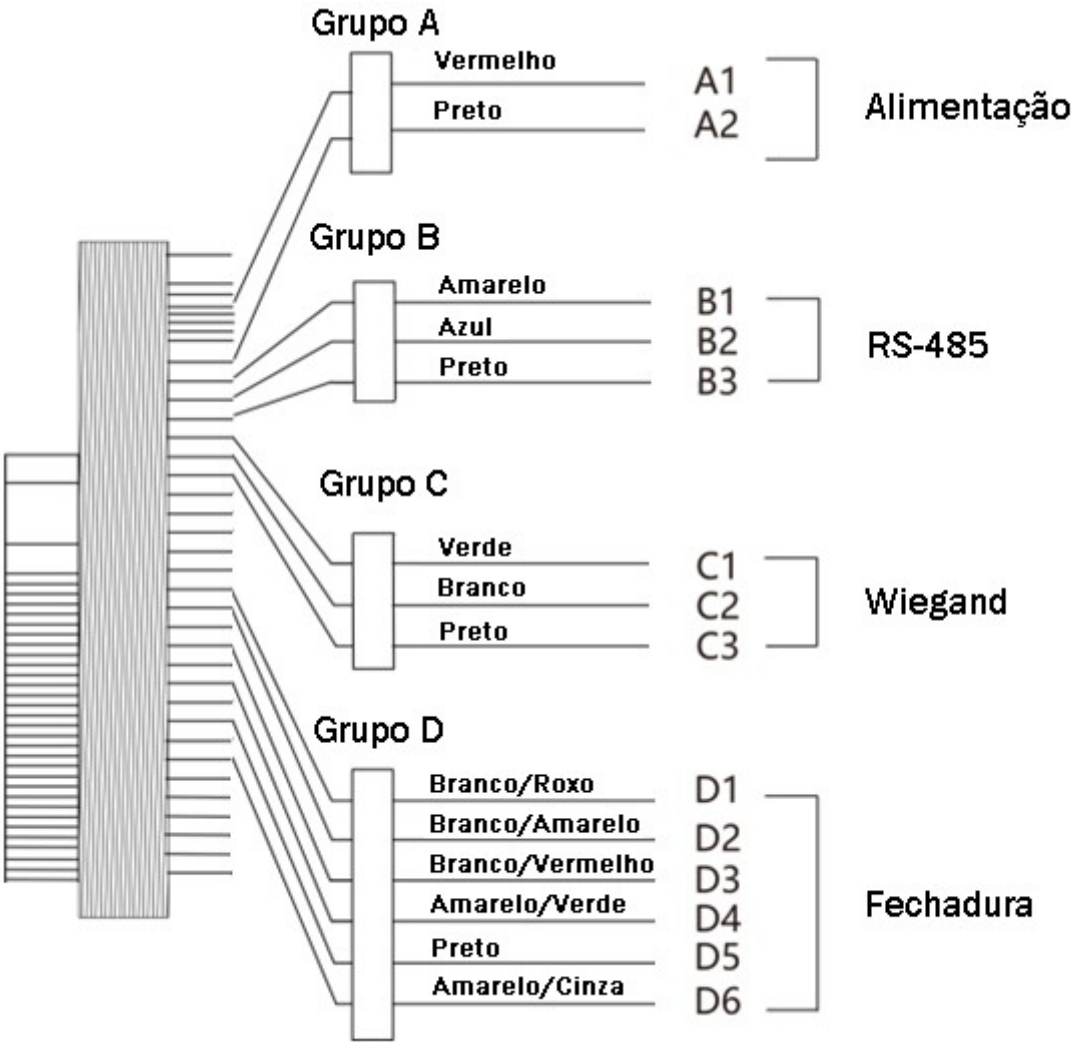

Figura 3.9: Fiação

Tabela 1: Diagrama Fiação

Grupo	N.º	Função	Cor	Nome	Descrição
Grupo A	A1	Alimentação	Vermelho	+12 V	Fonte de alimentação 12 Vd.c.
	A2		Preto	GND	Terra
Grupo b	B1	RS-485	Amarelo	485+	Fiação RS-485
	B2		Azul	485-	
	B3		Preto	GND	Terra
Grupo C	C1	Wiegand	Verde	W0	Wiegand 0
	C2		Branco	W1	Wiegand 1
	C2		Preto	GND	Terra
Grupo D	D1	Fechadura	Branco/Roxo	N.F.	Normalmente Fechado
	D2		Branco/Amarelo	COM	Comum
	D3		Branco/Vermelho	N.A.	Normalmente Aberto
	D4		Amarelo/Verde	SENSOR	Sensor De Porta
	D5		Preto	GND	Terra
	D6		Amarelo/Cinza	BTN	Botão de Saída

3.6 DIAGRAMA DE LIGAÇÃO DA FIAÇÃO

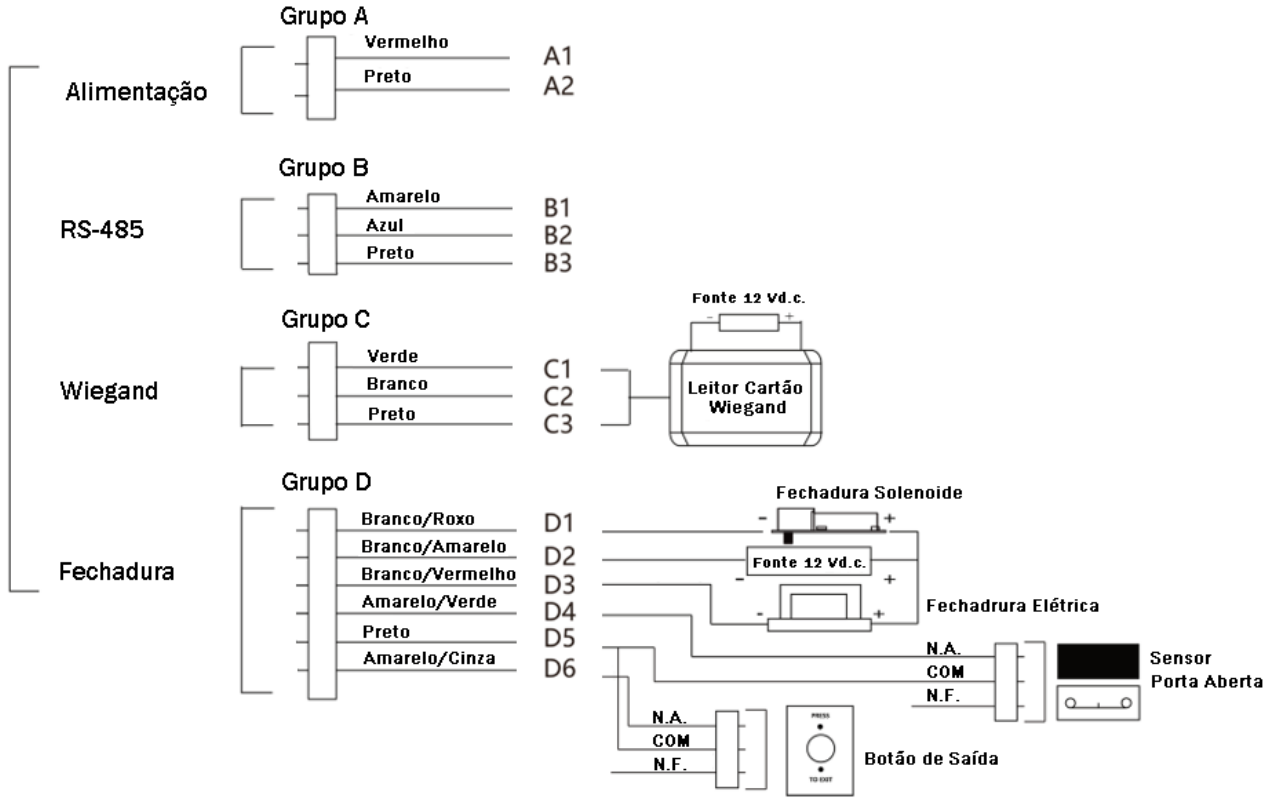

Figura 3.10: Diagrama de ligação fiação

4 ATIVAÇÃO

É necessário realizar a ativação do produto antes do primeiro acesso. Apos ligar o dispositivo, o sistema comutará para a página Ativação.

A ativação pode ser realizada no dispositivo, pelo software SADP e pelo acesso WEB. O dispositivo possui os seguintes valores padrões para acesso WEB:

- Endereço IP: 192.0.0.64;
- Porta Servidor: 8000;
- Usuário padrão: admin.

4.1 ATIVAÇÃO VIA PRODUTO

Ao ligar o produto e o mesmo não estiver ativado. Aparecerá a tela Ativar Dispositivo, crie a senha e confirme a senha. Toque em ATIVAR, com isso o dispositivo é ativado.

Figura 4.1: Ativação

4.2 ATIVAÇÃO VIA SADP

Passo:

1. **Execute o software SADP, caso não possua, o obtenha realizando o download via https://jflalarmes.com.br/softwares-drivers/;**
2. **Encontre e selecione o dispositivo na lista de dispositivos;**
3. **Digite a senha e confirma senha;**

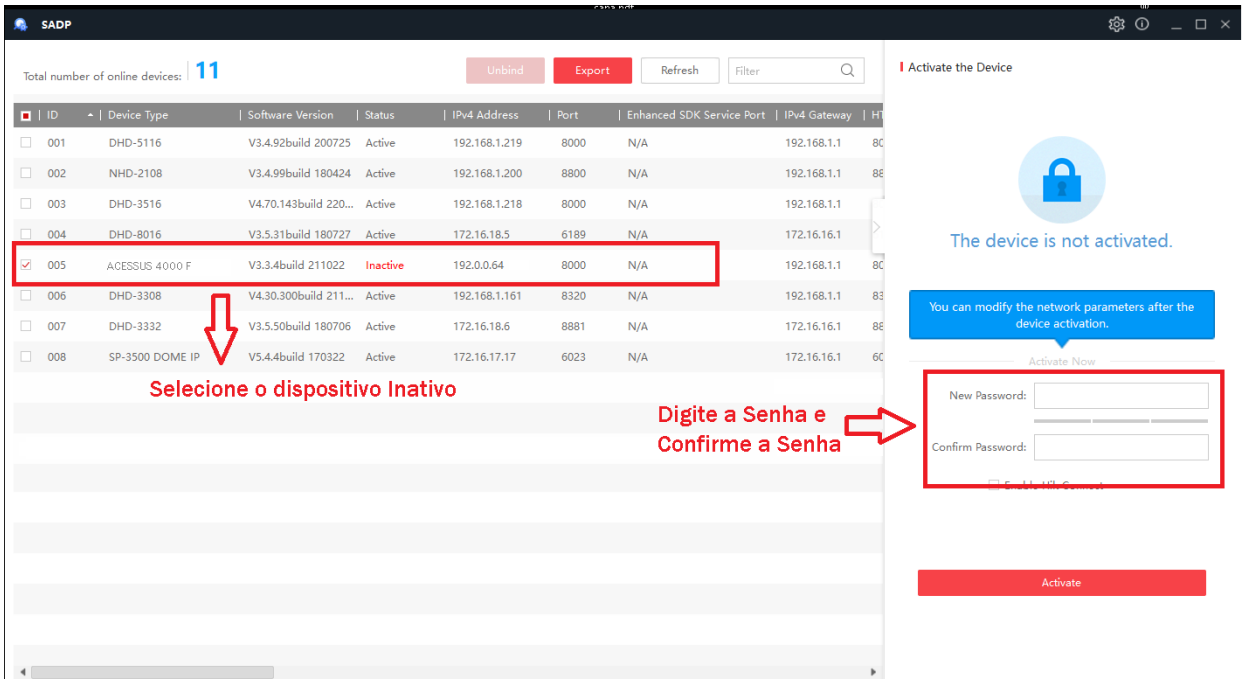

Figura 4.2: Software SADP

4. **Clique em ATIVAR para finalizar o processo de ativação.**

4.3 ATIVAÇÃO VIA NAVEGADOR WEB

Passos:

1. **Abra o navegador, e digite o endereço IP padrão do dispositivo (192.0.0.64);**

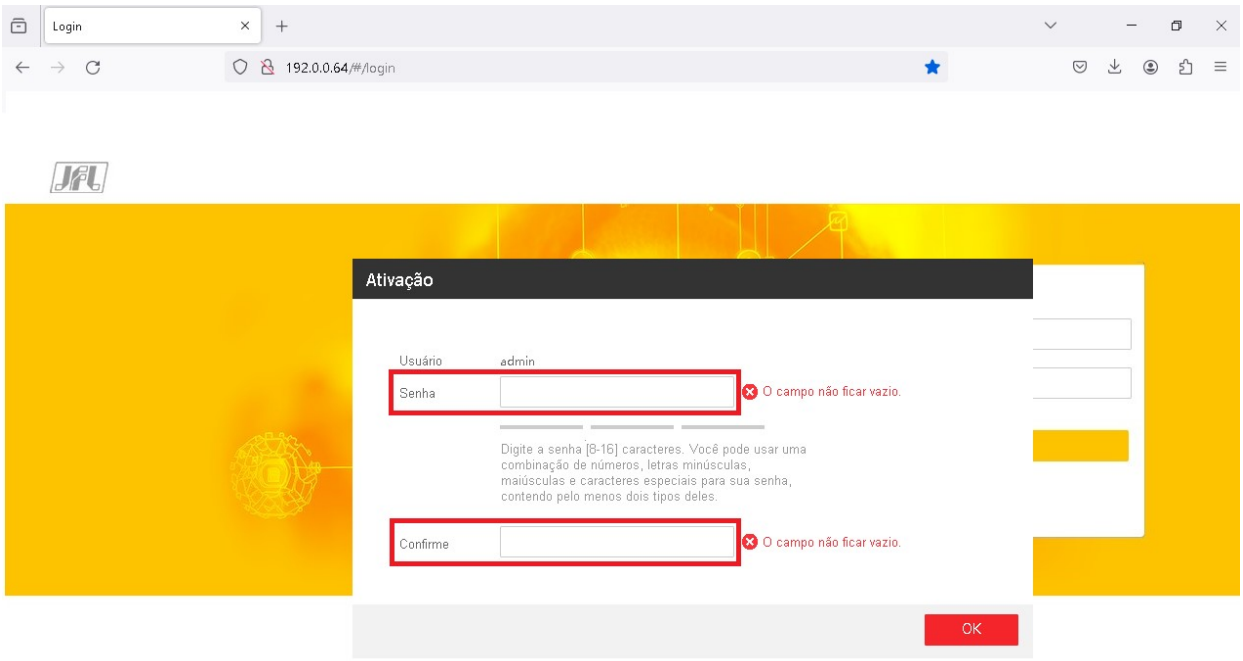

Figura 4.3: Ativação via navegador

2. **Digite e confirme a Senha;**
3. **Clique em OK e a ativação está realizada.**

É necessário o computador estar na mesma faixa de IP do equipamento para realizar a ativação via navegador Web.

5 OPERAÇÃO INICIAL

Apos ativar o dispositivo via produto, algumas configurações devem ser realizadas.

1. Selecione o Idioma, e toque em PRÓXIMO;

Figura 5.1: Idioma

2. Selecione o modo de Privacidade:
   - Carregar foto da autenticação;
   - Salvar foto da autenticação;
   - Salvar foto registrada;
   - Carregar foto após captura vinculada;
   - Salvar foto após captura vinculada.
3. Em seguida toque em PRÓXIMO.

Figura 5.2: Privacidade

6 OPERAÇÃO

6.1 LOGIN POR ADMINISTRADOR

Logue no dispositivo para setar as configurações básicas.

Passos:

1. **Toque na tela por 3 segundos e deslize para a esquerda e direita;**
2. **Autentique o acesso por face, senha ou cartão de usuário com privilégios de Administrador. Para senha toque em ;**

Figura 6.1: Autenticação

3. **Acesse o Menu e configure.**

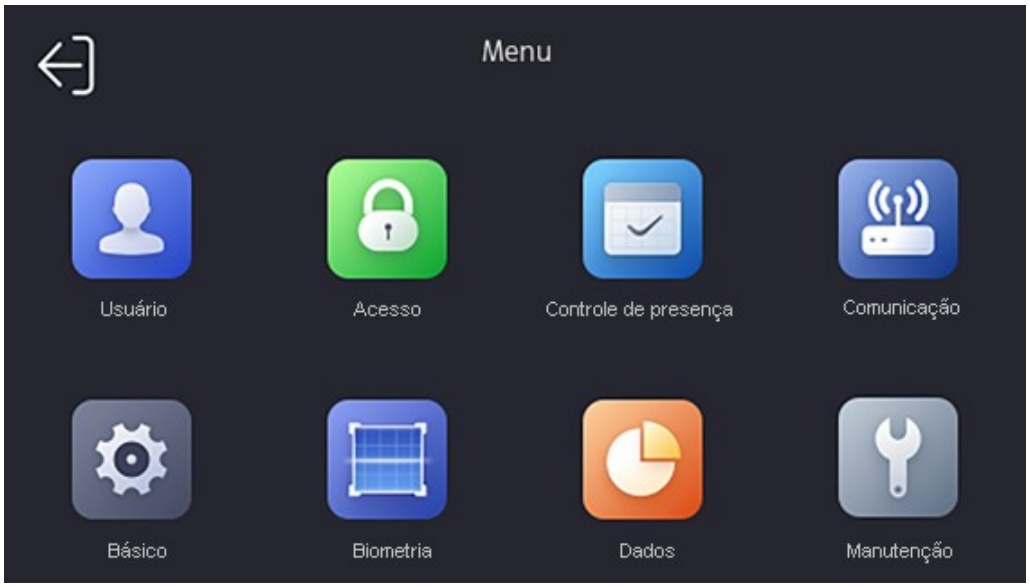

Figura 6.2: Menu

6.2 USUÁRIO

Configure, edite, apague e pesquise um usuário.

6.2.1 ADICIONAR USUÁRIO

Toque em usuário no menu principal, e depois toque +, no canto superior direito, para adicionar usuário.

Figura 6.3: Adicionar usuário

Toque em Nº do funcionário, para editar a identificação do usuário. O campo pode conter 32 caracteres;

Toque em Nome, para editar o Nome do usuário. O campo de Nome do usuário pode conter 128 caracteres;

Toque em Departamento, selecionar o departamento do funcionário;

Opcional toque em Rosto, para adicionar a face do usuário. A janela abaixo será exibida para fotografar o usuário. Posicione a face no centro do círculo indicado. Confirme a foto ou tire outra, caso seja necessário;

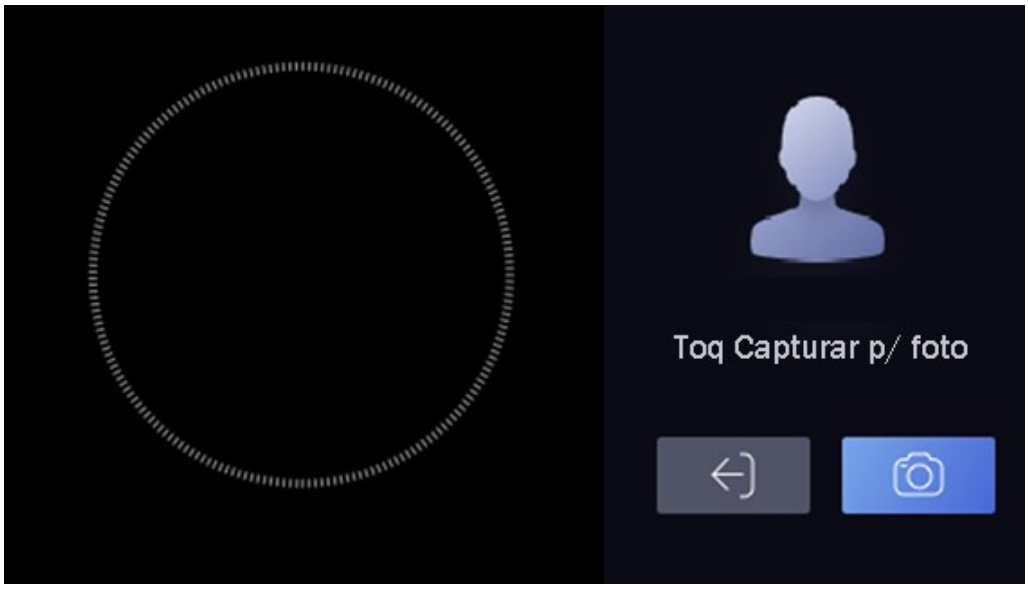

Figura 6.4: Capturar face

Opcional toque em cartão, em seguida toque em +, e na próxima tela aproxime o cartão que deseje adicionar para o usuário, e salve as configurações tocando em ;
Opcional toque em PIN, em seguida digite a senha e confirme a senha, a senha deve conter de 4 a 8 dígitos numéricos. Toque em OK para salvar a senha;
Toquem em Configuração de autenticação, para definir o modo de autenticação. Podendo operar com a configuração do Terminal de Reconhecimento, ou podendo personalizar a autenticação para cada usuário.

Tipo – Credencial exclusiva ou Múltipla;
Credencial exclusica, podendo ser Facial, Cartão ou Senha;
Múltipla, podendo selecionar, mas de uma credencial entre Facial, Cartão e/ou senha.

Toque em Tipo de pessoa, para configurar Administrador ou Usuário normal. Como administrador o usuário pode alterar as configurações do Terminal de Reconhecimento.

6.3 Acesso

Configure o modo de acesso pelo terminal de reconhecimento.

6.3.1 Configurações de Autenticação

Toque em Configurações de autenticação no menu principal, para configurar.

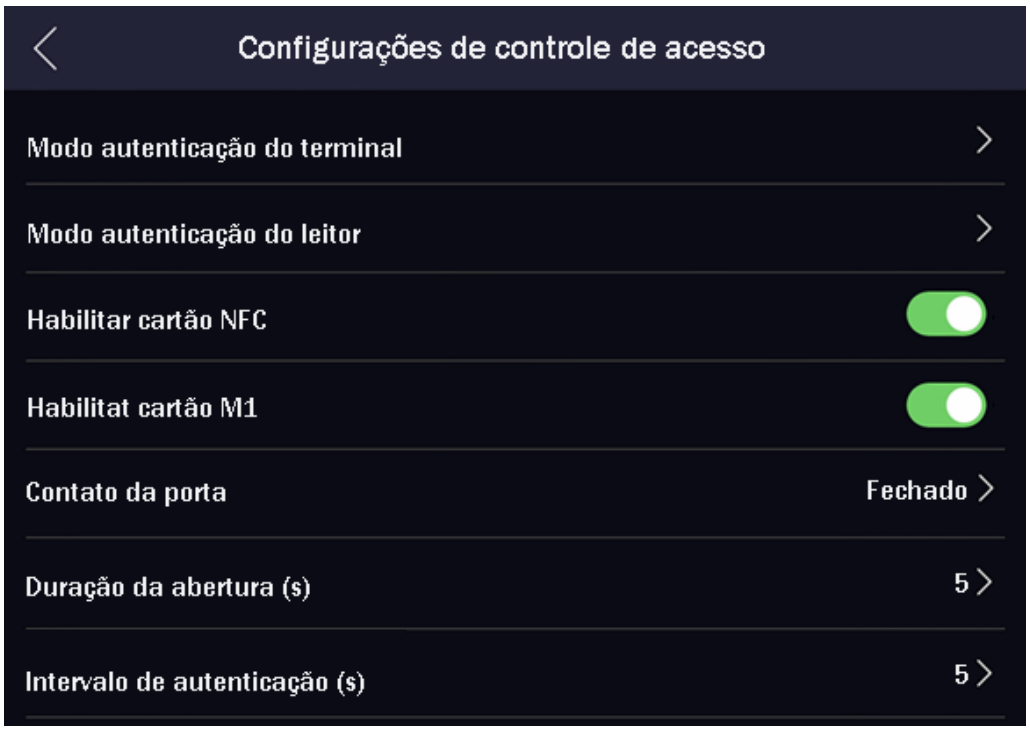

Figura 6.5: Acesso

Toque em Modo autenticação do terminal para configurar o modo de operação de modo geral para todos usuários.

Tipo – Credencial exclusiva ou Múltipla;
Credencial exclusiva, podendo ser Facial, Cartão ou Senha;
Múltipla, podendo selecionar, mais de uma credencial entre Facial, Cartão e/ou Senha.

Toque em Modo autenticação do leitor para configurar o modo de operação do leitor modo geral para todos usuários.

Tipo – Credencial exclusiva ou Múltipla;
Credencial exclusiva, podendo ser Facial, Cartão ou Senha;
Múltipla, podendo selecionar, mais de uma credencial entre Facial, Cartão e/ou Senha.

Toque em Habilitar cartão NFC, para habilitar/desabilitar Cartão NFC;
Toque em Habilitar cartão M1, para habilitar/desabilitar Cartão M1;
Toque em Habilitar Criptografia de cartão M1, para habilitar/desabilitar Criptografia de cartão M1;
Toque em Habilitar Autenticação Remota, para habilitar/desabilitar Autenticação Remota;
Toque em Contato da porta, para configurar o contato com Aberto ou Fechado;
Toque em Duração da abertura para configurar o tempo da abertura em segundos;
Toque em Intervalo de autenticação para configurar o tempo entre autenticações;
Toque em Duração exibição resultado da autenticação para configurar o tempo de exibição;
Toque em Modo de Senha, PIN definido pelo usuário ou PIN definido pelo dispositivo.

6.4 Presença na plataforma

Configure os parâmetros de presença na plataforma.

Toque em Presença na plataforma. Podendo configurar o modo de assistência como Desabilitado, Manual, Automático e, Manual e Automático.

6.4.1 Desabilitado

Nesse modo não é exibido o status de atendimento na tela de autenticação do usuário.

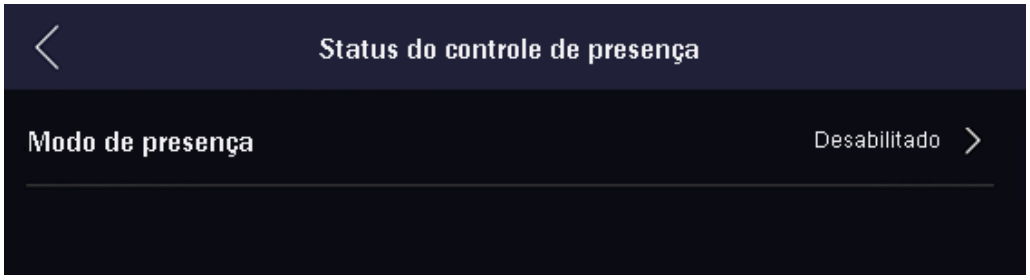

Figura 6.6: Desabilitado

6.4.2 Manual

No modo Manual e com Status de presença requerido, o usuário precisa indicar a ação que está realizando.

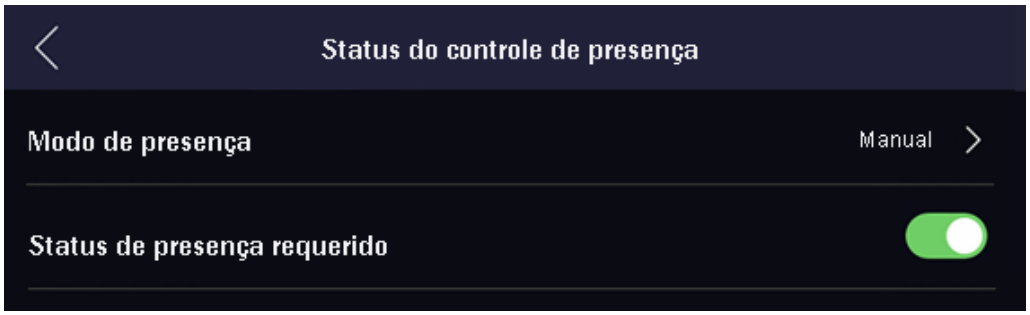

Figura 6.7: Manual

6.4.3 Automático

No modo Automático, são programados os horários de entrada e saída, parada e retorno, e início e fim de hora extra. Com isso se o usuário for autenticado dentro do horário, de maneira automática é registrada a ação automaticamente.

Toque em Entrada/Saída, Parada/Retorno, ou Início/Fim hora extra para configurar horários.

Exemplo: Caso o horário de entrada seja 8:00 e o de saída 11:00, o usuário ao ser autenticado as 8:10 é registrado como entrada, e caso seja autenticado as 11:30 é registrado como saída.

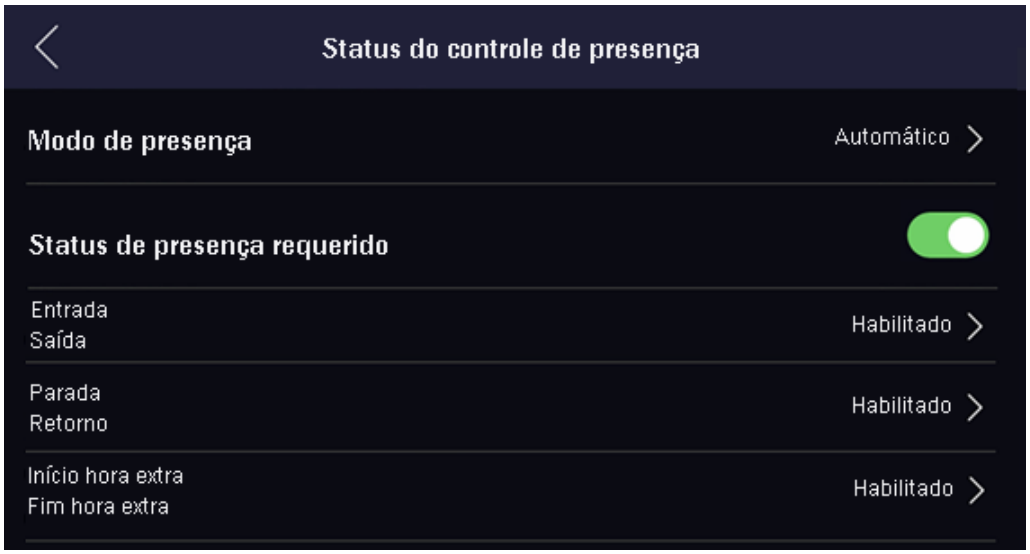

Figura 6.8: Automático

6.4.4 MANUAL E AUTOMÁTICO

No modo Manual e Automático, são programados os horários de entrada e saída, parada e retorno, e início e fim de hora extra. Com isso se o usuário for autenticado dentro do horário, de maneira automática é registrada a ação automaticamente. Caso o usuário seja autenticado em um horário que não exista programação automática, o usuário necessita indicar a ação que está realizando.

Toque em, Entrada/Saída, Parada/Retorno, ou Início/Fim hora extra para configurar os horários.

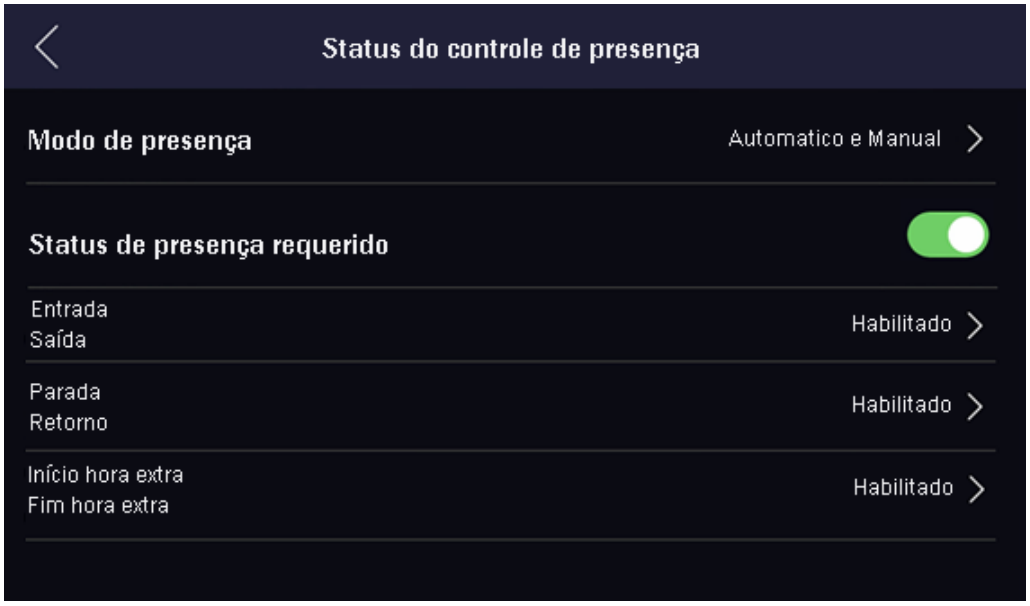

Figura 6.9: Automático e Manual

6.5 Comunicação

Configure os parâmetros referentes as comunicações.
Toque em Configurações do Sistema → Comunicação.

6.5.1 Rede com Fio

Toque em Rede com fio, para configurar os parâmetros de rede IPv4 ou IPv6, incluindo endereço IP, máscara de sub-rede, gateway e DNS.

Figura 6.10: Rede com fio

6.5.2 Wi-Fi

Toque em Wi-Fi, para configurar rede sem fio. Ative a rede Wi-Fi, selecione a rede sem fio e digite a senha.

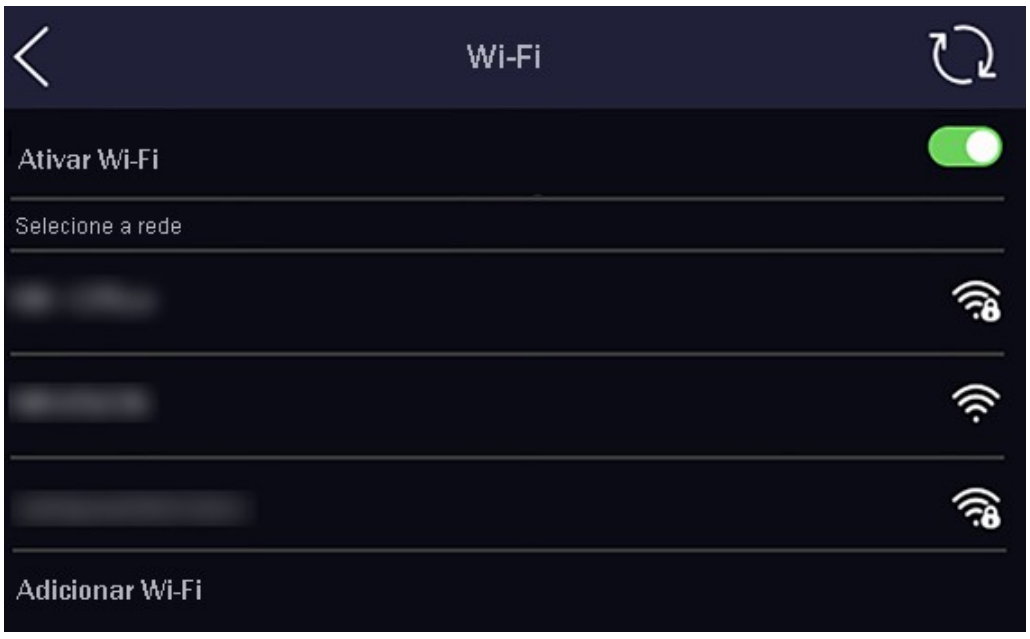

Figura 6.11: Rede sem fio

Caso a rede Wi-Fi não seja exibida, toque em Adicionar Wi-Fi e digite o nome da rede e senha.

6.5.3 RS-485

Toque em RS-485, para configurar o tipo de periférico conectado via RS-485, Controlador de acesso, Unidade de controle de porta segura ou Leitor de cartão.

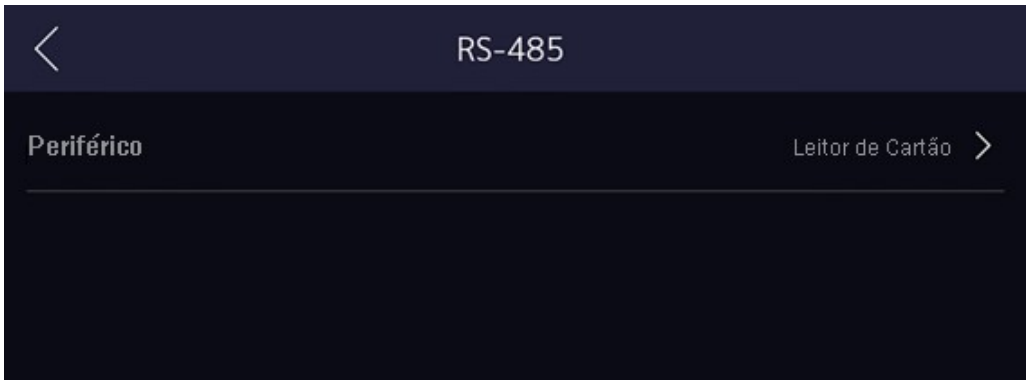

Figura 6.12: RS-485

Se selecionar Controlador de acesso, selecione o endereço conforme o número da porta, se o dispositivo for outro defina o endereço do mesmo como número 2.

6.5.4 Wiegand

Toque em Wiegand, para configurar o Modo de operação do protocolo Wiegand.

Figura 6.13: Wiegand

Na direção Saída, o terminal pode se conectar a um controle de acesso externo, os dispositivos transmitirão o número do cartão via Wiegand 26 ou Wiegand 34.

6.6 CONFIGURAÇÃO BÁSICA

Configure os parâmetros básicos de operação do terminal de reconhecimento.
Toque em Configurações do sistema → Configuração básica. Podendo configurar a Definições de Som, Configurações de hora, Em Suspensão, Selecionar idioma, Nº da comunidade, Nº do prédio e Nº da unidade, Privacidade e Padrão vídeo;

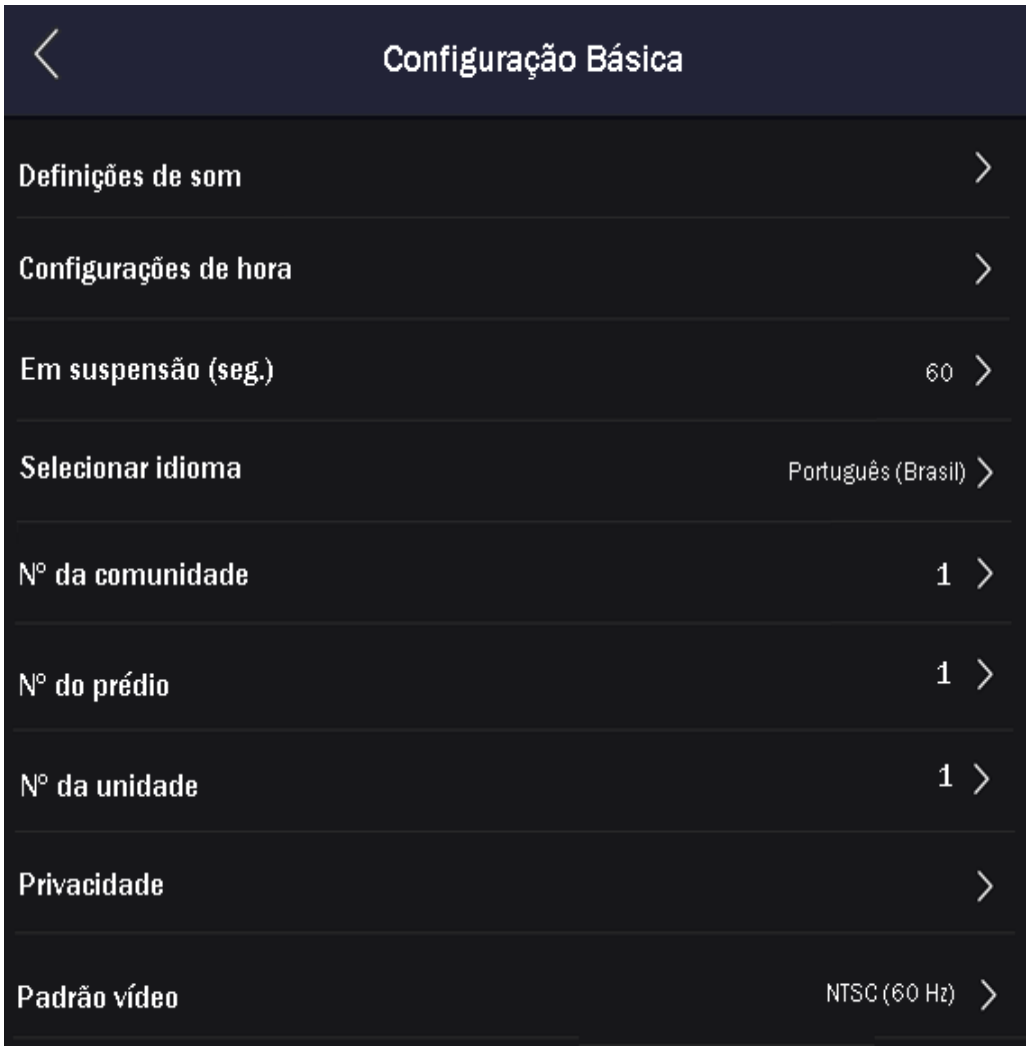

Figura 6.14: Básico

Toque em Definições de som, para configurar Comando de Voz Habilitar/Desabilitar e o Volume da voz com valor entre 0 e 10.
Toque em Configuração da hora, para configurar o Fuso Horário, Hora e Horário de verão.
Toque em Em Suspensão, para configurar a luz branca, com valor entre 0 e 100.
Toque em Selecionar Idioma, para selecionar o idioma de operação do produto.
Toque em Nº da comunidade, com valor entre 1 e 9.
Toque em Nº do prédio, com valor entre 1 e 999.
Toque em Nº da unidade, com valor entre 1 e 99.
Toque em Privacidade, para configurar as opções de privacidade;
Toque em Padrão Vídeo, para selecionar o padrão de vídeo Pal(50 Hz) ou NTSC(60HZ) de operação da câmera.

6.7 BIOMETRIA

Configure os parâmetros de biometria para obter o melhor desempenho do reconhecimento facial.

Toque em Configurações do sistema → Biometria para configurar os seguintes parâmetros, modo de aplicação, nível de vitalidade facial, distância de reconhecimento, intervalo de reconhecimento facial, nível de segurança facial 1:N, nível de segurança facial 1:1, configurações do modo ECO e configurações de máscara.

Figura 6.15: Biometria

Toque em Nível de vitalidade facial, para configurar como Geral ou Avançado.

Toque em Distância de reconhecimento, para configurar a distância para obter o reconhecimento facial entre 0.5, 1, 1.5, 2 ou Automática.

Toque em Intervalo de reconhecimento, para configurar o tempo de entre dois reconhecimentos contínuos, entre 1 e 10 segundos.

Toque em Nível de segurança facial 1:N, para configurar o nível de classificação da imagem capturada a imagens do banco de dados, quanto maior o valor, maior é o grau similaridade exigido.

Toque em Nível de segurança facial 1:1, para configurar o nível de classificação da imagem capturada a identidade única, quanto maior o valor, maior é o grau similaridade exigido.

Toque em Configuração ECO, para configurar o modo ECO. Quando ativado o terminal utilizará Câmera Infravermelho para realizar autenticação em locais com pouca iluminação.

- Toque em Modo ECO, para habilitar/desabilitar a função.
- Toque em Limite modo ECO, para configurar o modo ECO, com valor entre 0 e 7. Quanto maior o valor mais facilmente será acionado o modo ECO.
- Toque em Modo ECO (1:1), para configurar o nível de classificação da imagem capturada a imagens do banco de dados, quanto maior o valor, maior é o grau similaridade exigido.
- Toque em Modo ECO (1:N), para configurar o nível de classificação da imagem capturada a identidade única, quanto maior o valor, maior é o grau similaridade exigido.

Toque em Configurações de máscara, para Habilitar/Desabilitar a detecção e para configurar o nível de classificação 1:N da imagem capturada a identidade única, quanto maior o valor, maior é o grau similaridade exigido.

6.8 DADOS

Toque em Dados, para realizar umas dessas opções excluir, importar e exportar dados.

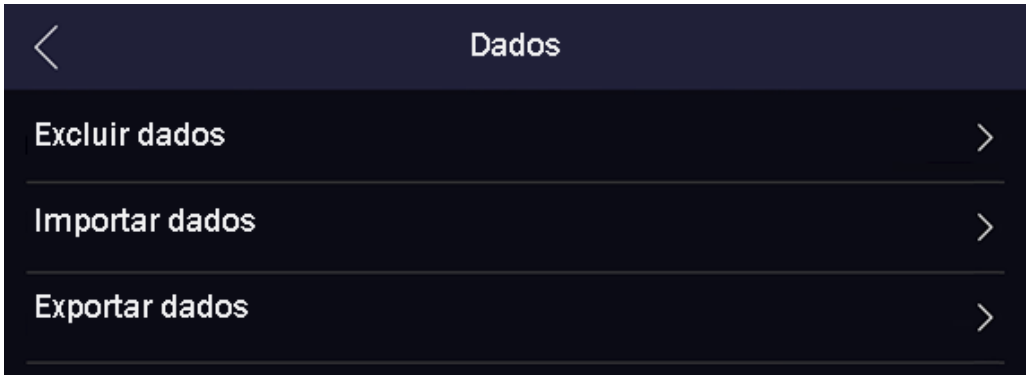

Figura 1: Dados

Toque em Excluir dados, para excluir dados dos usuários.

Toque em Importar dados, para importar dados dos usuários ou dados faciais. Se os dados a serem importados foram exportados com senha é necessário adicionar a senha.

Toque em Exportar dados, para exportar dados dos eventos, dados dos usuários ou dados faciais. Ao exportar é possível adicionar uma senha nos dados exportados.

6.9 SISTEMA

Toque Sistema, para visualizar informação do sistema, atualizar e restaurar o sistema do terminal.

Figura 1: Sistema

Toque em Informação do Sistema, para visualzar Modelo do dispositivo, Número de série, Versão do firmware, Endereço MCU, Endereço MAC, Data de produção, QR Code e Licença de código aberto.
Toque em Capacidade, para visualizar capacidade utilizada em relação a total de Usuários, Faces, Cartões e Eventos.
Toque em Atualização do dispositivo, conecte um pendrive e atualize o dispositivo.
Toque em Restaurar configurações de fábrica, para restaurar todos os dados.
Toque em Restaurar configurações padrão, para restaurar todos os dados, exceto configurações de comunicação.
Toque em Rncr, para reiniciar o dispositivo.

7 PRECAUÇÕES

- Não tente ajustar ou modificar o aparelho.
- A manutenção só poderá ser feita por pessoas qualificadas pela JFL Alarmes.
- Mantenha sempre o terminal de acesso atualizado.

• POR SE TRATAR DE EQUIPAMENTO DE SEGURANÇA E DE AJUSTES SENSÍVEIS, DEVE SER INSTALADO POR PESSOAS TÉCNICAS ESPECIALIZADAS E EXPERIENTES.

8 Regulamentação e informações legais

8.1 Direitos autorais

Este manual está protegido pelas leis internacionais dos direitos autorais. Parte alguma deste manual pode ser reproduzida, distribuída, traduzida ou transmitida de qualquer forma e em qualquer meio, seja eletrônico ou mecânico, incluindo fotocopiadora, gravação ou armazenamento em qualquer sistema de informação ou recuperação sem autorização da JFL.

8.2 Política de atualização de software

A JFL preocupada com a segurança dos equipamentos, visando minimizar ou corrigir vulnerabilidades, realiza melhorias periódicas nos softwares/firmwares dos equipamentos. Isto ajuda a manter os equipamentos protegidos contra softwares maliciosos, ataques de hackers, roubo de informações confidenciais e eventuais falhas exploradas por pessoas mal-intencionadas.

A JFL pratica as seguintes políticas nas centrais e aplicativos:

- Sempre atualizamos os aplicativos nas lojas das plataformas móveis a fim de mitigar problemas de segurança.
- Informações pessoais e informações sensíveis nos aplicativos são armazenadas de forma criptografadas como sugere a LGPD (lei geral de proteção de dados).
- A JFL disponibiliza atualizações do produto por no mínimo dois anos após o lançamento ou enquanto este produto estiver sendo distribuído ao mercado.
- A JFL disponibiliza um serviço de atendimento ao consumidor (SAC) para esclarecimentos de qualquer dúvida sobre os equipamentos.
- O histórico de atualizações do módulo incluindo as vulnerabilidades identificadas, medidas de mitigação e correções de segurança podem ser acessados aqui.
- Se você acreditar que encontrou uma vulnerabilidade de segurança ou privacidade em um produto da JFL, entre em contato com o SAC.
- Para garantir a proteção dos clientes, a JFL não divulga, não discute nem confirma problemas de segurança até que uma investigação seja conduzida e as correções estejam disponíveis.
- É dever do usuário manter sempre o módulo e o aplicativo com os seus respectivos softwares/firmwares atualizados. Para isso, a JFL recomenda que contrate uma empresa ou um profissional de segurança autorizado para que possa dar manutenção preventiva no sistema e analisar eventuais melhorias no sistema a fim de aumentar a proteção do usuário.

8.3 LGPD – lei geral de proteção de dados

A JFL não possui acesso, não coleta e não faz nenhum tratamento de dados através desse produto.

8.4 Marcas registradas e código aberto

- Bluetooth® é uma marca mundialmente registrada da Bluetooth SIG, Inc.
- Wi-Fi®, o logo Wi-Fi são marcas registradas da Wi-Fi Alliance.
- Apple, iPhone, iPad, Siri, Apple Watch e App Store são marcas registradas da Apple Inc registradas nos EUA e em outros países e regiões. iOS é uma marca comercial registrada da Cisco nos EUA e em outros países e é utilizada sob licença.
- O nome “Android”, o logotipo do Android, a marca “Google Play” e outras marcas registradas do Google são propriedades da Google LLC e não fazem parte dos recursos disponíveis no Android Open Source Project.
- Todas as outras marcas registradas e direitos autorais são de propriedade de seus respectivos proprietários.
- As licenças de código abertos usadas nos aplicativos e no firwmare dos equipamentos podem ser encontradas no site da JFL.

9 CERTIFICAÇÃO ANATEL

Este produto está homologado pela Anatel, de acordo com os procedimentos regulamentados pela Resolução Nº 715/2019 e atende aos requisitos técnicos aplicados.

Para maiores informações, consulte o site da Anatel – www.gov.br/anatel/pt-br/

Res. 680

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

GARANTIA

A JFL Equipamentos Eletrônicos Indústria e Comércio Ltda garante este aparelho por um período de 12 meses a partir da data de aquisição, contra defeitos de fabricação que impeçam o funcionamento dentro das características técnicas especificadas do produto. Durante o período de vigência da garantia, a JFL irá reparar (ou trocar, a critério próprio), qualquer componente que apresente defeito, excluindo a bateria que sofre desgaste naturalmente.

Excetuam-se da garantia os defeitos ocorridos por:
- Instalação fora do padrão técnico especificado neste manual;
- Uso inadequado;
- Violação do equipamento;
- Fenômenos atmosféricos e acidentais.

A visita de pessoa técnica a local diverso dependerá de autorização expressa do cliente, que arcará com as despesas decorrentes da viagem, ou o aparelho deverá ser devolvido a empresa vendedora para que seja reparado.

JFL EQUIPAMENTOS ELETRÔNICOS IND. COM. LTDA
Rua João Mota, 471 - Jardim das Palmeiras
CEP 37538-714 - Santa Rita do Sapucaí / MG

Fone: (35) 3473-3550 / Fax: (35) 3473-3571
www.jfl.com.br

Acessus 3000 F REV.: 3 18/06/2025