Manual do usuário

SS 5530 MF FACE LITE

intelbras

SS 5530 MF FACE LITE
Controlador de acesso com reconhecimento facial

Parabéns, você acaba de adquirir um produto com a qualidade e segurança Intelbras.

O SS 5530 MF FACE LITE é um controlador de acesso com autenticação por reconhecimento facial, cartão RFID 13,56 MHz e senha. Através de uma tela sensível ao toque de 7 polegadas proporciona fácil posicionamento para o usuário para melhor leitura da face e praticidade para realizar cadastros e alterar configurações. Pode ser instalado em ambientes internos para acessar catracas ou portas em geral, liberando o acesso através do acionamento de fechaduras elétricas, eletroímãs ou solenoides.

Para download desse guia em espanhol, acesse o QR code abaixo e selecione a aba *Arquivos para download*.

Para descargar esta guía en español, acceda al código QR a continuación y seleccione la pestaña *Archivos para descargar.*

Guia em português

Guía en español

ANATEL
01267-20-00160

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

Este produto contém a placa BL-M8821CS1 código de homologação Anatel 05096-20-00160.

Para mais informações do produto homologado acesse o site: *https://www.gov.br/anatel/pt-br.*

Cuidados e segurança

- As instruções de segurança e operação devem ser guardadas para referências futuras.
- Use a fonte de alimentação que acompanha o produto.
- O produto deve ser utilizado em ambientes internos com temperatura superior a -20 °C e inferior a 50 °C.
- A tentativa de abrir o produto pode danificá-lo e implica em perda do direito a garantia.
- Cuidado ao manejar os cabos para não danificá-los.
- Não sobrecarregue as tomadas ou extensões, pois pode causar incêndio ou choque elétrico.
- Instale-o em um local seguro.
- Não coloque ou instale o produto em lugares expostos a luz solar ou fontes de calor.
- Mantenha o produto longe de umidade, poeira ou fuligem.
- Instale o produto de forma horizontal e em local estável, garantindo a correta fixação para que não caia causando danos ao equipamento.
- É proibido jogar ou borrifar água ou qualquer outro líquido no equipamento.
- Limpe o produto somente com pano seco.
- Instale o produto em local ventilado e não bloqueie a ventilação do controlador de acesso.
- Use apenas acessórios recomendados pelo fabricante.
- LGPD - Lei Geral de Proteção de Dados Pessoais: este produto faz tratamento de dados pessoais, porém a Intelbras não possui acesso aos dados a partir deste produto. Este produto possui criptografia na transmissão e armazenamento dos dados pessoais.

Atenção: danos causados pelo não cumprimento das recomendações de instalação ou uso inadequado do produto não são cobertos pela garantia. Vide certificado de garantia do produto.

Índice

1. Especificações técnicas

Tensão de alimentação		12 Vdc
Potência		12 W
Temperatura de operação		-20 °C a 50 °C
Umidade de operação		0 a 90%
Display		7" sensível ao toque (capacitivo)
Câmera		2 MP CMOS
Intervalo de reconhecimento facial		Distância da câmera à face: 0,3 m a 2 m
		Altura do usuário: 0,9 m a 2,4 m
Tempo de reconhecimento facial		0,3s
Métodos de autenticação		Reconhecimento facial, cartão e senha
Interface de comunicação		Wiegand, 485, 232
Capacidade	usuários	20.000
	faces	20.000
	cartões	20.000
	senhas	20.000
	registros	100.000
Wi-Fi	Antena	Interna
	Padrões	IEEE 802.11b, 802.11g, 802.11n
	Frequência operacional	2.4 GHz ~ 2.4835 GHz
	Largura de banda	Suporta 20 MHz e 40 MHz
	Protocolo de segurança	64/128 bit WEP, WPA/WPA2, WPA-PSK/ WPA2-PSK
	Taxa de transmissão	802.11b: até 11 Mbps 802.11g: até 54 Mbps 802.11n: até 300 Mbps (HT40)
RFID	Modulação	ASK
	Frequência	13,56 MHz
	Taxa de transmissão	106 a 848 kbps
	Código de emissão	13M5K2D
	Tipo antena	Interna
Dimensões (L × A × P)		130 × 283 × 36,9 mm

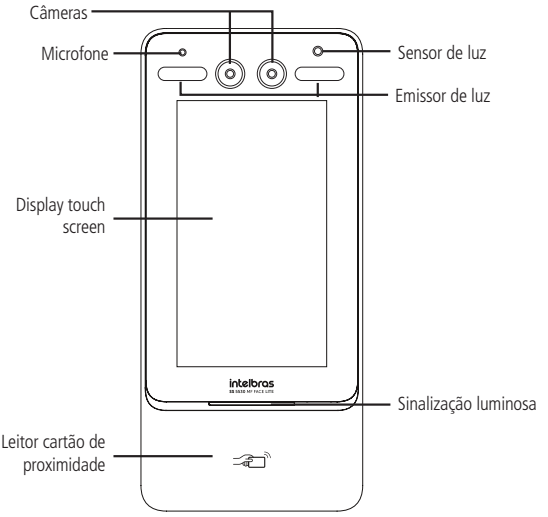
2. Características

- Fácil instalação.
- Visual moderno e funcional.
- Capacidade de armazenar até 100.000 eventos.
- Compatível com leitor auxiliar Wiegand.
- Saída Wiegand configurável.
- Conexão com o software InControl Web.
- Compatível exclusivamente com controladores da linha Bio-T.
- Para uso em ambiente interno.
- Função anti-fake que impossibilita a autenticação por foto.
- Suporta reconhecimento facial, leitor RFID e senha.
- Câmera de 2 MP e WDR.
- Distância de leitura de 0,3 m a 2m de distância.
- Precisão de verificação de face >99,5%.
- Baixo índice de falsa rejeição.

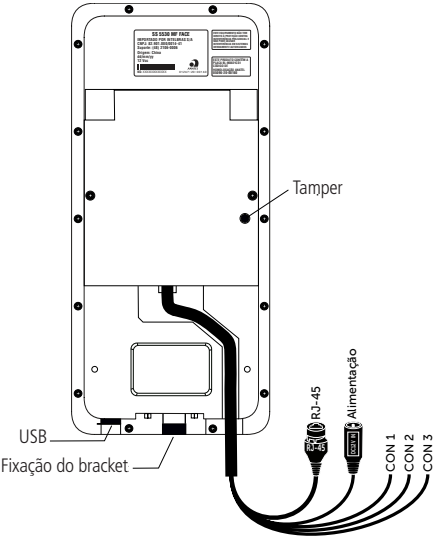
3. Conteúdo da embalagem

- 1× controlador de acesso SS 5530 MF FACE LITE
- 1× fonte de alimentação
- 1× conjunto de buchas e parafusos
- 1× suporte para fixação
- 1× conjunto de ferramentas
- 1× manual do usuário

4. Produto



Vista frontal SS 5530 MF FACE LITE



Vista traseira SS 5530 MF FACE LITE

Onde:

Conector	Cor	Detalhe
CON1	Preto	GND
	Vermelho	12V
	Azul	TAMP
	Branco	WD1
	Verde	WD0
	Marrom	LED
	Amarelo	485-
	Roxo	485+

Conector	Cor	Detalhe
CON2	branco/ vermelho	ALM1_NA
	branco/ laranja	ALM1_COM
	branco/ azul	ALM2_NA
	branco/ cinza	ALM2_COM
	branco/ verde	GND
	branco/ marrom	ALM1_IN
	branco/ amarelo	GND
	branco/ roxo	ALM2_IN

Conector	Cor	Detalhe
CON3	preto/ vermelho	RX
	preto/ laranja	TX
	preto/ azul	GND
	preto/ cinza	SEN
	preto/ verde	BOT
	preto/ marrom	PORTA_ COM
	preto/ amarelo	PORTA_NA
	preto/ roxo	PORTA_NF

4.1. Descrição dos cabos

Interface de leitores (CON1)

Cor	Nome	Descrição
Preto	GND	Saída de alimentação para leitor auxiliar (GND).
Vermelho	12V	Saída de alimentação para leitor auxiliar (+12 V).
Azul	TAMP	Entrada para conexão do sinal TAMPER de um leitor auxiliar.
Branco	WD1	Entrada Wiegand D1 (para conectar a um leitor auxiliar) / Saída Wiegand D1 (para conectar a uma controladora quando em modo escravo).
Verde	WD0	Entrada Wiegand D0 (para conectar a um leitor auxiliar) / Saída Wiegand D0 (para conectar a uma controladora quando em modo escravo).
Marrom	LED	Saída para sinalizar acesso liberado para um leitor auxiliar / Entrada para receber a sinalização de acesso liberado quando estiver em modo escravo.
Amarelo	485-	Entrada RS485 negativa (para conectar a um leitor auxiliar) / Saída RS485 negativa (para conectar a uma controladora quando em modo escravo).
Roxo	485+	Entrada RS485 positiva (para conectar a um leitor auxiliar) / Saída RS485 positiva (para conectar a uma controladora quando em modo escravo).

Interface de alarmes (CON2)

Cor	Nome	Descrição
Branco/ vermelho	ALM1_NA	Contato seco normalmente aberto da saída de alarme 1.
Branco/ laranja	ALM1_COM	Contato comum o relé da saída de alarme 1.
Branco/ azul	ALM2_NA	Contato seco normalmente aberto da saída de alarme 2.
Branco/ cinza	ALM2_COM	Contato comum o relé da saída de alarme 2.
Branco/ verde	GND	Referência para a entrada de alarme 1.
Branco/ marrom	ALM1_IN	Entrada de alarme 1.
Branco/ amarelo	GND	Referência para a entrada de alarme 2.
Branco/ roxo	ALM2_IN	Entrada de alarme 2.

Interface de porta (CON3)

Cor	Nome	Descrição
Preto/ vermelho	RX	Recepção de dados RS232.
Preto/ laranja	TX	Transmissão de dados RS232.
Preto/ azul	GND	Referência para sinal de botão de saída e sensor de porta.
Preto/ cinza	SEN	Conexão para sensor de porta.
Preto/ verde	BOT	Conexão para botão de saída.
Preto/ marrom	PORTA_ COM	Contato comum do relé de acionamento de liberação de acesso.
Preto/ amarelo	PORTA_NA	Contato normalmente aberto do relé de acionamento de liberação de acesso.
Preto/ roxo	PORTA_NF	Contato normalmente fechado do relé de acionamento de liberação de acesso.

5. Esquemas de ligação

5.1. Fonte de alimentação

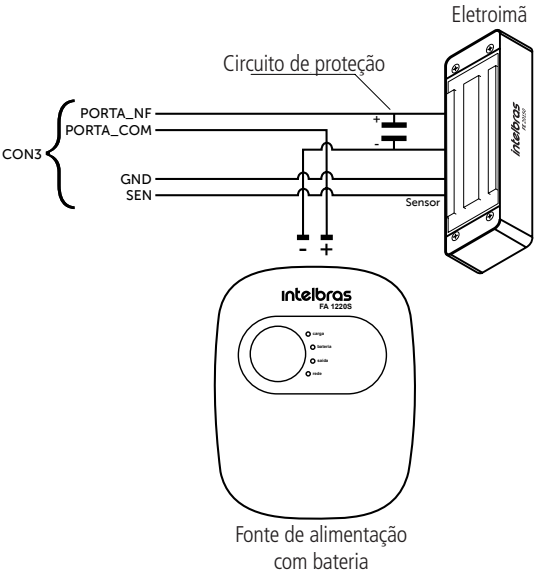
Conecte a fonte de alimentação ao dispositivo e, em seguida, ligue-a na tomada.

Alimentação do produto

Obs.: *recomenda-se o uso de um nobreak para suprir situações de queda de energia.*

5.2. Fechaduras

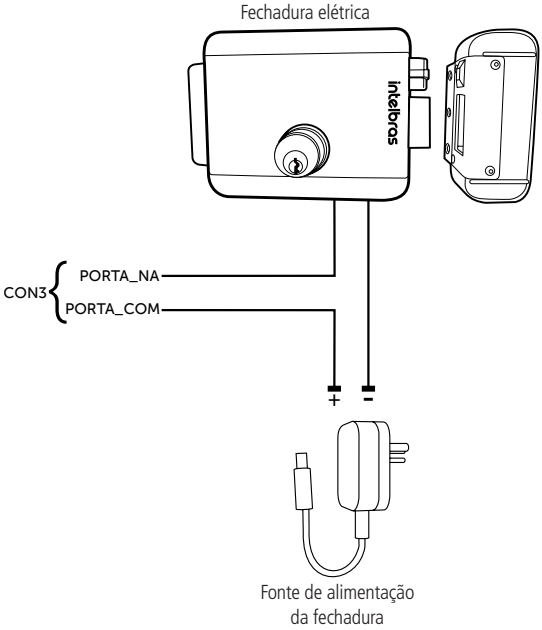
Fechadura eletroímã



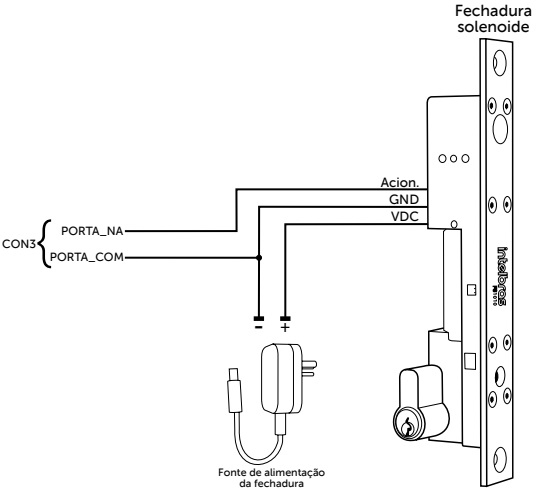
Exemplo de ligação de fechadura eletroímã

Obs.: *caso a fechadura não possua sensor, desconsidere a ligação deste.*

Fechadura elétrica

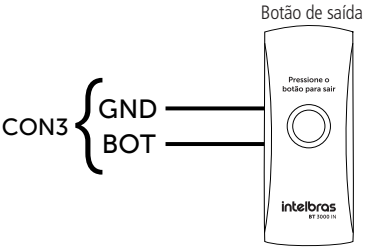


Fechadura solenoide



Exemplo de ligação de fechadura solenoide

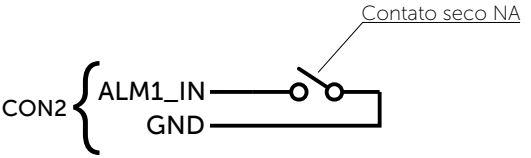
5.3. Botão de saída



Exemplo de ligação de botão de saída

5.4. Alarme

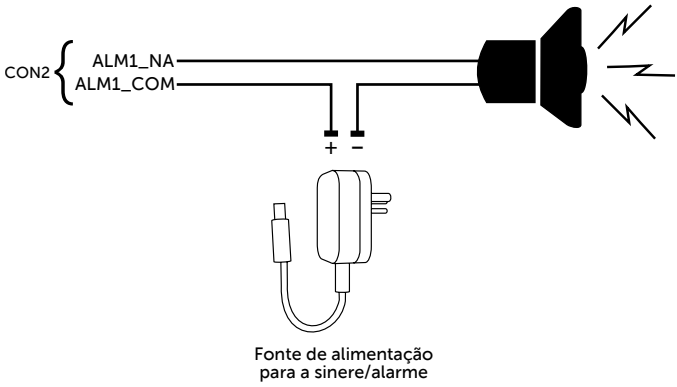
Entrada de alarme



Exemplo de ligação de entrada de alarme

Obs.: *a entrada de alarme é acionada quando o contato seco for fechado.*

Saída de alarme

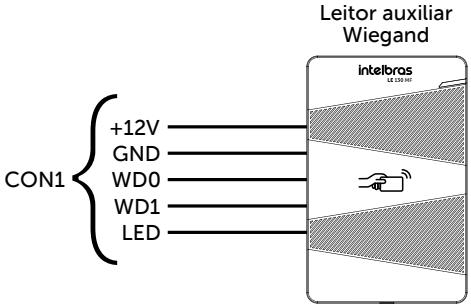


Exemplo de ligação da saída de alarme

Obs.: *o mesmo esquema de ligação se aplica para a saída de alarme 2 (ALM2_NA e ALM2_COM).*

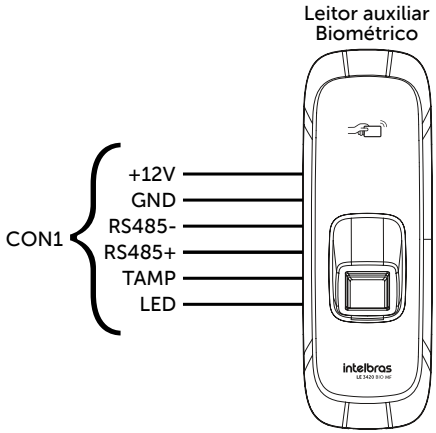
5.5. Leitores auxiliares

Leitor auxiliar wiegand



Exemplo de ligação de leitor auxiliar wiegand

Leitor auxiliar RS-485

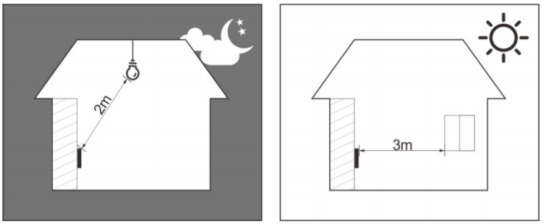


Exemplo de ligação de leitor auxiliar RS-485

6. Instalação

6.1. Locais recomendados

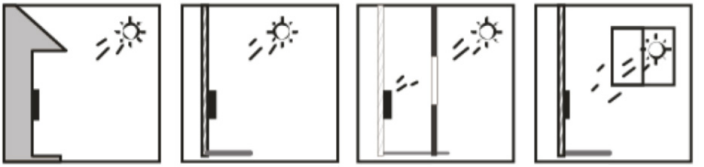
O dispositivo deve ser instalado a pelo menos 2 m de uma lâmpada e a pelo menos 3 metros de um local onde possa entrar claridade proveniente de raios solares.



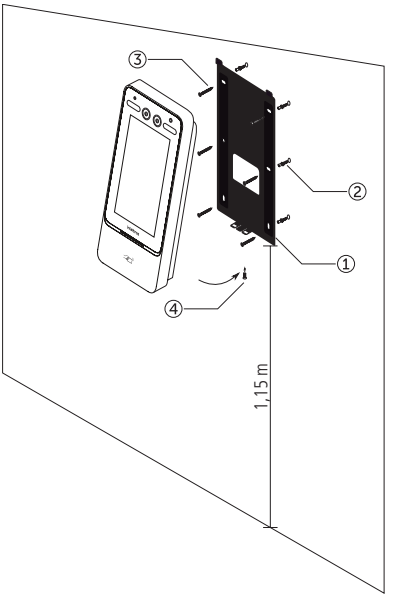
6.2. Locais não recomendados

Certifique-se que o dispositivo está instalado em um local onde não fique com muita claridade atrás do rosto a ser identificado e a luz do sol não incida diretamente no dispositivo mesmo que passando através de uma janela.

Qualquer cenário que ocorre os descritos acima pode afetar no funcionamento do dispositivo.



6.3. Diagrama de instalação



Modelo de fixação

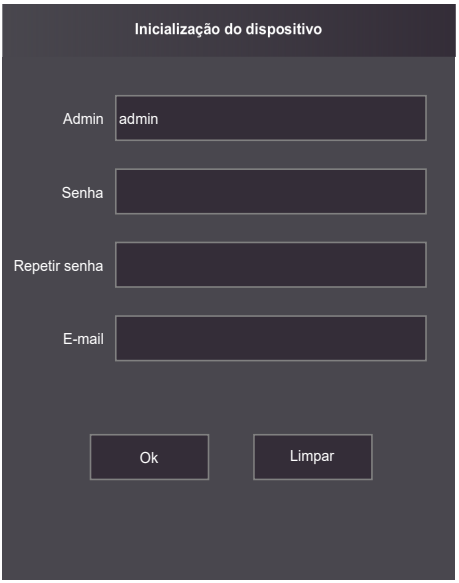
1. Remova o suporte (1) do equipamento;
2. Faça sete orifícios (seis orifícios de instalação do suporte e uma entrada de cabo) na parede de acordo com os orifícios no suporte e fixe o suporte na parede utilizando as buchas (2) e parafusos (3) que acompanham o produto;
3. Efetue a ligação dos cabos (ver item *5. Esquemas de ligação*);
4. Encaixe o controlador de acesso no suporte e coloque o parafuso de fixação (4).

Obs.: *para garantir a leitura de usuários conforme especificações técnicas (altura do usuário: 0,9 m a 2,4 m), recomenda-se a instalação do dispositivo a uma altura de 1,15 m.*

7. Operações do dispositivo

7.1. Inicialização do dispositivo

Ao inicializar o dispositivo pela primeira vez se faz necessário a criação de um usuário administrador. Uma senha e um e-mail são de cadastro obrigatório e devem ser definidos na primeira vez que o controlador de acesso é ativado. O nome de usuário do administrador é *admin* por padrão. O controlador de acesso não poderá ser utilizado sem a realização desse cadastro.



Importante:

- A senha do administrador pode ser redefinida através do endereço de e-mail digitado, utilize um e-mail válido e ativo.
- A senha deve conter de 8 a 32 caracteres, não pode conter espaços e deve conter pelo menos dois tipos de caracteres entre maiúsculas, minúsculas, número e caracteres especiais (excluindo ' " ; : &).

7.2. Tela inicial

Tela inicial

Nessa tela inicial o usuário é capaz de fazer a autenticação do seu acesso seja através da face ( ), cartão ( ) e/ou senha ( ) como indicado no canto superior esquerdo. À direita são exibidos os ícones de conexão como Ethernet, Wi-Fi e USB.

Na parte inferior o ícone para acesso ao menu principal ( ), disponível apenas para o administrador e usuários com esse nível de acesso, e o ícone para acesso por senha ( ).

7.3. Autenticação

O usuário pode fazer o desbloqueio da porta por reconhecimento facial, senha e/ou cartão.

Facial

Para autenticar-se por reconhecimento facial basta se posicionar em frente ao equipamento de maneira que o rosto esteja sendo exibido e enquadrado na tela. Um sinal visual é exibido na tela e uma luz verde acende logo abaixo da tela. De forma opcional, pode haver uma sinalização sonora.

Senha

Para autenticar por senha é preciso acessar o menu *Senha* ( ).

No menu *Senha* duas opções são apresentadas ao usuário: *Senha e senha mestra*.

Na opção *Senha* o usuário poderá autenticar-se utilizando sua ID de usuário e senha cadastrados.

A opção *Senha Mestre* não está relacionada a um usuário específico e necessita ser habilitada pelo administrador do sistema. A senha mestre irá destravar a porta independente dos modos de autenticação ativos, zona de tempo, feriados e regras de anti-passback.

Cartão

A verificação acontece ao passar o cartão na área indicada logo abaixo da tela.

7.4. Menu principal

No menu principal pode-se cadastrar usuários, alterar configurações de acesso, conexão e sistema, verificar a capacidade do dispositivo etc.

Para acessar o menu principal se faz necessário autenticar-se como administrador. Essa autenticação pode ser através da face, cartão, senha de usuário ou ainda através da senha cadastrada na inicialização do equipamento.

Na tela inicial, abra o menu principal através do ícone ( ).

Se esse for o primeiro acesso ao menu principal, selecione a opção Admin e digite a senha cadastrada na inicialização do dispositivo.

Métodos de autenticação do menu principal

Menu principal

7.5. Gerenciamento de usuários

O menu *Usuário* oferece opção para cadastro de um novo usuário, visualizar e editar lista de usuários e lista de administradores, além de habilitar/desabilitar ou modificar a senha mestra.

Novo usuário

Ao acesso *Novo usuário* é exibida a tela de cadastro.

- **ID do usuário:** número que identifica o usuário. Esse número deve ser único e é incrementado automaticamente, entretanto pode ser personalizado pelo administrador como, por exemplo, a matrícula ou alguma referência ao apartamento, sala etc.
- **Nome:** nome que será exibido para esse usuário.
- **Face:** foto do usuário que será utilizada para identifica-lo através do método de autenticação de reconhecimento facial (ver seção *10. Boas práticas para o Reconhecimento Facial*).
- **Cartão:** permite o cadastro de até 5 cartões ou tags RFID por usuários. Nessa opção é permitido habilitar um desses cadastros como coação (emite um alerta para o software de monitoramento e/ou aciona uma saída de alarme).
- **Senha:** permite a criação de uma senha de acesso individual de até 8 dígitos numéricos. Para acessar por esse método de autenticação é necessário que o usuário insira também a ID do usuário.
- **Permissão:** esse campo define se esse cadastro será de um Usuário comum ou um Admin. Este último com acesso ao menu principal e todas as configurações do dispositivo.
- **Zona de tempo:** ID da zona de tempo atribuída ao usuário.
- **Plano de feriado:** ID do plano de feriado atribuída ao usuário.
- **Data de validade:** data limite que esse usuário terá acesso. A partir dessa data o usuário continuará cadastrado no dispositivo, mas seu acesso será negado.
- **Perfil:** define o perfil que será atribuído ao usuário. Dos quais:
  - **Geral**.
  - **Lista negra:** o usuário inserido desse perfil gera um evento de alarme ao efetuar o acesso.
  - **Visitante:** o usuário tem um número limitado de acessos a esse dispositivo.
  - **Ronda:** apenas registra evento, não faz nenhum acionamento.
  - **VIP:** libera o acesso independente das configurações de zona de tempo.
  - **PcD:** estende o tempo de acionamento em 5 segundos para pessoa com deficiência.
- **Nº de usos:** campo permite selecionar quantos acessos o usuário Visitante (do campo anterior) pode realizar no dispositivo.

Informações de usuário

É possível acessar a lista de usuários, lista de usuários administradores e editar suas informações dentro do menu *Usuários*.

Lista de usuários

Apresenta a lista de usuários por ordem de cadastro. Não lista os usuários definidos como administradores, ver subseção seguinte. Ao selecionar um usuário é possível editar informações de acesso, exceto o número da ID do usuário.

Lista de administradores

Apresenta apenas a lista de usuários definidos com permissão de administradores (Admin). Ao selecionar um usuário é possível editar informações de acesso, exceto o número da ID do usuário.

Senha mestra

Nessa opção do menu é possível ativar e desativar a função *Senha mestra,* bem como criar e alterar essa senha.

A opção *Senha mestre* não está relacionada a um usuário específico e irá destravar a porta independente dos modos de autenticação ativos, zona de tempo, feriados e regras de anti-passback.

7.6. Gerenciamento de acesso

Zona de tempo/Feriados

As zonas de tempos servem para restringir ou liberar grupos específicos de usuários em dias e horários da semana. O mesmo pode ocorrer ao cadastrar um feriado.

Zona de tempo

Podem ser configurados até 128 zonas de tempo numeradas no intervalo de 0 a 127. Cada zona de tempo pode ser configurada com 4 períodos de tempo para cada dia da semana.

Ao atribuir uma zona de tempo a um usuário, este só poderá realizar o acesso no dispositivo nos horários pré-estabelecidos. A zona de tempo padrão tem valor 255, que confere ao usuário a possibilidade de acesso em qualquer horário.

Grupo de feriado

O dispositivo permite criar até 128 grupos de feriado, cada um contendo até 16 feriados. Com o grupo criado, pode-se configurar um plano de acesso.

Para criar um grupo acesse o menu ***Acesso>Zonas de tempo/Feriados>Grupo de feriado> +*** (ícone localizado no canto superior direito). Pode ser configurado o número e o nome do grupo de feriado.

Pressione *Grupo de feriado>+* para adicionar os dias ou períodos de feriado. É possível configurar o nome do feriado, seu início e fim. Pressione  para salvar.

Plano de feriado

Os planos de feriado servem para restringir ou liberar grupos específicos de usuários nos períodos definidos.

Acesse o menu *Acesso>Zonas de tempo/Feriados>Plano de feriado> +* (ícone localizado no canto superior direito) para iniciar um plano. Defina um número para o plano (0-127), um nome e a qual grupo de feriado esse plano será aplicado. Em período podem ser estabelecidos até 4 intervalos de tempo na qual o usuário desse perfil terá acesso.

Zona de tempo sempre aberta

Ao atribuir uma zona de tempo neste campo, a porta permanecerá aberta durante os períodos especificados.

Zona de tempo sempre fechada

Ao atribuir uma zona de tempo neste campo, a porta permanecerá fechada durante os períodos especificados e não poderá ser desbloqueada.

Zona de tempo de acesso remoto

Se a zona de tempo de acesso remoto estiver configurada e habilitada, então a verificação remota será requerida. Na verificação remota, sendo apresentada uma credencial válida, é enviada uma mensagem ao software de gerenciamento solicitando a liberação do acesso. Se confirmado, a porta abre, do contrário nada é exibido ao usuário. Após definir a zona de tempo que funcionará nesse modo é necessário ativá-la 

.

Métodos de autenticação

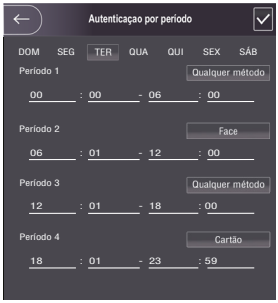
Ao selecionar a opção *Acesso > Método de autenticação* são apresentadas três opções:

» **Autenticação por usuário:** ao selecionar esse método pode-se optar por realizar a autenticação por Cartão, Face (reconhecimento facial), impressão digital (se houver auxiliar) e senha. Nesse menu também é possível fazer a combinação de acesso. Para abrir a opção pressione sobre o nome Autenticação por usuário. O botão *On/Off* serve para habilitar o método. Remover um método fará que seja retornado acesso negado para o mesmo.

» **Ao utilizar a opção +E:** o usuário terá que utilizar todos os métodos selecionados para que o seu acessa seja liberado, ou seja, caso as opções Cartão e Face estejam selecionadas, o usuário terá que passar seu Cartão/tag RFID e na sequência realizar a verificação da Face. O acesso é liberado ao verificar ambas as credenciais.

» **Na opção /Ou:** o usuário utiliza de qualquer um dos métodos para realização do acesso, ou seja, considerando as opções *Cartão e Face selecionadas*, o usuário terá seu acesso liberado se fazer a verificação apenas da Face e também terá seu acesso liberado se fizer a liberação apenas através do cartão/tag RFID.

» **Autenticação por período:** é possível definir até 4 períodos não sobrepostos para cada dia da semana e atribuir um método de autenticação para cada um desses períodos.



Exemplo de configuração de Autenticação por período

No exemplo acima, de 00:00 até 6:00 é possível acessar através de qualquer método disponível no equipamento. No período 2, de 6:01 a 12:00 pode-se acessar apenas por reconhecimento facial e assim por diante. Repare que o período 2 não pode ser de 6:00 a 12:00 para não haver sobreposição. Após efetuar a configuração, pressione  para salvar e então ative o método por período 

.

» **Autenticação por grupo:** permite a criação de grupos de usuários, atribuindo a esse grupo um método de acesso específico e um número de usuários necessários para realizar a validação do acesso.

» Para adicionar um novo grupo, selecione + no canto superior direito e então adicione os usuários desse grupo em Lista de usuários. Adicione o método de autenticação que será utilizado pelo grupo e quantos usuários desse grupo necessitam se autenticar para liberar o acesso no campo *N° min autent.* Caso a lista de usuários seja composta por 10 usuários, o campo *N° min autent.* Poderá variar de 1-10, onde 1 significa que apenas um usuário é o suficiente para abrir a porta e 10 significa que todo o grupo precisa ser validado para abertura da porta.

Alarme

O administrador do sistema pode através do menu *Acesso > Alarme* habilitar ou desabilitar alarmes.

» **Anti-passback:** após autenticar-se no dispositivo na direção de entrada é necessário autenticar-se para sair antes de uma nova autenticação de entrada e vice-versa. Para tanto, é necessário um leitor auxiliar.

» **Coação:** cartões e tag RFID podem ser cadastrados como credencial de coação. Caso esta opção esteja ativa, além de um evento de coação, também será acionada a saída de alarme se houver um acesso utilizando uma credencial de coação.

» **Múltiplas credenciais inválidas:** tentativa recorrente de utilização de cartões ou senhas não cadastradas. Número de tentativas configurada em software.

» **Intrusão:** abertura indevida da porta (requer uso do sensor de porta).

» **Porta aberta:** define depois de quanto tempo soa um alarme sonoro no próprio dispositivo. Pode ser configurado de 1-9999 segundos.

» **Sensor de porta ativado:** necessário estar ativado para que o dispositivo detecte abertura indevida da porta ou que a mesma permaneceu aberta.

Obs.: *a integração de alarme do dispositivo e sua configuração (relé de acionamento, evento ou alarme sonoro) requer uso de software.*

Estado da porta

São três opções para o estado da porta: *NA, NF e Normal.*

- » **NA:** define que a porta estará sempre aberta, ou seja, relé de acionamento sempre ativo.
- » **NF:** define que a porta estará sempre fechada, ou seja, não haverá acionamento mesmo que uma credencial válida seja verificada.
- » **Normal:** porta será liberada com uma credencial válida.

Tempo de abertura de porta

Define o tempo de acionamento do relé de abertura, por padrão 3 segundos.

7.7. Configuração de conexão

Através do menu *Conexão* é possível gerenciar conexões de rede e wiegand.

Configuração de rede

- » **Rede cabeada:** configurações de endereço de IP, máscara de rede e gateway padrão. Se houver um serviço DHCP na rede é possível ativar esta opção para que uma configuração de IP seja atribuída automaticamente.
- » **Registro ativo:** permite conectar o controlador de acesso a plataforma de gerenciamento e dessa forma efetuar gerenciar o dispositivo. É necessário configurar o endereço IP e porta de comunicação do servidor e atribuir uma ID ao dispositivo.
- » **Wi-Fi:** ao ativar o rede Wi-Fi, procure pelas redes disponíveis utilizando a lupa no canto superior direito. Escolha a SSID desejada e insira a senha. O serviço DHCP vem habilitado por padrão.

Obs.:

- » *Para uso do software InControl Web é necessário um IP fixo. Antes de usar a opção DHCP, certifique-se que sua rede irá atribuir sempre o mesmo IP para esse equipamento.*
- » *Para evitar conflitos de IP, certifique-se que configurar a rede cabeada para uma faixa não utilizada em casos que se opte por usar a rede sem fio.*

Porta serial

Selecione a opção desejada de acordo com a direção dos dados, entrada ou saída. As opção estão disponíveis através do menu *Conexão > Porta serial.*

Selecione entrada serial quando utilizar um dispositivo externo com capacidade de ler e gravar cartões ao controlador de acesso. A entrada serial é utilizada para obter informações de acesso do cartão para o controlador de acesso e então para a plataforma de gerenciamento.

A saída serial enviará as informações de abertura e fechamento para o controlador de acesso. Essas informações podem ser de dois tipos: ID do usuário ou N° do cartão.

Selecionar a opção Entrada OSDP quando utilizar um leitor de cartões com protocolo OSDP conectado ao controlador de acesso.

Wiegand

Selecione a opção desejada de acordo com a direção dos dados, entrada ou saída. As opção estão disponíveis através do menu *Conexão > Wiegand.*

Utilize Entrada Wiegand quando utilizar um leitor auxiliar RFID. A seleção entre Wiegand 26 bits ou Wiegand 34 bits é feita de maneira automática.

Para usar o barramento como saída, selecione *Saída Wiegand* e configure os parâmetros de acordo com o dispositivo que receberá o dado de saída, que pode ser a ID do usuário ou N° do cartão.

7.8. Sistema

Data e hora

Para alterar informações de data e hora como ajustar data, formato de data, ajustar hora, horário de verão, serviço NTP e fuso horário, acesse *Sistema > Data e hora.*

Parâmetros de face

Pressione sobre a(s) opção(ões) que deseja alterar, faça o devido ajuste e pressione salvar  .

» **Limiar de detecção facial:** ajusta a precisão do reconhecimento facial. Quanto maior o valor, maior tem de ser a semelhança da captura do dispositivo com a foto utilizada para realizar o cadastro, ou seja, menor será a tolerância a variações de aparência como expressões faciais, barba, acessórios e idade do cadastro. Valor padrão é de 85.

» **Máx. ângulo de reconhecimento facial:** ajusta o ângulo do perfil aceito pelo dispositivo para iniciar o reconhecimento facial. Valor padrão é 90°.

» **Distância pupilar:** representa a quantidade de pixels na imagem entre os centros das pupilas. O valor muda de acordo com o tamanho da face e a distância entre a face e a lente. Quanto mais próximo o rosto da câmera, maior deve ser esse valor. A distância pupilar para um adulto posicionado a 1,5 metros do dispositivo está entre 50 e 70. Valor padrão é 60.

» **Tempo limite de reconhecimento (s):** tempo limite entre a apresentação para o reconhecimento facial e a mensagem de acesso liberado.

» **Tempo limite para acesso facial negado:** tempo limite entre o momento que se apresenta a face que não tem acesso no dispositivo e a mensagem de acesso negado.

» **Limiar anti-fake:** previne o uso de fotos, imagens ou vídeos em meio impresso ou digital de ter acesso ao dispositivo.

Modo de imagem

Em *Sistema > Modo de imagem* selecione a opção que se adequa ao seu cenário. É possível fazer o ajuste da tela para o modo: *Interno, Externo ou Outro*.

Modo do *FLASH*

Há três modos que podem ser utilizados de acordo com o cenário:

» **Automático:** quando o sensor de foto detecta que o ambiente não está escuro, o complemento de luz é desligado, do contrário é ligado.

» **NA:** o complemento de luz permanece sempre ligado.

» **NF:** o complemento de luz permanece sempre desligado.

Configurações do FLASH

Aqui é possível alterar a intensidade do complemento de luz de acordo com a necessidade.

Volume

Utilize as teclas + e – para ajustar o volume do equipamento.

Intensidade da luz infravermelha

Utilize as teclas + e – para ajustar a intensidade da luz infravermelha. Quanto mais, mais limpa a imagem.

Restaurar padrões de fábrica

Dados serão perdidos ao selecionar restaurar padrões de fábrica.

As configurações de IP não são alteradas ao restaurar os padrões de fábrica.

Há duas opções para restaurar os padrões de fábrica:

» **Restaurar padrões de fábrica:** restaura as configurações para o padrão e apaga todos os dados do dispositivo.

» **Restaurar padrões de fábrica (manter usuários e eventos):** restaura as configurações para o padrão e mantém os dados de usuário.

Após selecionar a opção desejada, confirme sua escolha.

Reiniciar

Selecione *Sistema > Reiniciar* confirme para que o dispositivo seja reiniciado.

7.9. USB

Atenção: verifique se o dispositivo USB está corretamente inserido antes de exportar/importar dados de usuário ou atualizar o dispositivo. Nunca remova o dispositivo enquanto faz a exportação/importação ou atualização dos dispositivo. Do contrário a operação falhará.

É necessário exportar as informações de um controlador de acesso antes de importar essas configurações em outro dispositivo

A porta USB também pode ser utilizada para atualização de firmware.

Exportar

Para exportar dados do dispositivo selecione *USB > Exportar*.

Selecione os dados que deseja exportar e confirme. O administrador pode optar por exportar os usuários, os dados faciais, cartões, impressões digitais (quando houver), informações de acesso ou todas as opções anterior selecionando a opção *Todos.*

Importar

Apenas informações que foram exportadas anteriormente podem ser importadas.

Para importar dados para o dispositivo selecione *USB > Importar.*

Selecione os dados que deseja importar e confirme

Atualizar

Para atualizar através de um dispositivo de armazenamento USB renomeie o arquivo de atualização para *update.bin* e salve esse arquivo na raiz do dispositivo USB.

Para atualizar selecione *USB > Atualizar e confirme*.

7.10. Utilidades

Nesse menu estão as configurações de segurança, opção para inverter o código recebido na entrada wiegand, habilitar o módulo de segurança, configurar tipo do sensor de porta e o resultado do feedback.

Configurações de segurança

- **Habilitar redefinição de senha:** se habilitado, é permitida a redefinição de senha através da interface web.
- **HTTPS:** quando habilitado, o protocolo HTTPS será utilizado para o acesso aos comandos CGI, do contrário será utilizado HTTP. O dispositivo irá reiniciar ao habilitar ou desabilitar o protocolo HTTPS.
- **CGI:** oferece um protocolo para servidores web executares aplicações. Habilita o uso do protocolo CGI.
- **SSH:** habilita o protocolo de segurança SSH.
- **Capturar foto:** o dispositivo irá tirar uma foto do usuário quando houver uma tentativa de acesso.
- **Limpar todas as fotos capturadas:** promove a remoção de todas as capturadas.

Inverter Nº do cartão

Permite inverter os bytes recebidos na entrada wiegand para compatibilidade com outros sistemas caso necessário.

Módulo de segurança

Habilita o uso de um relé externo para acionamento da porta. Quando essa opção está habilitada, a entrada de botão e conexões de fechadura do controlador são desabilitadas, devendo-se utilizar a entrada de botão e conexões de fechadura do relé externo.

Caso essa opção esteja habilitada e o relé externo não esteja conectado, ou não responda, o dispositivo retornará acesso negado mesmo que sejam apresentadas credenciais válidas.

Para verificar o esquema de ligação com um relé externo, consulte o manual do produto XR 2201 em nosso site: *https://www.intelbras.com.br.*

Tipo de sensor de porta

O sensor de porta pode ser configurado como NA ou NF.

- **NA:** quando a porta está aberta, o estado do sensor é normalmente aberto ou NA.
- **NF:** quando a porta está aberta, o estado do sensor é normalmente fechado ou NF.

Resultado do feedback

- **Sucesso ou falha:** mostra a mensagem *Sucesso!* para acesso liberado e a mensagem *Não autorizado* para acesso negado.
- **Somente nome:** apresenta ID do usuário, nome e horário para o acesso liberado e a mensagem *Não autorizado* e horário para o acesso negado.
- **Foto e nome:** apresenta ID do usuário, nome e horário acompanhado da foto cadastrada para o acesso liberado e a mensagem *Não autorizado* e horário para o acesso negado.

» **Foto, imagem e nome:** apresenta ID do usuário, nome e horário acompanhado da foto cadastrada e da foto atual para o acesso liberado e a mensagem *Não autorizado* e horário acompanhada da foto atual para o acesso negado.

» **Modo personalizado:** apresenta uma grande seta com fundo verde para o acesso liberado e um grande "X" com fundo vermelho para acesso negado.

7.11. Eventos

No menu Eventos é possível visualizar todos os eventos de acesso. É possível fazer busca por ID de usuário ao acessar o ícone de lupa no lado superior direito.

7.12. Testes

Se o controlador de acesso apresentar algum mal funcionamento, pode-se usar o menu de testes para checar se o dispositivo está funcionamento normalmente. Siga as instruções de acordo com a opção escolhida.

7.13. Infor. Sistema

Em informações do sistema é possível consultar a capacidade do dispositivo, número de série, versão de software, versão de firmware e endereço MAC.

8. Interface web

O controlador de acesso pode ser configurado e operado na web. Através da web, é possível definir parâmetros de rede e de vídeo de acesso.

A interface web pode ser utilizada para a atualização do sistema.

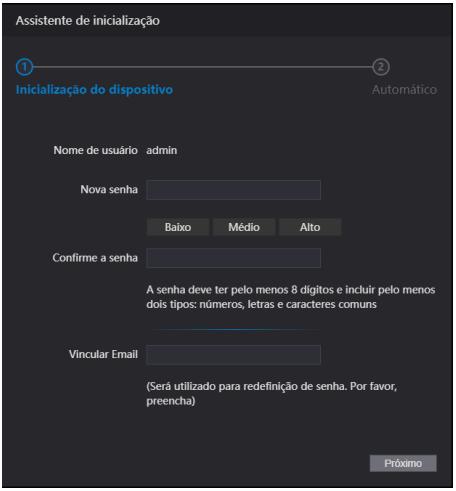
Importante: o gerenciamento de usuários só pode ser feito diretamente no dispositivo ou com o auxílio de software, não é possível realizar cadastros de usuário ou exportar/importar dados de usuários através da interface web.

8.1. Inicialização

Alternativamente a inicialização do dispositivo em tela (item *7.1. Inicialização do dispositivo*), pode-se cadastrar a senha do administrador do sistema através da interface WEB.

Para isso, abra o navegador e acesse o IP do dispositivo (IP padrão é 192.168.1.201).

Obs.: *utilize a última versão do Internet Explorer® ou Chrome®.*



Tela de inicialização através da Interface web

Entre com a nova senha, confirme e adicione um e-mail válido e avance para a próxima etapa.

Importante:

» A senha do administrador pode ser redefinida através do endereço de e-mail digitado, utilize um e-mail válido e ativo.

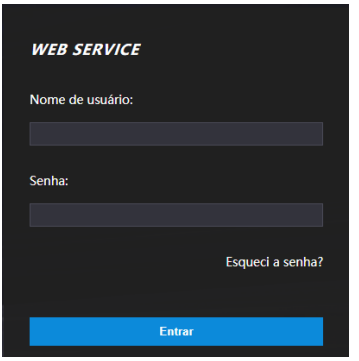
» A senha deve conter de 8 a 32 caracteres, não pode conter espaços e deve conter pelo menos dois tipos de caracteres entre maiúsculas, minúsculas, número e caracteres especiais (excluindo ' " ; : &).

Na tela seguinte o administrador pode optar por ser informado de uma nova versão quando disponível (exige que o dispositivo esteja conectado a internet).

8.2. Login

Abra o navegador e acesse o IP do dispositivo (IP padrão é 192.168.1.201).

Entre com o *Nome de usuário e Senha* e pressione *Entrar*.



Tela de login

Importante:

» O nome de usuário padrão do administrador é admin e a senha é criada na inicialização do dispositivo (ver item *7.1. Inicialização do dispositivo* ou *8.1. Inicialização*)

» Se a senha de administrador for esquecida, pressione *Esqueci a senha?* na tela de login da interface web e siga as instruções na tela (ver item *Esqueci a senha*).

Esqueci a senha

Caso tenha esquecido a senha, utilize a opção Esqueci a senha? na interface WEB. Utilize a câmera do seu celular para escanear o código QR apresentado e siga as instruções. Uma contrassenha será enviada no endereço de e-mail cadastrado na inicialização do dispositivo. Insira essa contrassenha e uma janela para cadastrar nova senha será exibida. Caso o administrador não esteja mais disponível, tão pouco o e-mail cadastrado, siga os procedimentos apresentados na seção *9. Restaurar senha de administrador*.

8.3. Link de alarme

Configuração de link de alarme

Dispositivos de alarme podem ser conectados ao controlador de acesso e pode-se configurar a ação do controlador de acesso quando receber uma entrada de alarme.

Em *Link de alarme > Link de alarme* são apresentadas dois canais de entrada. Para editar pressione o ícone na coluna editar.

» **Canal entrada:** não pode ser modificado. Entrada 1 refere-se a entrada de alarme 1 (ALM1) e entrada 2 a entrada de alarme 2 (ALM2).

» **Nome:** insira um nome para a zona de alarme.

» **Tipo de alarme:** selecione de acordo com o sistema de alarme. Ao selecionar NA, o alarme será disparado caso um contato seja detectado o fechamento entre GND e a entrada de alarme. Ao selecionar NF, haverá o disparo de um alarme quando for detectado que a entrada de alarme não está conectada ao GND.

- **Ativar link de incêndio:** se o link de incêndio estiver ativo, o controlador de acesso irá acionar as saídas de alarme e destravará a porta se houver um acionamento na entrada de alarme correspondente. Ao ativar o link de incêndio também são ativadas as saídas de alarme e a porta configurada para sempre aberta. Verifique as demais configurações para a ação desejada.
- **Habilitar saída:** se ativo, envia um sinal através do contato seco da saída de alarme.
- **Duração (seg.):** define duração da saída de alarme.
- **Canal de saída:** define se atracará os relés das saídas de alarme 1 e/ou 2.
- **Ativar link de acesso:** quando ativo permite forçar o estado da porta no campo *Tipo de canal*.
- **Tipo de canal:** se NA, abrirá e manterá a porta aberta. Na opção NF manterá a porta fechada e negará qualquer tentativa de acesso.

8.4. Capacidade

Ao acessar a aba capacidade são apresentadas as quantidades de usuários e credenciais cadastradas no dispositivo.

8.5. Configuração de vídeo

Estão disponíveis configurações de vídeo, detecção de movimento e modo de imagem.

Configurações de vídeo

Permite ajustes no streaming de vídeo e na imagem apresentada na tela do dispositivo.

Detecção de movimento

A área em vermelho representa a área utilizada para detectar objetos em movimento. O gráfico ao lado permite visualizar a interação entre movimento e detecção. Por padrão, todo frame é utilizado para detecção de movimento e os parâmetros Sensibilidade e Limiar com o valor de 50. Para salvar sua alteração pressione *Ok*. Após pressionar *Padrão* para restaurar os padrões de fábrica, também é necessário pressionar *Ok*.

Modo de imagem

Em *Config. De vídeo > Modo de imagem* selecione a opção que se adequa ao seu cenário. É possível fazer o ajuste da tela para o modo: *Interno, Externo ou Outro.*

8.6. Detecção de face

Nessa janela é possível estabelecer uma região para o controle de acesso facial e o tamanho da face (que vai definir a distância de reconhecimento).

Através do botão *Detectar região* é possível ajustar a área da tela em que o dispositivo irá efetuar o reconhecimento facial. Fora dessa área o dispositivo não efetuará o reconhecimento facial.

O botão *Desenhar alvo* permite especificar a partir de qual tamanho o dispositivo efetuará a verificação da face. Quanto maior essa área, mais próximo tem de estar o usuário que será identificado. Quanto menor esse valor, maior a distância que o dispositivo efetuará a leitura da face.

- **Limiar de reconhecimento facial:** ajusta a precisão do reconhecimento facial. Quanto maior o valor, maior tem de ser a semelhança da captura do dispositivo com a foto utilizada para realizar o cadastro, ou seja, menor será a tolerância a variações de aparência como expressões faciais, barba, acessórios e idade do cadastro. Valor padrão é de 85.
- **Máx. ângulo de reconhecimento facial:** ajusta o ângulo do perfil aceito pelo dispositivo para iniciar o reconhecimento facial. Valor padrão é 90°.
- **Limiar anti-fake:** previne o uso de fotos, imagens ou vídeos em meio impresso ou digital de ter acesso ao dispositivo.
- **Config. de brilho de flash:** aqui é possível alterar a intensidade do complemento de luz de acordo com a necessidade.
- **Modo do flash:** há três modos que podem ser utilizados de acordo com o cenário:
  - **Automático:** quando o sensor de foto detecta que o ambiente não está escuro, o complemento de luz é desligado, do contrário é ligado.
  - **NA:** o complemento de luz permanece sempre ligado.
  - **NF:** o complemento de luz permanece sempre desligado.
- **Luz infravermelha:** ajusta a intensidade da luz infravermelha. Quanto mais, mais limpa a imagem.
- **Tempo limite de reconhecimento (s):** tempo limite entre a apresentação para o reconhecimento facial e a mensagem de acesso liberado.

» **Tempo limite para acesso facial negado:** tempo limite entre o momento que se apresenta a face que não tem acesso no dispositivo e a mensagem de acesso negado.

» **Distância pupilar:** representa a quantidade de pixels na imagem entre os centros das pupilas. O valor muda de acordo com o tamanho da face e a distância entre a face e a lente. Quanto mais próximo o rosto da câmera, maior deve ser esse valor. A distância pupilar para um adulta posicionado a 1,5 metros do dispositivo está entre 50 e 70. Valor padrão é 60.

» **ID canal:** são duas opções: 1 para a câmera de luz visível e 2 para a câmera de luz infravermelha.

» **Ativar Exp. Facial:** ao ativar essa opção, prepara o dispositivo para funcionar melhor em ambientes mais iluminados como recepções e áreas de acesso a visitantes.

Para salvar sua alteração pressione *Ok*. Após pressionar Padrão para restaurar os padrões de fábrica, também é necessário pressionar *Ok*.

8.7. Configuração de rede

As configurações de endereço de IP, máscara de rede e gateway padrão podem ser consultadas ou alteradas em *Config. de rede > TCP/IP.*

8.8. Segurança

Em *Segurança > Serviços* o administrador do dispositivo pode habilitar/desabilitar os protocolocar SSH, CGI, HTTPS, bem como habilitar a redefinição de senha através da opção *Esqueci a senha?* da tela de login na interface web.

8.9. Configuração de voz

No menu *Config. de voz* pode-se alterar a volume do dispositivo.

8.10. Usuários rede

Permite cadastrar outros usuários administradores e editar o usuário admin.

Importante: o usuário admin não pode ser excluído.

8.11. Manutenção

Define horário para que o dispositivo seja reiniciado automaticamente. Dessa forma o sistema operacional pode fazer os ajustes necessários para melhorar a performance e desempenho. O dispositivo tem por padrão a configuração definida para reiniciar toda terça-feira às duas horas da manhã (de acordo com relógio do dispositivo).

8.12. Backup

Permite ao usuário administrador salvar uma cópia das configurações do dispositivo ou restaurar uma configuração previamente criada. Pode ser utilizado quando vários dispositivos necessitam utilizar a mesma configuração.

Para salvar pressione *Exportar configurações* e um arquivo será salvo no seu dispositivo.

A importação pode ser realizada iniciando por Procurar o arquivo desejado e então Importar configurações.

8.13. Atualizar

Importante: utilize apenas arquivos fornecidos pela intelbras.

Mantenha o dispositivo e o controlador de acesso energizados durante todo o processo de atualização.

A atualização inicia pelo botão *Procurar* para indicar a localização do arquivo. Utilize arquivos locais, arquivos em rede podem causar falha no processo de atualização.

8.14. Informações da versão

Apresenta informações do sistema como versão de firmware, da interface web, número de série e MAC.

8.15. Usuário online

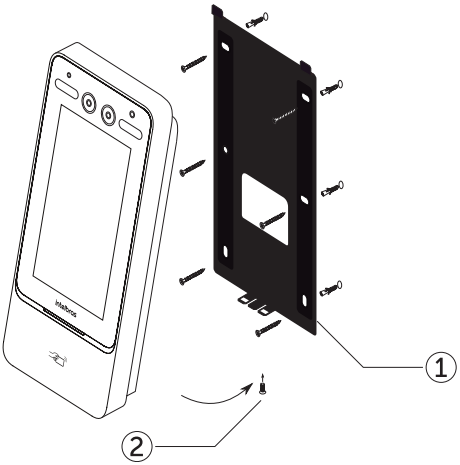
Ao acessar Usuário online uma lista com o ID do usuário, nome do usuário, endereço de IP e hora do login é exibida.

8.16. Eventos

Exibe uma lista com os eventos de administradores e eventos de sistema.

9. Restaurar senha de administrador

Caso não se tenha mais a senha do administrador e/ou acesso ao e-mail cadastrado na inicialização do dispositivo, pode-se realizar uma restauração através do hardware. Para isso, siga as etapas listadas abaixo.



Modelo de fixação

1. Desligue o equipamento;
2. Remova o parafuso de fixação do suporte (2);
3. Remova o dispositivo do suporte (1);
4. Pressione e segure o tamper localizado na parte traseira do equipamento;
5. Religue o dispositivo;
6. Aguarde a total inicialização do dispositivo;
7. Solte o tamper;
8. Aguarde 30 segundos. O LED de sinalização irá piscar na cor verde;
9. Pressione e solte o tamper 3 vezes. Cada vez que pressionar e soltar o tamper o LED piscará na cor verde. Ao soltar o tamper pela terceira vez o dispositivo reiniciará e voltará na tela de inicialização permitindo o cadastro de uma nova senha de administrador.

10. Boas práticas para o reconhecimento facial

10.1. Antes do registro

» Óculos, chapéus e barbas podem influenciar o desempenho do reconhecimento de rosto. Não cubra as sobrancelhas ao usar chapéus.

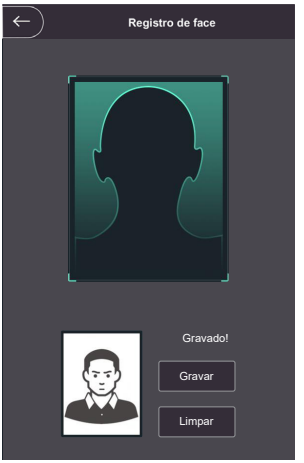
» Atualize o cadastro caso haja uma grande mudança visual, como a retirada da barba, se houver dificuldade no acesso.

» Mantenha seu rosto visível.

» Mantenha o dispositivo a pelo menos dois metros de distância da fonte de luz e a pelo menos três metros de janelas ou portas; caso contrário, a luz solar direta pode influenciar o desempenho do reconhecimento de face do dispositivo.

10.2. Durante o registro

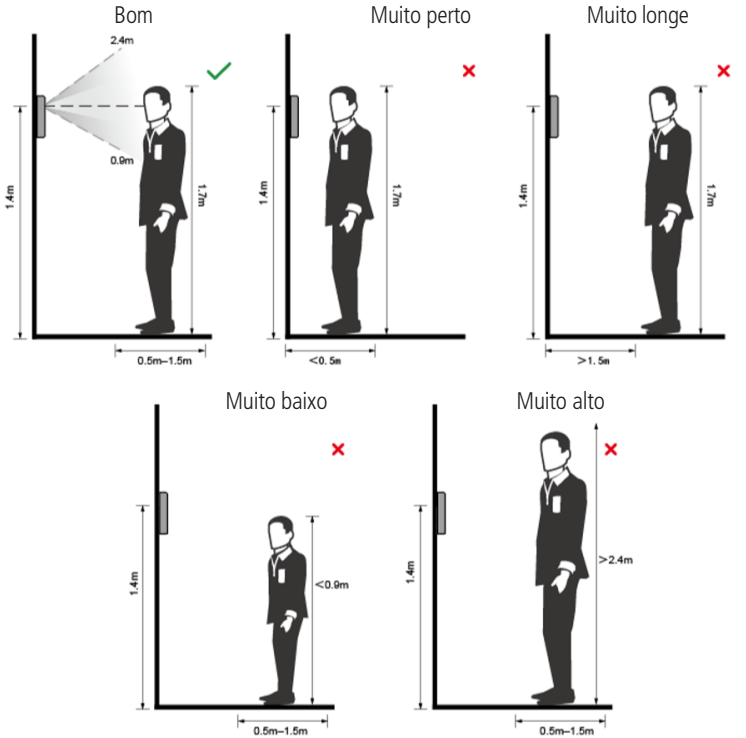
Você pode registrar faces através do controlador de acesso ou através do software. Para registro através do software, consulte o manual do usuário do software. Posicione sua cabeça na moldura de captura de fotos. Uma foto do seu rosto será capturada automaticamente.



» Não balance a cabeça ou o corpo, pois o registro pode falhar.
» Evite que duas faces apareçam na caixa ao mesmo tempo.

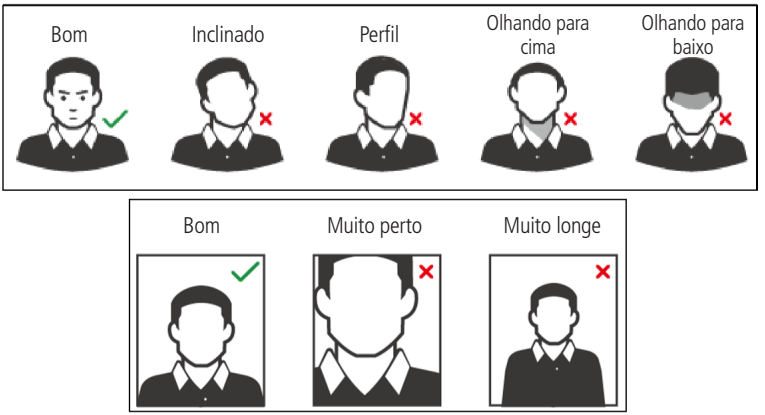
Posição do rosto

Se seu rosto não estiver na posição apropriada, o efeito de reconhecimento de rosto poderá ser influenciado.



Requisitos de rostos

- » Verifique se o rosto está visível e se a testa não está coberta por cabelos.
- » Não use óculos, chapéus, barbas pesadas ou outros ornamentos para o rosto que influenciem a gravação da imagem do rosto.
- » Com os olhos abertos, sem expressões faciais, e faça seu rosto ficar voltado para o centro da câmera.
- » Ao gravar seu rosto ou durante o reconhecimento de rosto, não o mantenha muito próximo ou muito longe da câmera.



Requisitos para importação de fotos

Quando importar as fotos de usuários - seja através da porta USB ou utilizando um software de gestão de controle de acesso compatível - recomenda-se a utilização de imagens com resolução superior a 500 × 500 pixels (L × A)[1], onde o rosto não deve ocupar mais de 2/3 da área total da imagem. No caso de bases de dados pré-existente, atente-se para as resoluções mínima e máxima:

- » Resolução Mínima: 150 × 300 pixels (L × A)[1]
- » Resolução Máxima: 600 × 1200 pixels (L × A)[1]

Para todos os casos, o tamanho máximo do arquivo deve ser inferior a 100 KB e estar no formato JPG.

[1] A altura não deve exceder duas vezes a largura. Por exemplo, se largura for 300 pixels, então a altura poderá ser igual ou inferior a 600 pixels.

Termo de garantia

Fica expresso que esta garantia contratual é conferida mediante as seguintes condições:

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo: Nº de série:

Revendedor:

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais vícios de fabricação, que porventura venham a apresentar, pelo prazo de 1 (um) ano – sendo este de 90 (noventa) dias de garantia legal e 9 (nove) meses de garantia contratual –, contado a partir da data da compra do produto pelo Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo o território nacional. Esta garantia contratual compreende a troca gratuita de partes, peças e componentes que apresentarem vício de fabricação, incluindo as despesas com a mão de obra utilizada nesse reparo. Caso não seja constatado vício de fabricação, e sim vício(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com essas despesas.
2. A instalação do produto deve ser feita de acordo com o Manual do Produto e/ou Guia de Instalação. Caso seu produto necessite a instalação e configuração por um técnico capacitado, procure um profissional idôneo e especializado, sendo que os custos desses serviços não estão inclusos no valor do produto.
3. Constatado o vício, o Senhor Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado mais próximo que conste na relação oferecida pelo fabricante – somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia aqui previsto. Se isso não for respeitado, esta garantia perderá sua validade, pois estará caracterizada a violação do produto.
4. Na eventualidade de o Senhor Consumidor solicitar atendimento domiciliar, deverá encaminhar-se ao Serviço Autorizado mais próximo para consulta da taxa de visita técnica. Caso seja constatada a necessidade da retirada do produto, as despesas decorrentes, como as de transporte e segurança de ida e volta do produto, ficam sob a responsabilidade do Senhor Consumidor.
5. A garantia perderá totalmente sua validade na ocorrência de quaisquer das hipóteses a seguir: a) se o vício não for de fabricação, mas sim causado pelo Senhor Consumidor ou por terceiros estranhos ao fabricante; b) se os danos ao produto forem oriundos de acidentes, sinistros, agentes da natureza (raios, inundações, desabamentos, etc.), umidade, tensão na rede elétrica (sobretensão provocada por acidentes ou flutuações excessivas na rede), instalação/uso em desacordo com o manual do usuário ou decorrentes do desgaste natural das partes, peças e componentes; c) se o produto tiver sofrido influência de natureza química, eletromagnética, elétrica ou animal (insetos, etc.); d) se o número de série do produto tiver sido adulterado ou rasurado; e) se o aparelho tiver sido violado.
6. Esta garantia não cobre perda de dados, portanto, recomenda-se, se for o caso do produto, que o Consumidor faça uma cópia de segurança regularmente dos dados que constam no produto.
7. A Intelbras não se responsabiliza pela instalação deste produto, e também por eventuais tentativas de fraudes e/ou sabotagens em seus produtos. Mantenha as atualizações do software e aplicativos utilizados em dia, se for o caso, assim como as proteções de rede necessárias para proteção contra invasões (hackers). O equipamento é garantido contra vícios dentro das suas condições normais de uso, sendo importante que se tenha ciência de que, por ser um equipamento eletrônico, não está livre de fraudes e burlas que possam interferir no seu correto funcionamento.
8. Descarte adequadamente seu produto após vida útil - entregue em pontos de coleta de produtos eletroeletrônicos, em alguma assistência técnica autorizada Intelbras ou consulte nosso site www.intelbras.com.br e suporte@intelbras.com.br ou (48) 2106-0006 ou 0800 7042767 para mais informações.

Sendo estas as condições deste Termo de Garantia complementar, a Intelbras S/A se reserva o direito de alterar as características gerais, técnicas e estéticas de seus produtos sem aviso prévio.

Todas as imagens deste manual são ilustrativas.

intelbras

fale com a gente

Suporte a clientes: (48) 2106 0006
Fórum: forum.intelbras.com.br
Suporte via chat: chat.apps.intelbras.com.br
Suporte via e-mail: suporte@intelbras.com.br
SAC / Onde comprar? / Quem instala? : 0800 7042767

Importado no Brasil por: Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – 88122-001
CNPJ 82.901.000/0014-41 – www.intelbras.com.br

01.25
Origem: China