



Manual do usuário

SS 710

intelbras

SS 710

Controlador de acesso

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

O SS 710 é um controlador de acesso stand alone que possui conexão com software de gerenciamento de acesso SoapAdmin 3.5, via Ethernet. Com um design mais moderno e várias opções de gerenciamento de acesso, possui como método de autenticação a senha numérica, a biometria digital, a biometria facial e o cartão de proximidade.



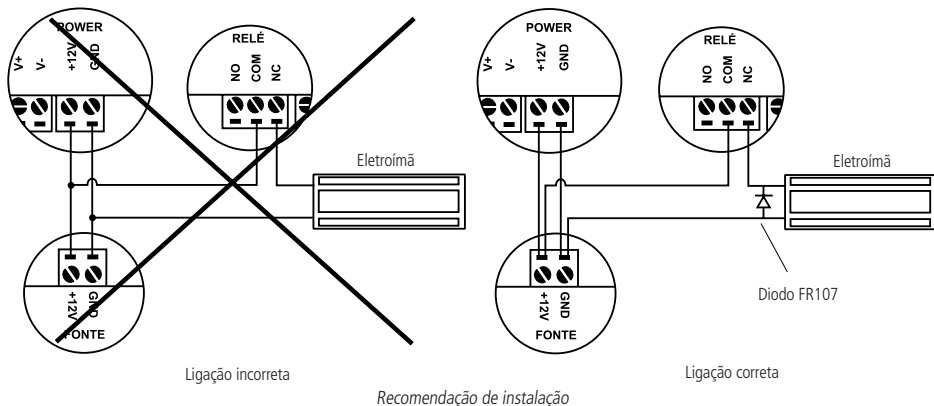
Este equipamento opera em caráter secundário, isto é, não tem direito à proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

Cuidados e segurança

- » Respeite a altura de instalação (1,15 m), conforme instruções contidas na seção 4.1. *Recomendações de instalação*, para que o reconhecimento facial funcione corretamente.
- » Com a rede elétrica desligada, execute toda a instalação e somente após verificar se a instalação está correta, ligue a rede elétrica.
- » Ligue primeiro o cabo GND (0 V) e depois os outros cabos. Isso previne danos causados pela energia estática.
- » Utilize cabos flexíveis de 0,75 mm² ou superiores para ligações de alimentação do equipamento e fechadura.
- » Utilize cabos flexíveis de 0,50 mm² ou superiores para as demais ligações do equipamento. Não utilize cabos UTP para fazer qualquer tipo de ligação, pois, além de não serem adequados, podem prejudicar o funcionamento do produto.

Obs.: recomenda-se o uso de cabos-manga blindados para ligação dos leitores em ambientes que possam sofrer interferência eletromagnética.

- » Não se deve passar cabos de rede elétrica e cabos de dados (manga) na mesma tubulação.
- » Não faça derivação dos terminais de alimentação da controladora para os terminais de ligação da fechadura. Deve-se trazer dois fios separados da fonte de alimentação, como exige a imagem a seguir:

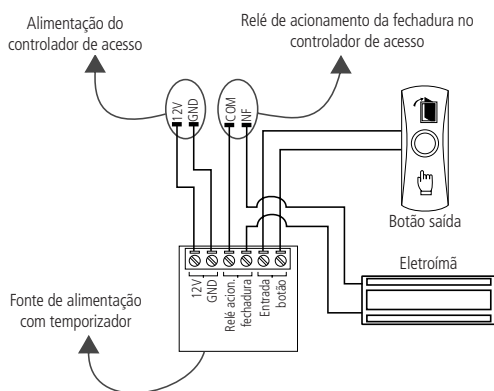
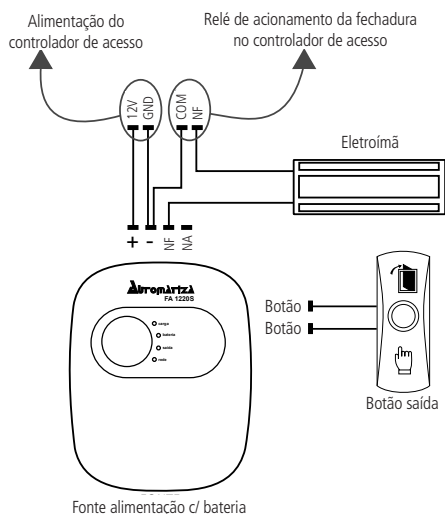


- » Use o diodo FR107 nas fechaduras-eletroímã que não são da marca Automatiza, como demonstrado na figura acima.
- » Use o circuito desmagnetizante fornecido junto com a fechadura-eletroímã Automatiza.
- » Não instale o produto em locais sujeitos a extremo calor ou umidade.
- » Recomenda-se utilizar uma rede isolada com o servidor ligado no mesmo switch das controladoras, para melhorar o desempenho do sistema. Não recomendamos o cascadeamento entre switches.
- » Não exponha o produto ao sol ☀️, à chuva ☔ ou à umidade. Este produto deve ser instalado em locais cobertos.
- » Não utilize produtos químicos para limpeza do sensor biométrico.

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.

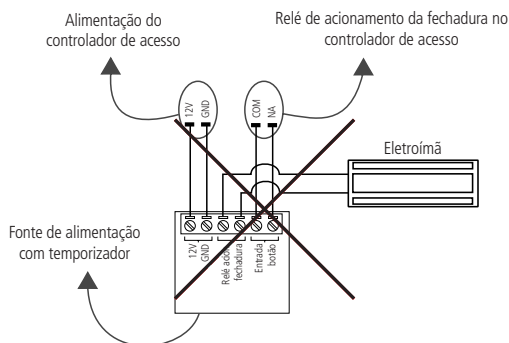
Outros cuidados a serem tomados ao utilizar o controlador de acesso

Para acionar a fechadura, utilize diretamente o relé do controlador de acesso. Ao utilizar uma placa temporizadora ou uma fonte com temporizador, utilize uma ligação em série entre os relés de acionamento, como está representado abaixo:



Atenção:

NÃO instale o produto de modo que o relé de acionamento da fechadura, no controlador de acesso, seja utilizado para acionar uma fonte com temporizador, como apresentado no exemplo a seguir:



Índice

1. Especificações técnicas	6
2. Características	6
3. Conteúdo da embalagem	6
4. Produto	7
4.1. Recomendações de instalação	8
5. Esquemas de ligação	8
5.1. Fonte de alimentação	8
5.2. Fechadura-eletrôimã	9
5.3. Fechadura elétrica	10
5.4. Fechadura solenoide	10
5.5. Botão de saída	11
5.6. Saída alarme 12 V	11
5.7. Campainha	12
5.8. Leitor auxiliar	13
5.9. Leitor LE 311	13
5.10. Entrada auxiliar	14
6. Operações do sistema	14
6.1. Menu de programação	15
6.2. Usuário-adm	15
6.3. Privilégios usuário	21
6.4. Sistema	22
6.5. Personalização	25
6.6. Gerenciamento de dados	27
6.7. Controle acesso	28
6.8. Procurar registros	34
6.9. Autoteste	35
6.10. Informações do sistema	35
6.11. Gerenciamento pen drive	36
6.12. Reset administrador	37
7. Comunicação do equipamento	39
7.1. Configurar comunicação	39
8. Detalhes e cuidados com o leitor biométrico	41
Termo de garantia	42

1. Especificações técnicas

Tensão de alimentação	12 Vdc
Corrente de operação	400 mA
Corrente de chaveamento	1,5 A
Temperatura de operação	0 °C ~ 45 °C
Umidade de operação	20% a 80%
Métodos de autenticação	Cartão de proximidade, senha numérica, biometria digital e biometria facial
Capacidade máxima de cartões	5.000
Capacidade máxima de biometrias digitais	1.000
Capacidade máxima de biometrias faciais	400
Modulação	ASK
Frequência de operação	125 kHz
Taxa de transmissão	3,906 kbps
Código de emissão	125KA2DCN
Tipo antena	Interna
Interface de comunicação	Ethernet
Dimensões (L x A x P)	87 × 187 × 62,5 mm

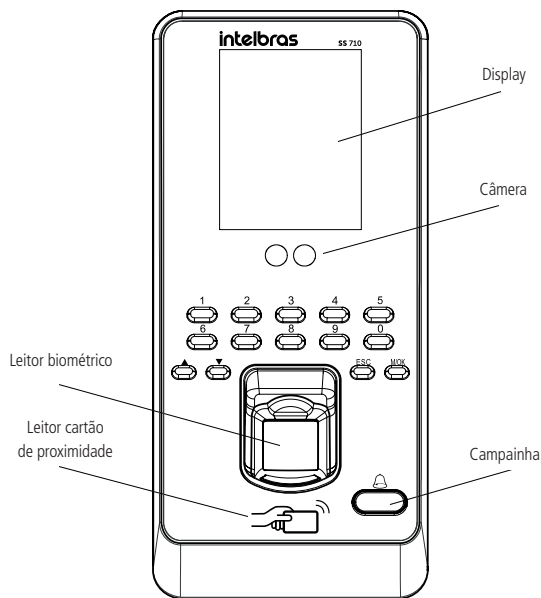
2. Características

- » Fácil instalação.
- » Gabinete resistente.
- » Visual moderno e funcional.
- » Capacidade de armazenar até 100.000 eventos.
- » Compatível com leitores auxiliares Wiegand 125 kHz.
- » Compatível com o LE 311E.
- » Possui entrada e saída Wiegand configuráveis.
- » Possui conexão com o software SoapAdmin 3.5, via Ethernet.
- » Capacidade de realizar download e upload através de um pen drive.

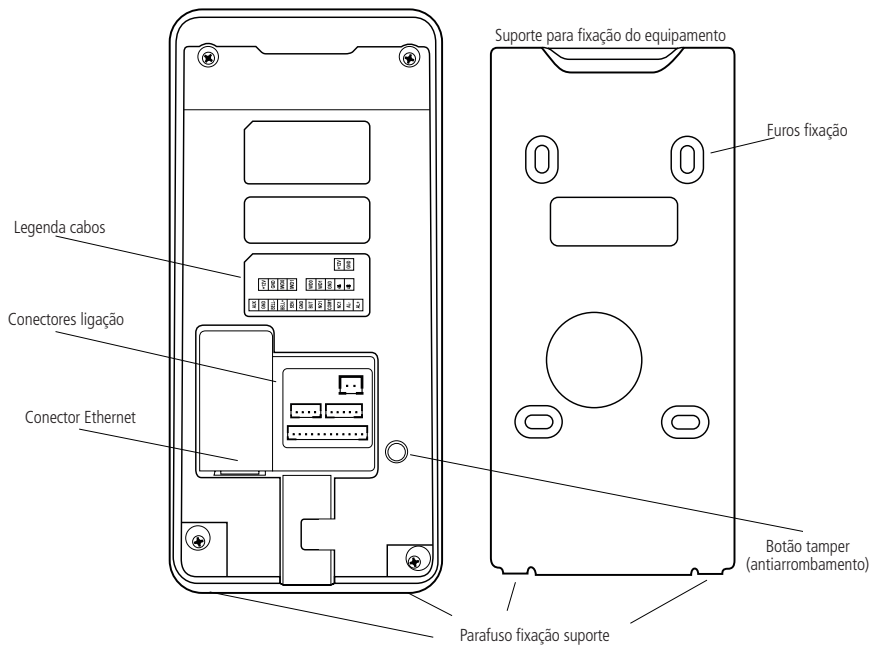
3. Conteúdo da embalagem

- » 1 controlador de acesso SS 710
- » 1 conjunto de cabos para ligação
- » 1 chave Tork
- » 6 parafusos
- » 4 buchas
- » 1 diodo FR107
- » 1 manual de instruções

4. Produto



Vista frontal SS 710

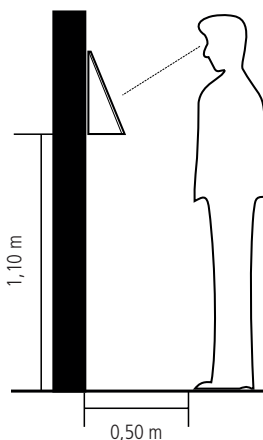


Fixação SS 710

4.1. Recomendações de instalação

Recomenda-se que a distância entre uma pessoa e o dispositivo seja de 0,5 m (para pessoas com altura entre 1,55 m a 1,85 m). A relação entre altura da pessoa e a distância entre ela e o dispositivo poderá ser ajustada com base na imagem facial capturada pelo dispositivo (*tela do SS 710*), afastando-a ou aproximando-a do equipamento até atingir o enquadramento sugerido.

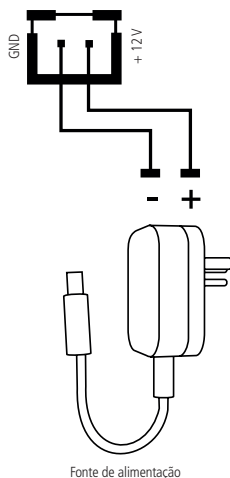
Altura de instalação recomendada (como mostra a figura):



Tanto no cadastro quanto na verificação, a altura da instalação do dispositivo deverá ser respeitada (1,10 m), caso contrário, o desempenho do reconhecimento facial do equipamento será comprometido.

5. Esquemas de ligação

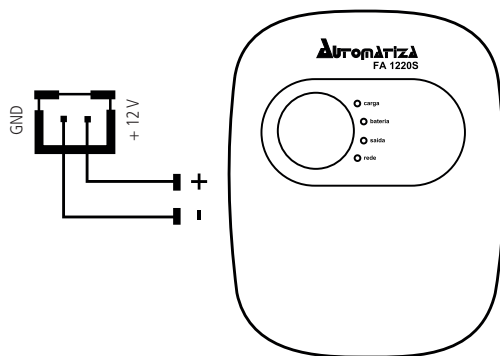
5.1. Fonte de alimentação



Fonte de alimentação

Ligação da fonte de alimentação

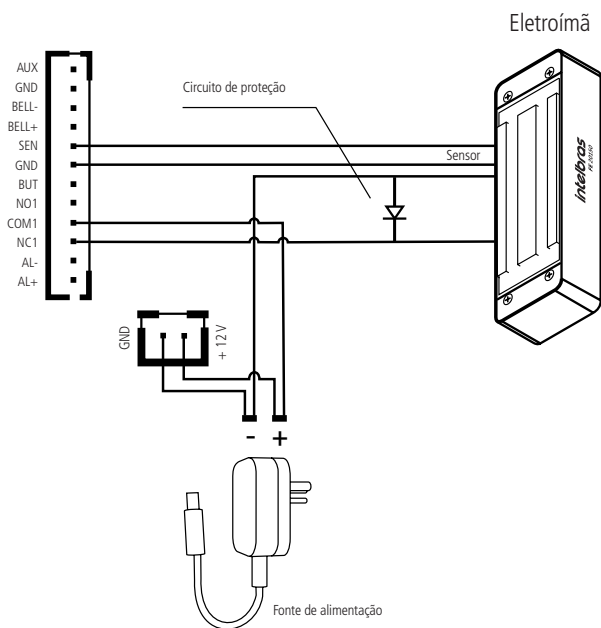
Obs.: caso não haja nobreak para alimentar o equipamento em situações de queda de energia, é recomendável a instalação de uma fonte de alimentação que possua bateria.



Fonte de alimentação com bateria

Ligação da fonte de alimentação FA 1220S

5.2. Fechadura-eletrôimã

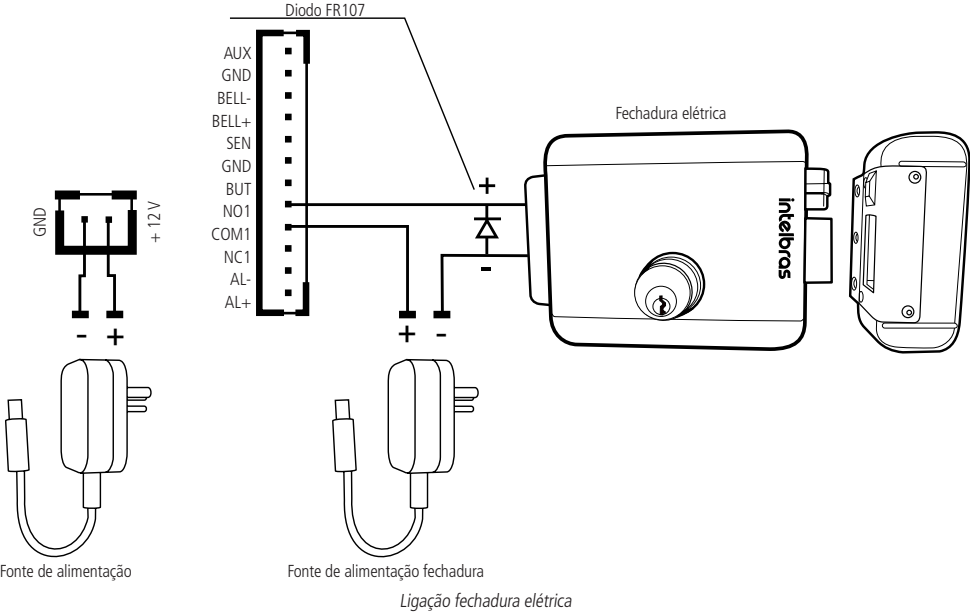


Ligação fechadura-eletrôimã

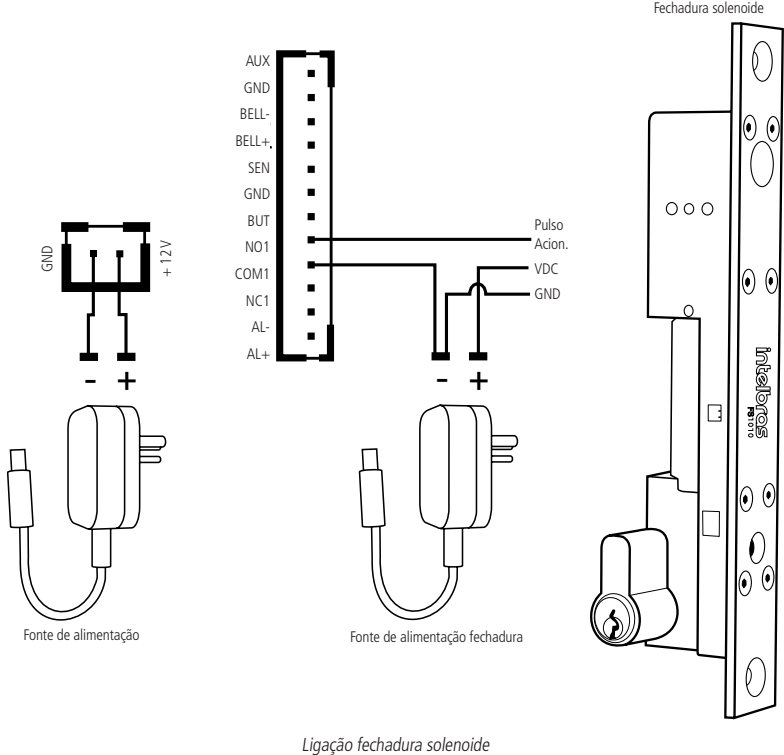
Obs.: caso a fechadura não possua sensor, desconsidere a ligação deste.

Nota: ao utilizar fechadura-eletrôimã de outro fabricante, utilize o diodo FR107 na ligação dela (circuito desmagnetizante).

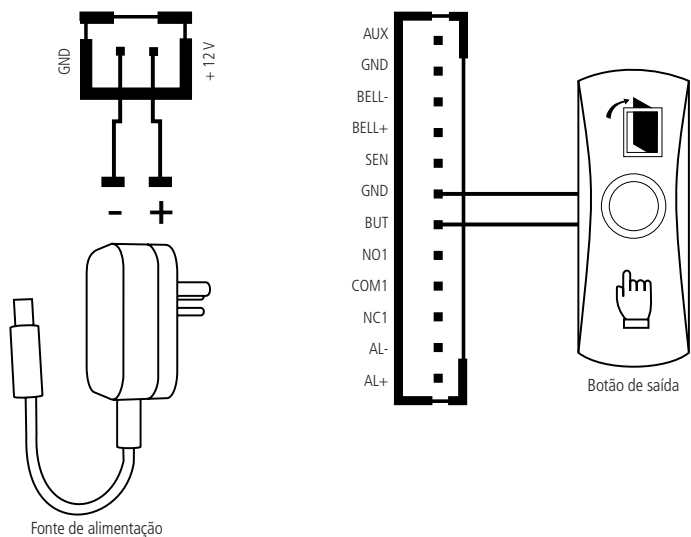
5.3. Fechadura elétrica



5.4. Fechadura solenoide

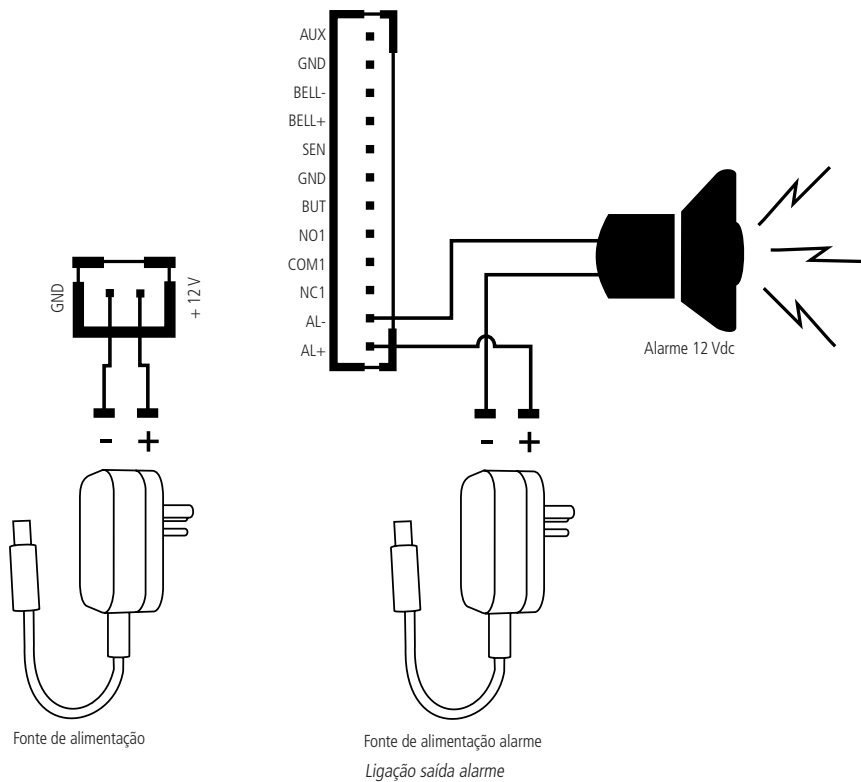


5.5. Botão de saída



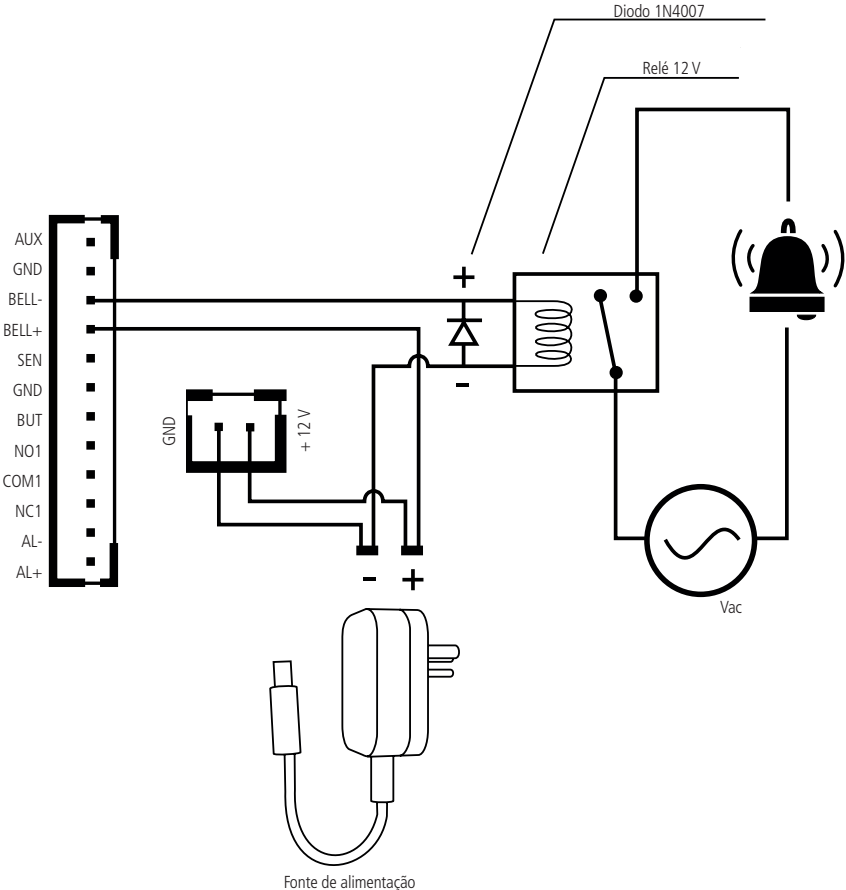
Ligação botão de saída

5.6. Saída alarme 12 V



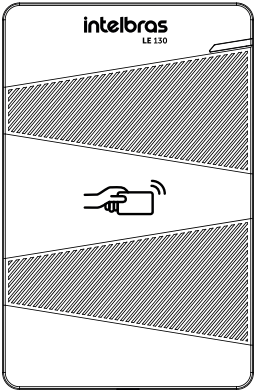
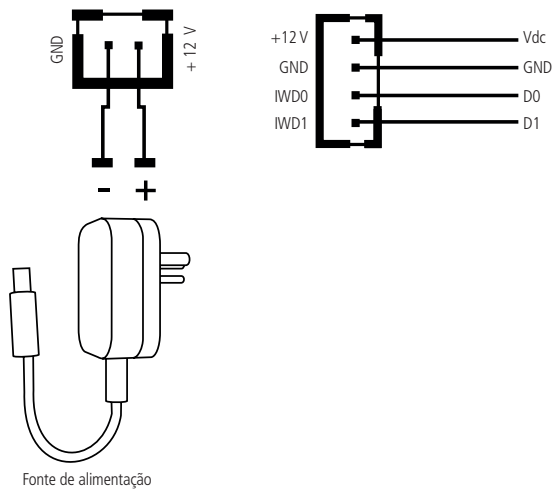
Ligação saída alarme

5.7. Campainha



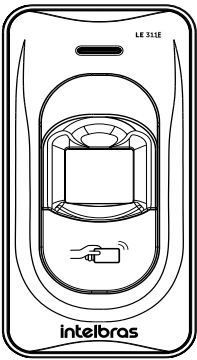
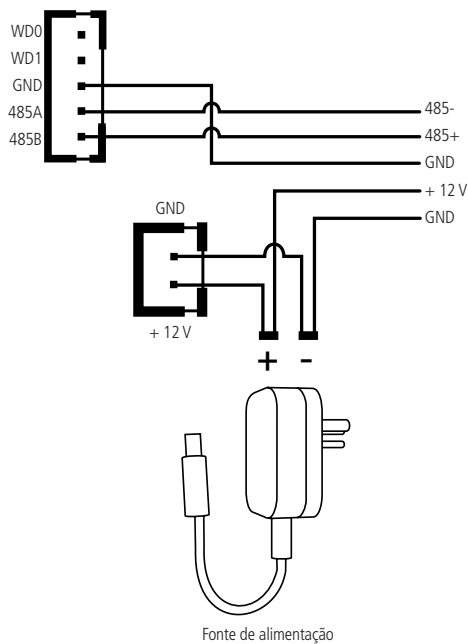
Ligação campainha 110/220 Vac

5.8. Leitor auxiliar



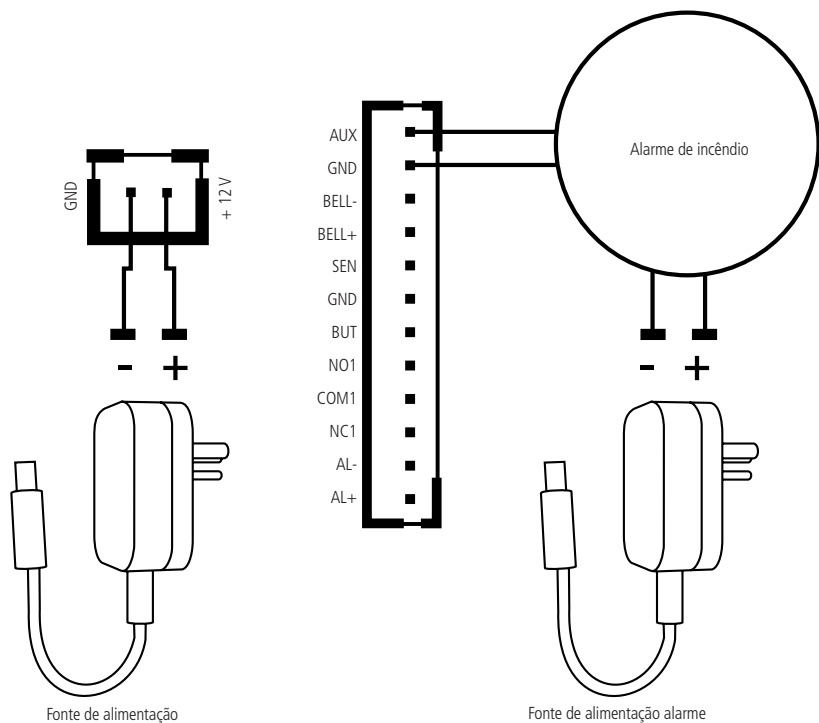
Ligação leitor auxiliar

5.9. Leitor LE 311



Ligação leitor LE 311

5.10. Entrada auxiliar



Ligação entrada auxiliar

6. Operações do sistema



Operações do sistema

6.1. Menu de programação

Pressione a tecla *Menu* para entrar no menu de programação.



Acessar o menu de programação

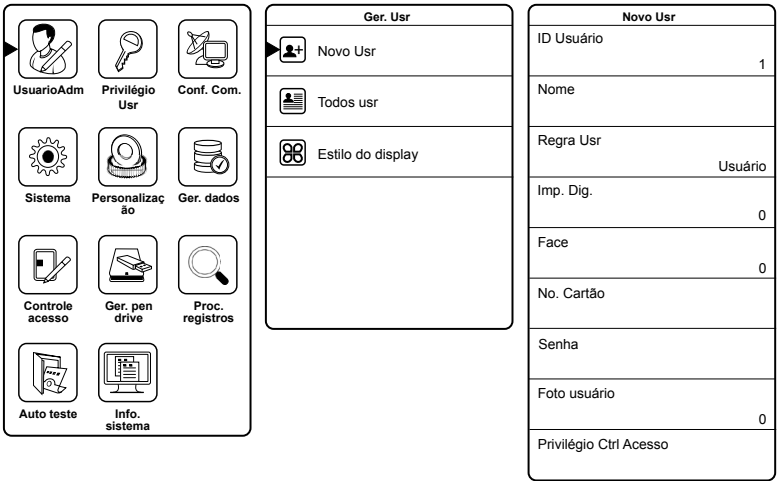
Atenção: para segurança do sistema de controle de acesso, é altamente recomendável o cadastro de uma senha ou um cartão-administrador para acesso ao menu de programação.

6.2. Usuário-adm

É possível importar usuários através do software ou de um pen drive. Para mais detalhes sobre como importar usuários para o equipamento através do software, consulte o manual do SoapAdmin 3.5. Para mais detalhes sobre importação de usuários através de um pen drive, consulte o item 6.11. *Gerenciamento pen drive>Enviar* deste manual.

Novo usuário

Para cadastrar usuários no equipamento, realize o seguinte procedimento.



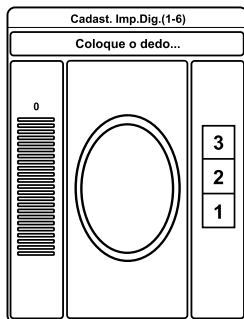
Cadastrar usuário

- » **ID usuário:** número de identificação do usuário, preenchido automaticamente.
- » **Nome:** vinculado ao número de identificação (não alterável).
- Obs.:** é possível alterar o nome através do software SoapAdmin3.5.

» **Regra Usr:** permite definir se o usuário terá perfil de usuário normal ou de administrador.

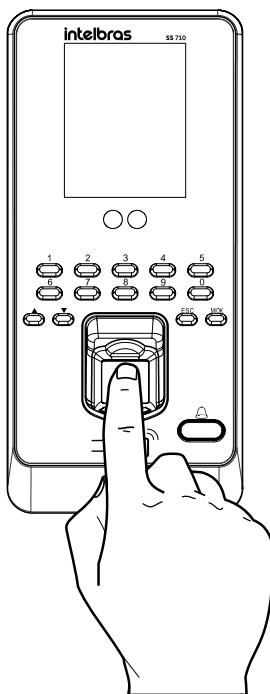
Ao utilizar o equipamento, é essencial definir um usuário-administrador, pois limita o acesso ao menu de programação. Apenas o administrador será responsável por cadastrar usuários e configurar o equipamento.

» **Impressão digital:** após selecionar o dedo a ser cadastrado, insira-o no leitor biométrico por três vezes, observando o procedimento descrito a seguir:



Cadastrar impressão digital

1. Posicione-se na frente do equipamento, coloque o dedo reto sobre o leitor biométrico e aguarde a confirmação de captura do template.



- » Não pressione demasiadamente o dedo no sensor biométrico, isso distorce a imagem da digital, não permitindo que o aparelho identifique os pontos formados pelas intersecções das linhas (cristas e vales) que compõem a digital.
- » Não posicione o dedo torto ou apenas a ponta do dedo no sensor biométrico. O uso inadequado do sensor biométrico no momento da leitura da digital impede que o sistema transmita uma imagem capaz de ser transformada em um template.



2. Ao ouvir um bipe, inserindo a digital, remova o dedo do leitor biométrico. Repita o processo mais duas vezes, totalizando três leituras consecutivas.



- » Não remova o dedo antes do bipe. Se isso ocorrer, a leitura poderá falhar e o processo de cadastro deverá ser refeito.
- » Não esqueça o dedo no leitor biométrico. Se o dedo for mantido no leitor após o bipe, o equipamento fará duas leituras consecutivas, e a terceira só será efetuada se o dedo for removido do leitor e reposicionado na sequência. Isso causará uma falha de leitura, pois a terceira captura será diferente das duas iniciais.

» Face

Para que o equipamento tenha um bom desempenho no reconhecimento biométrico facial, é necessário observar as instruções a seguir:

3. Antes de efetuar o cadastro facial, considere cadastrar o usuário com um dos outros métodos de verificação e anote o seu ID. Caso o cadastro seja feito a partir do *software SoapAdmin 3.5*, ele poderá ser nomeado, facilitando posteriormente sua identificação no dispositivo.
4. Existe restrição quanto ao uso de óculos de grau no cadastro/autenticação da face. Por este motivo, recomendamos não utilizar óculos durante o cadastro. Para os acessos, caso o equipamento não reconheça a face com o uso dos óculos, o usuário poderá retirá-lo no momento da verificação.
5. Disponha a pessoa a ser cadastrada à frente do equipamento, posicionando a face no centro da área verde, conforme a figura 1:

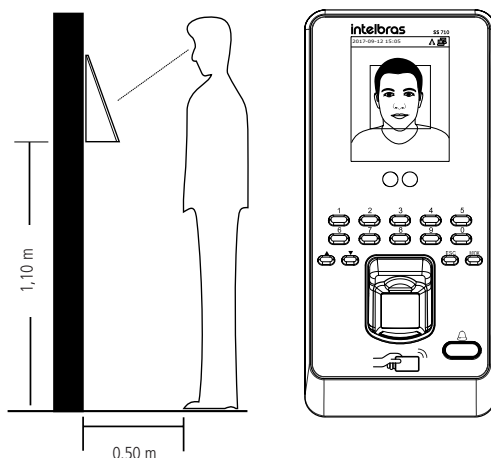





Figura 1


Obs.: essas cotas são para usuários com uma faixa de estatura entre 1,55 e 1,85 m. Para o cadastro de pessoas fora dessa faixa, sugerimos que se utilizem um dos outros métodos de autenticação disponíveis (biometria, senha ou RFID).


6. Inicie o cadastro da face conforme o procedimento:



UsuárioAdm



Priv. usuário



Conf. Com.



Sistema



Personalização



Ger. dados


Controle acesso



Ger. pen drive



Proc. registros



Auto teste


Info. sistema

Ger. Usr

 Novo Usr

 Todos usr

 Estilo do display

Novo Usr

ID Usuário

1

Nome

Perfil

Usuário

Imp. Dig.

0

Face

0

No. Cartão

Senha

Foto usuário

0

Priv. controle acesso

7. Ao seleccionar *Face*, será exibida a imagem da *figura 2*. Em seguida, a câmera irá mostrar a face do usuário a ser cadastrado, que deverá seguir as instruções de posicionamento conforme a *figura 3*. Serão feitas 3 capturas de tela, em 3 posições diferentes.

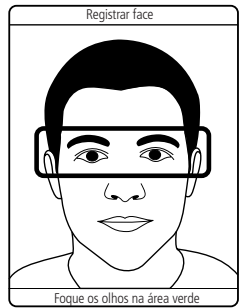


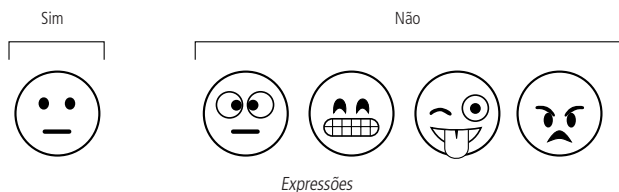
Figura 2

Observe a área que a face ocupa na tela do dispositivo, afastando-se levemente à medida que o posicionamento do retângulo verde muda na tela.

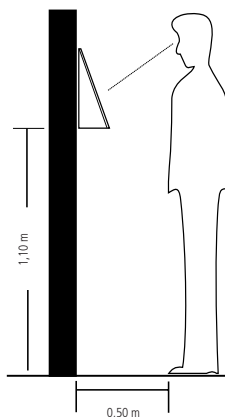


Figura 3

Obs.: no momento do cadastro facial, além de manter uma postura correta, evite o uso de expressões forçadas.



8. Finalizado o cadastro, teste o acesso respeitando a distância entre usuário e equipamento, conforme ilustração a seguir:
- » Posicione-se a 0,5 m do equipamento



- » Ao aproximar-se do dispositivo, este apresentará a imagem da pessoa a ser cadastrada na tela, sugerindo um enquadramento (em verde) para iniciar a busca do template no banco de dados do dispositivo (figura 4). Se o usuário estiver cadastrado, o equipamento irá liberar o acesso, confirmando o ID do usuário, o nome (caso editado no software SoapAdmin 3.5), o modo da verificação (Face) e a mensagem: *Verificado com sucesso!* Conforme a figura 5.

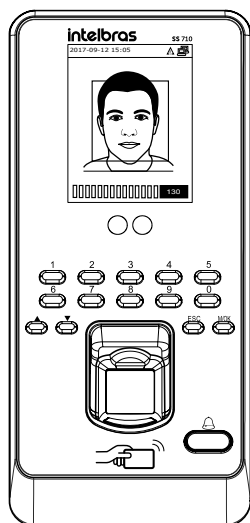


Figura 4

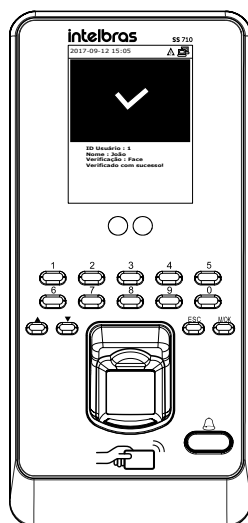
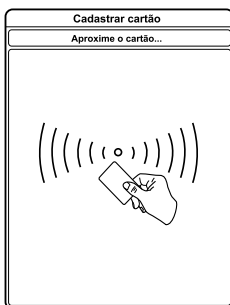


Figura 5

- » **No. cartão:** passe o cartão a ser cadastrado sobre o leitor.



Cadastrar cartão de proximidade

- » **Senha:** inserir senha que deve ter de três a seis dígitos. Depois confirme-a.
- » **Foto usuário:** capturar uma imagem do usuário.
- » **Priv. controle acesso:** definição do grupo, horário de acesso, modo de verificação e coação.

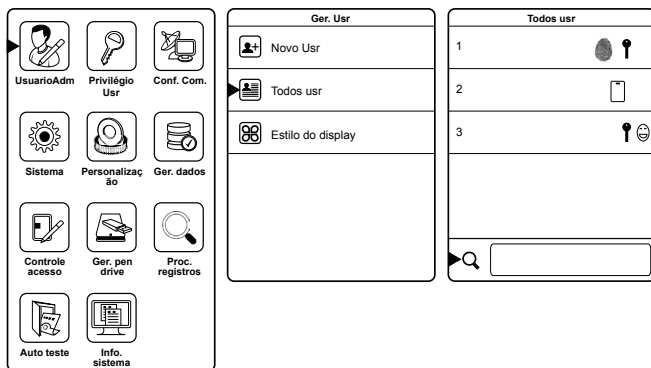
Controle acesso	
No. Grupo	1
Modo verific.	Aplicar config do grupo
Imp.Dig. Coação	Indefinido
Imp.Dig. Coação	<input type="button" value="ON"/>

Definir parâmetros para o usuário

- » **No. grupo:** definir número do grupo ao qual o usuário irá pertencer.
- » **Modo de verificação:** definir qual modo de autenticação o usuário irá usar para o acesso.
- » **Impressão digital coação:** definir impressão digital que será utilizada para coação.
- » **Aplicar horário do grupo:** ativar ou desativar horário do grupo para o usuário. Caso não queira utilizar o horário do grupo, é possível definir até três zonas de horário para o usuário.

Todos os usuários


Listar todos os usuários cadastrados no dispositivo, assim, é possível selecionar e editar ou excluir o usuário.




Editar ou excluir usuário

Estilo do display


Definir estilo do display ao listar os usuários.




UsuárioAdm




Privilegio
Usr




Conf. Com.




Sistema




Personalizaç
ão




Ger. dados




Controle
acesso




Ger. pen
drive



Proc.
registros





Auto teste




Info.
sistema

Ger. Usr

 Novo Usr

 Todos usr

 Estilo do display

Estilo do display



☒ Uma linha


☐ Múltiplas linhas



☐ Linhas mistas


1.

Todos usr

1



2


3






2.

Todos usr

1



2


3






3.

Todos usr

1

2


3




Definir estilo do display ao listar usuários

6.3. Privilegios usuário


Essa função é utilizada para definir os privilégios que o usuário-administrador terá sobre o equipamento.




UsuárioAdm




Privilegio
Usr




Conf. Com.




Sistema




Personalizaç
ão




Ger. dados




Controle
acesso




Ger. pen
drive



Proc.
registros





Auto teste




Info.
sistema

Privilegio Usr

 Usuário personalizado 1

 Usuário personalizado 2

 Usuário personalizado 3

Usuário personalizado 1

Habilitar atribuir permissões ☐ OFF

Nome
Usuário personalizado 1

Atribuir permissões

Definir privilégios do usuário-administrador


















21

- » **Habilitar atribuir permissões:** habilitar as atribuições definidas para o usuário-administrador.
- » **Nome:** nome do usuário (não alterável).
- » **Atribuir permissões:** selecionar, da lista de atribuições, o conteúdo que o usuário-administrador terá sobre o equipamento.

6.4. Sistema

Data e hora


















Configurações de data, hora e horário de verão.

Sistema	Data e hora
<div> <div>  <p>UsuarioAdm</p> </div> <div>  <p>Privilegio Usr</p> </div> <div>  <p>Conf. Com.</p> </div> </div> <div> <div>  <p>Sistema</p> </div> <div>  <p>Personaliza ção</p> </div> <div>  <p>Ger. dados</p> </div> </div> <div> <div>  <p>Controle acesso</p> </div> <div>  <p>Ger. pen drive</p> </div> <div>  <p>Proc. registros</p> </div> </div> <div> <div>  <p>Auto teste</p> </div> <div>  <p>Info. sistema</p> </div> </div>	<div> <div>  <p>Data e hora</p> </div> <div>  <p>Gerenciamento de eventos</p> </div> <div>  <p>Face</p> </div> <div>  <p>Imp.Dig.</p> </div> <div>  <p>Resetar</p> </div> <div>  <p>Atualização USB</p> </div> </div>
	<div> <div> <p>Conf. Data</p> <p>01/01/16</p> </div> <div> <p>Conf. Hora</p> <p>16:00:43</p> </div> <div> <p>Formato 24h</p> <p><input checked="" type="checkbox"/> ON <input type="checkbox"/></p> </div> <div> <p>Formato data</p> <p>DD/MM/YY</p> </div> <div> <p>Horário verão</p> <p><input type="checkbox"/> OFF <input checked="" type="checkbox"/></p> </div> </div>

Configuração de data e hora

Configuração de registro de eventos

Nesta função é possível configurar os eventos gerados pelos usuários.

Sistema	Gerenciamento de eventos
<div> <div>  <p>UsuarioAdm</p> </div> <div>  <p>Privilegio Usr</p> </div> <div>  <p>Conf. Com.</p> </div> </div> <div> <div>  <p>Sistema</p> </div> <div>  <p>Personaliza ção</p> </div> <div>  <p>Ger. dados</p> </div> </div> <div> <div>  <p>Controle acesso</p> </div> <div>  <p>Ger. pen drive</p> </div> <div>  <p>Proc. registros</p> </div> </div> <div> <div>  <p>Auto teste</p> </div> <div>  <p>Info. sistema</p> </div> </div>	<div> <div>  <p>Data e hora</p> </div> <div>  <p>Gerenciamento de eventos</p> </div> <div>  <p>Face</p> </div> <div>  <p>Imp.Dig.</p> </div> <div>  <p>Resetar</p> </div> <div>  <p>Atualização USB</p> </div> </div>
	<div> <div> <p>Tempo nova marcação(m)</p> <p>Nenhum</p> </div> <div> <p>Mostra foto usuário</p> <p><input checked="" type="checkbox"/> ON <input type="checkbox"/></p> </div> <div> <p>Log Alerta</p> <p>Desabilitado</p> </div> <div> <p>Ciclo exclusão de dados</p> <p>999</p> </div> <div> <p>Atraso de tela (s)</p> <p>3</p> </div> <div> <p>Inter. ver. face(s)</p> <p>0</p> </div> <div> <p>Salva registros de ver. inválida</p> <p><input type="checkbox"/> OFF <input checked="" type="checkbox"/></p> </div> </div>

Configuração de registros de eventos

- » **Tempo nova marcação (m):** definir tempo, em minutos, em que o equipamento não irá registrar eventos duplicados.
- » **Mostra foto usuário:** ativar ou desativar o aparecimento da foto do usuário ao autenticar-se no equipamento.
- » **Log alerta:** quando o número de eventos restantes for menor que o valor definido, o equipamento emitirá um alarme informando que o espaço de armazenamento está quase cheio.
- » **Ciclo exclusão de dados:** número de eventos que será permitido excluir quando o número armazenado alcançar seu valor máximo.

- » **Atraso de tela:** tempo em segundos que um evento do tipo *Acesso liberado* permanecerá na tela.
- » **Intervalo verificação face (s):** definir intervalo de tempo, em segundos, entre a comparação da mesma face.
- » **Salva registros de verificação inválida:** armazenar, ou não, os eventos de acesso negado.

Face

Configurações da leitura da impressão facial.

Sistema	Face
Data e hora	Limiar 1:1 75
Gerenciamento de eventos	Limiar 1:N 82
Face	Detectar rosto falso <input checked="" type="checkbox"/>
Imp.Dig.	Exposição 300
Resetar	Qualid. 80
Atualização USB	

Configuração da leitura biométrica facial

- » **Limiar¹ 1:1:** na verificação 1:1, o acesso liberado acontecerá somente quando a face verificada e a face do usuário forem maiores do que o valor inserido.
- » **Limiar¹ 1:N:** na verificação 1:N, o acesso liberado acontecerá somente quando a face verificada e a face de todos os usuários registrados forem maiores do que o valor inserido.
- » **Detectar rosto falso:** ativar ou não a detecção de rosto falso.
- » **Exposição:** definir o valor da exposição da câmera.
- » **Qualidade:** definir qualidade máxima da imagem. Quando a qualidade da imagem for maior do que esse valor, o dispositivo recebe essa imagem facial e inicia um processamento de um algoritmo. Caso contrário, o dispositivo filtra essa imagem facial. O valor-padrão é 80.

¹ Quanto maior o valor inserido para limiar, maior será a falsa rejeição do dispositivo.

Impressão digital

Configurações da leitura da impressão digital.

Sistema	Imp.Dig.
Data e hora	Limiar 1:1 15
Gerenciamento de eventos	Limiar 1:N 35
Face	Sensibilidade sensor Baixa
Imp.Dig.	Num. tentativas 3
Resetar	Imagem Imp.Dig. Mostrar Ambos
Atualização USB	

Configuração da leitura biometria digital

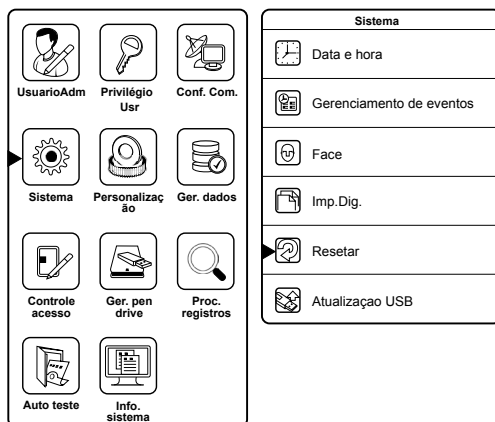
- » **Limiar¹ 1:1:** na verificação 1:1, o acesso liberado acontecerá somente quando a digital verificada e a digital do usuário forem maiores do que o valor inserido.
- » **Limiar¹ 1:N:** na verificação 1:N, o acesso liberado acontecerá somente quando a digital verificada e a digital de todos os usuários registrados forem maiores do que o valor inserido.
- » **Sensibilidade sensor:** definir sensibilidade do sensor biométrico. É recomendável a utilização do valor médio. Quando o ambiente for seco, resultando em uma captura mais lenta recomenda-se o valor alto. E quando o ambiente for úmido, tornando uma captura difícil, recomenda-se o valor baixo.
- » **Número de tentativas:** para diminuir o processo de reinsertir o número do usuário na verificação 1:1 ou senha ao inserir uma digital não cadastrada ou ao digitar uma senha erroneamente, é possível definir um número de tentativas em que o equipamento copiará esse número.
- » **Imagem impressão digital:** selecionar se a imagem da impressão digital aparecerá no display ao autenticar-se.

¹ Quanto maior o valor inserido para limiar, maior será a falsa rejeição do dispositivo.

Resetar

Função utilizada para retomar todas as configurações para os padrões de fábrica, como configuração de porta, alarme de coação, anti-passback, parte de comunicação do equipamento e configurações do sistema (volume, voz, teclado, entre outros).

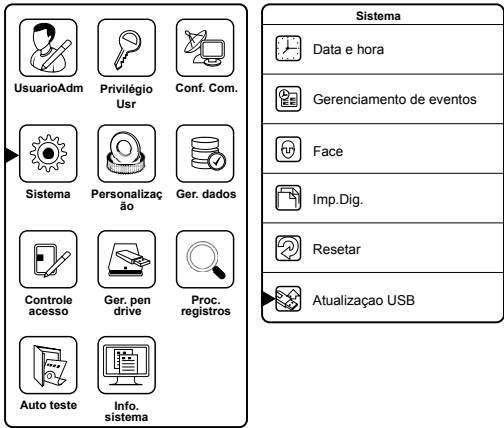
Obs.: esta função não afeta usuário cadastrado, data e hora.



Reset configurações de fábrica

Atualização USB

Função utilizada para atualizar firmware do equipamento via USB. Para realizar a atualização, conecte o pen drive com o arquivo de atualização no equipamento e execute a função.

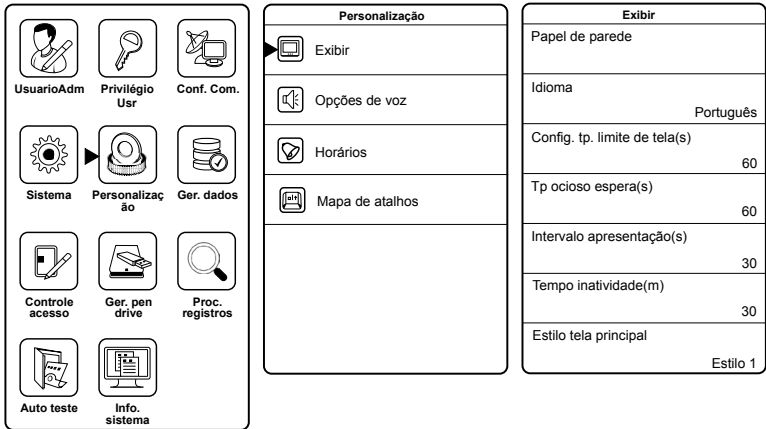


Atualização firmware

6.5. Personalização

Exibir

Configurações de tela

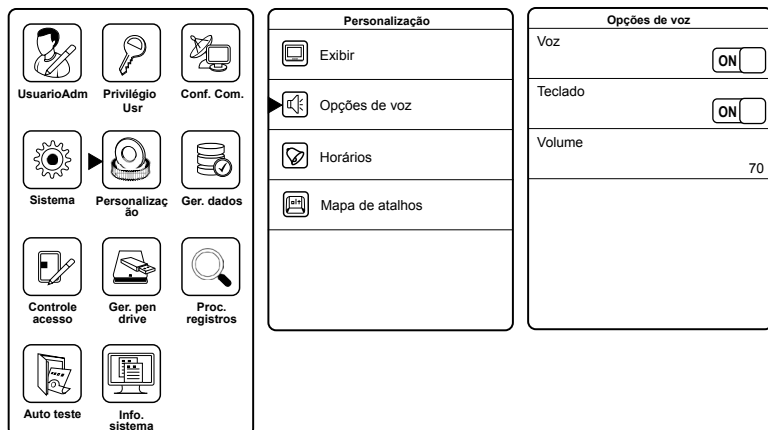


Configurações de tela

- » **Papel de parede:** definir papel de parede da tela principal.
Obs.: é possível enviar fotos para o equipamento e definir como papel de parede. Para mais informações consulte o tópico 6.11. Gerenciamento pen drive>Enviar.
- » **Idioma:** definir idioma do equipamento.
- » **Configuração tempo limite de telas:** tempo máximo em segundos de inatividade em telas do menu de programação, definido para o equipamento retornar à tela principal.
Obs.: caso a opção Desabilitado seja definida, o equipamento não sairá do menu de programação por inatividade.
- » **Modo de espera (s):** tempo máximo em segundos de inatividade na tela principal, definido para o equipamento iniciar a apresentação do descanso de tela.

- » **Intervalo apresentação (s):** tempo em segundos de intervalo entre as imagens do descanso de tela.
- » **Tempo inatividade (m):** tempo em minutos de inatividade para o equipamento entrar em modo *Stand by*.
- » **Estilo tela principal:** estilo da tela principal.

Opções de voz



Opções de voz

- » **Voz:** ativar ou desativar voz do equipamento.
- » **Teclado:** ativar ou desativar sons do teclado.
- » **Volume:** volume do equipamento.

Horários

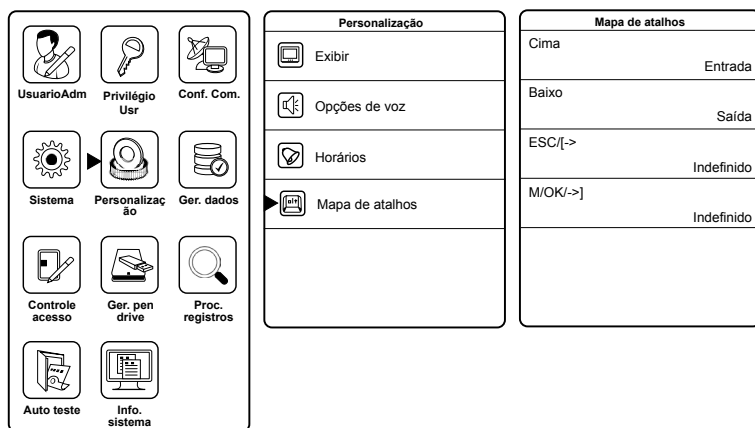
Essa função está indisponível.

Configurar status de evento

Essa função está indisponível.

Mapa de atalhos

Nessa função é permitido definir atalhos para as teclas de navegação.




Definir atalhos para teclas


6.6. Gerenciamento de dados


Essa função é utilizada para gerenciar os dados do equipamento, excluir ou realizar backup.


Apagar dados


Função utilizada para excluir registros.



UsuárioAdm



Privilegio
Usr



Conf. Com.



Sistema



Personalizaç
ão



Ger. dados


Controle
acesso



Ger. pen
drive



Proc.
registros



Auto teste


Info.
sistema

Ger. dados

 Apagar dados

 Backup dados

 Restaurar dados

Apagar dados

Apagar eventos

Apagar tudo

Apagar priv. Admin

Apag. Dados acesso

Apagar foto usr.

Apagar papel de parede

Apagar prot. Tela


Excluir dados Backup


Apagar dados


- » **Apagar log evento:** exclui eventos dos usuários.
- » **Apagar tudo:** exclui todos os dados (usuários, eventos, opções de acesso, entre outros).
- » **Apagar privacidade administrador:** exclui a privacidade do administrador no dispositivo, fazendo com que ele se torne um usuário comum.
- » **Apagar dados acesso:** exclui as opções de acesso (grupos, zonas de horário, configuração coação).
- » **Apagar foto usuário:** exclui as fotos dos usuários.
- » **Apagar papel de parede:** exclui papéis de paredes do equipamento.
- » **Apagar proteção de tela:** exclui proteções de tela do equipamento.
- » **Excluir dados backup:** exclui dados de backup.


Backup dados


Realizar backup dos dados presentes no equipamento.



UsuárioAdm



Privilegio
Usr



Conf. Com.



Sistema



Personalizaç
ão



Ger. dados


Controle
acesso



Ger. pen
drive



Proc.
registros



Auto teste


Info.
sistema

Ger. dados

 Apagar dados

 Backup dados

 Restaurar dados

Backup dados

Backup para dispositivo

Backup para pen-drive

Backup de dados

- » **Backup para dispositivo:** realiza backup dos dados do dispositivo para o dispositivo.
- » **Backup para pen drive:** realiza backup dos dados do dispositivo para um pen drive.

Restaurar dados

Restaura os dados em backup para o equipamento.

	Ger. dados	Restaurar dados
	Apagar dados	Restaurar do dispositivo
	Backup dados	Restaurar do pen-drive
	Restaurar dados	

Restauração de dados

- » **Restaurar do dispositivo:** restaura os dados em backup realizados no equipamento.
- » **Restaurar do pen drive:** restaura os dados em backup realizados no pen drive.

6.7. Controle acesso

Configuração de porta

Configurar parâmetros de porta


	Controle de Acesso	Conf. porta
	Opc. controle acesso	Tempo abertura porta(s) 10
	Conf. zona de tempo	Atraso do Sensor(s) 10
	Conf. feriado	Tipo de sensor Normal aberto(NA)
	Conf. grupo	Atraso alarme(s) 30
	Aces.Comb.Grupos	Recorrência negação 3
	Conf. Anti-Passback	Tempo NF Nenhum
	Alarme coação	Tempo NA Nenhum
		Config. de entrada auxiliar
		Verificar por RS485 Somente Imp.Dig
		Feriados válidos <input type="checkbox"/> OFF
		Alarme <input type="checkbox"/> OFF
	Reset Config. Acesso	

Configurações de porta

- » **Tempo abertura porta (s):** tempo em segundos de porta aberta ao realizar acesso.
- » **Atraso do sensor (s):** tempo em segundos para o sensor realizar a leitura do estado da porta.
- » **Tipo de sensor:** tipo de sensor de porta utilizado (NA ou NF).
- » **Atraso alarme (s):** tempo em segundos para acionamento do alarme do sensor de porta.
- » **Recorrência de negação:** função recorrência de negação. Quantidade de acessos negados para acionamento do alarme.
- » **Tempo NF:** zona de horário em que o dispositivo ficará fechado, ou seja, ninguém terá acesso liberado.
- » **Tempo NA:** zona de horário em que o dispositivo permanecerá com a porta aberta.
- » **Configuração de entrada auxiliar:** definir ação da entrada auxiliar no equipamento.
 - » **Saída auxiliar/tempo de abertura (s):** tempo em que permanecerá acionado.
 - » **Configurar tipos de abertura:** tipos de abertura.
- » **Verificar por RS485:** definir o(s) método(s) que o leitor auxiliar irá operar.
- » **Feriados válidos:** ativar ou desativar feriados para o dispositivo.
- » **Alarme:** ativar ou desativar o alarme antiarrombamento.
- » **Reset configurações de acesso:** reset, para os padrões de fábrica, das configurações de porta.

Configuração zona de tempo


Configurar zonas de tempo para acesso dos usuários.




UsuarioAdm

Privilegio


Usr



Conf. Com.




Sistema




Personalizaç

ão




Ger. dados




Controle

acesso




Ger. pen

drive




Proc.

registros




Auto teste




Info.

sistema


Controle acesso




Conf. porta




Conf. zona de tempo




Conf. feriado




Conf. grupo



Aces.Comb.Grupos



Conf. Anti-Passback



Alarme coação

Conf. zona tempo:01 / 50

Domingo	00:00	23:59
Segunda	00:00	23:59
Terça	00:00	23:59
Quarta	00:00	23:59
Quinta	00:00	23:59
Sexta	00:00	23:59
Sábado	00:00	23:59
<div> <div>Buscar horários (1-50)</div> <div>1</div> </div>		


Configurações de zonas de tempo

- » **Buscar horários (1-50):** nesse campo é inserido o número da zona de tempo que se deseja mexer, ou seja, primeiro insira o número da zona e depois configure os horários.


29

Configurar feriado


Esta função é utilizada para negar o acesso dos usuários, mesmo com permissão ou zona de tempo cadastrados, em feriados, inicialmente agendados, em que o ambiente controlado estará fechado sem o desejo de que o mesmo seja frequentado.




UsuárioAdm




Privilegio
Usr




Conf. Com.




Sistema




Personalizaç
ão




Ger. dados




Controle
acesso




Ger. pen
drive



Proc.
registros




Auto teste




Info.
sistema


Controle de ACESS




Conf. porta




Conf. zona de tempo




Conf. feriado




Conf. grupo



Aces.Comb.Grupos



Conf. Anti-Passback



Alarme coação

Conf. feriado

Adic. feriado

Todos feriados


Configurações de feriado

- » **No:** número do feriado.
- » **Data inicial:** data em que o feriado inicia.
- » **Data final:** data em que o feriado termina.
- » **Função horária:** determinar zona de tempo para o feriado.


Configurar grupo

É possível cadastrar e configurar grupos e associar aos usuários para diferenciação de zona de tempo, ativação de feriados e métodos de autenticação.


Obs.: caso o cadastro de mais grupos seja necessário, além do grupo-padrão, uma combinação de acesso deverá ser preenchida, impreterivelmente (ver item 6.7. Controle acesso>Acesso combinado>Exemplo 2).




UsuárioAdm




Privilegio
Usr




Conf. Com.




Sistema




Personalizaç
ão




Ger. dados




Controle
acesso




Ger. pen
drive



Proc.
registros




Auto teste




Info.
sistema


Controle acesso




Conf. porta




Conf. zona de tempo




Conf. feriado




Conf. grupo



Aces.Comb.Grupos



Conf. Anti-Passback



Alarme coação

Conf. grupo

Novo grupo

Todos grupos


Configurações de grupo de usuário


- » **No:** número do grupo.
- » **Modo verificação:** métodos de autenticação que o grupo irá utilizar.
- » **Zona de tempo:** definir até três zonas de tempo para o grupo.
- » **Incluir feriados:** ativar ou desativar feriados para o grupo.


30


Acesso combinado entre grupos (usuários)


Esta função é utilizada para dar permissão aos grupos no equipamento em forma de acesso combinado entre usuários. É possível definir até cinco usuários, do mesmo grupo ou de grupos diferentes, para realizar um acesso combinado. Para cada grupo cadastrado é necessário incluir uma permissão na tela *Aces.comb.grupo*, mesmo que não haja combinação de acesso.



UsuarioAdm



Privilegio
Usr



Conf. Com.



Sistema



Personalizaç
ão



Ger. dados


Controle
acesso



Ger. pen
drive



Proc.
registros



Auto teste



Info.
sistema


Controle acesso


 Conf. porta


 Conf. zona de tempo

 Conf. feriado

 Conf. grupo


 Aces.Comb.Grupos

 Conf. Anti-Passback

 Alarme coação

Aces.Comb.Grupos

1	01 00 00 00 00
2	00 00 00 00 00
3	00 00 00 00 00
4	00 00 00 00 00
5	00 00 00 00 00




Configuração de acesso do grupo

Veja um exemplo do acesso combinado já cadastrado por padrão de fábrica.


Exemplo 1:

Aces.Comb.Grupos


1	01 00 00 00 00
---	----------------




Aces.Comb.Grupos





1







0







0






0





0



1

2

3

4

5

Confirma (OK)

Cancela(ESC)

Exemplo combinação de acesso

A combinação 1 está preenchida apenas com o grupo número 1, e o resto está vazio (00), ou seja, não há combinação de acesso. Assim, é necessário apenas um usuário do grupo 1 para abrir a porta.

Exemplo 2:

Caso um grupo número 2 seja cadastrado e se deseje realizar o acesso normalmente, sem combinar acesso, é necessário preencher uma combinação para o grupo. Veja:

Aces.Comb.Grupos

2

02 00 00 00 00

2

2

Aces.Comb.Grupos

2

0

0

0

0

12345

Confirma (OK)Cancela(ESC)

Exemplo combinação de acesso

A combinação 2 está preenchida apenas com o grupo número 2, e o resto está vazio (00). Assim, é necessário apenas um usuário do grupo 2 para abrir a porta.

Exemplo 3:

Supondo que um grupo número 3 seja cadastrado e que se deseje que dois usuários do grupo 3, um do grupo 2 e um do grupo 1 sejam necessários para abrir a porta, os parâmetros são preenchidos da seguinte forma:

Aces.Comb.Grupos

3

03 03 02 01 00

3

3

Aces.Comb.Grupos

3

3

2

1

0

12345

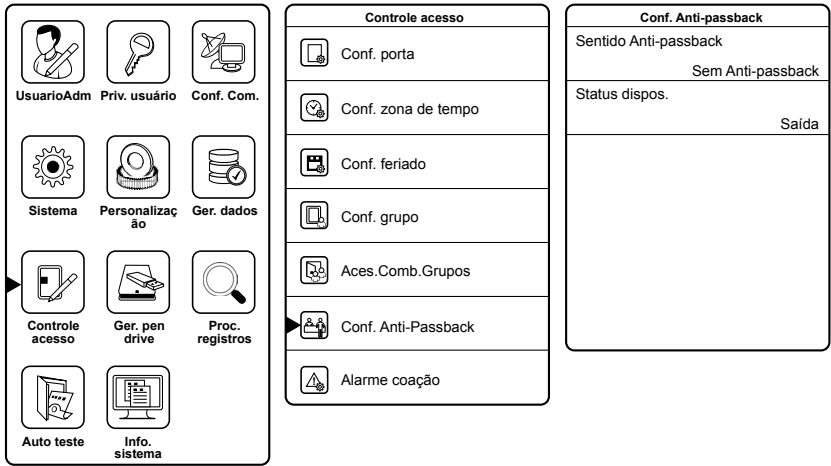
Confirma (OK)Cancela(ESC)

Exemplo combinação de acesso

A combinação 3 está preenchida com o grupo número 3 (duas vezes), com o grupo número 2 e o grupo número 1. Assim, serão necessários, respectivamente, dois usuários do grupo 3, um usuário do grupo 2 e um usuário do grupo 1 para abrir a porta.

Configurar anti-passback

Para evitar que pessoas fiquem seguindo outros usuários para entrar em uma porta sem verificação, resultando em um problema na segurança do ambiente, o equipamento fornece a opção *Anti-passback*. Esta função requer a utilização do SS 710 com um leitor escravo.





Configurar anti-passback


- » **Sentido anti-passback:** definir sentido em que será aplicado o anti-passback.
- » **Sem anti-passback:** anti-passback desabilitado.
- » **Anti-passback saída:** depois de um evento de saída, somente depois de um evento de entrada que o usuário poderá sair novamente. Caso contrário, o alarme será ativado.
- » **Anti-passback entrada:** depois de um evento de entrada, somente depois de um evento de saída que o usuário poderá entrar novamente. Caso contrário, o alarme será ativado.
- » **Anti-passback entrada/saída:** independentemente do evento, o usuário só poderá entrar depois de um evento de saída, e só poderá sair depois de um evento de entrada.
- » **Nulo e salvar:** função *Anti-passback* desabilitada, porém é registrado.
- » **Status dispositivo:** definir tipo de evento do dispositivo.
- » **Nenhum:** desativa função *Anti-passback*.
- » **Saída:** definir acesso no dispositivo como evento de saída.
- » **Entrada:** definir acesso no dispositivo como evento de entrada.


Alarme coação


A opção de coação permite que o usuário ative a função com o intuito de solicitar ajuda ao ser coagido, acionando um alarme externo.



UsuarioAdm



Privilegio
Usr



Conf. Com.



Sistema



Personalizaç
ão



Ger. dados


Controle
acesso



Ger. pen
drive



Proc.
registros



Auto teste



Info.
sistema


Controle acesso


 Conf. porta


 Conf. zona de tempo

 Conf. feriado

 Conf. grupo

 Aces.Comb.Grupos

 Conf. Anti-Passback

 Alarme coação

Alarme coação

Função coação

☐ OFF

1:1 Gatilho

☐ OFF

1:N Gatilho

☐ OFF

Senha de alarme

☐ OFF

Atraso alarme(s)


10


Configurar alarme coação


- » **Função coação:** ativar alarme de coação através da tecla menu (->]) de coação mais a autenticação com biometria. Para isso ative a função coação, em seguida vá no menu *Mapa de atalhos* (ver item 6.5. *Personalização>Mapa de atalhos*) e defina a tecla M/OK/->] para coação. Assim, para acionar o alarme, basta pressionar a tecla de coação e realizar o acesso com qualquer biometria cadastrada.
- Obs.:** para acessar o menu do equipamento com a tecla de coação ativada, mantenha pressionado a tecla Menu.
- » **1:1 Gatilho:** na verificação 1:1, o alarme é ativado através da biometria de coação selecionada pelo usuário.
- » **1:N Gatilho:** na verificação 1:N, o alarme é acionado através de qualquer biometria cadastrada pelo usuário.
- » **Senha de alarme:** ativar alarme de coação através da senha cadastrada pelo usuário.
- » **Atraso alarme (s):** tempo em segundos de espera para acionar o alarme de coação.


6.8. Procurar registros


Consulta de eventos de acesso no equipamento:



UsuarioAdm



Privilegio
Usr



Conf. Com.



Sistema



Personalizaç
ão



Ger. dados


Controle
acesso


Ger. pen
drive


Proc.
registros


Auto teste


Info.
sistema

ID Usuário

Introduza(consultar todos)


Confirma (OK)


Cancela(ESC)


Consulta de eventos


6.9. Autoteste


O equipamento realiza um autoteste para conferir sua tela, seus áudios, câmera, sensor biométrico, entre outros.



UsuarioAdm



Privilégio
Usr



Conf. Com.



Sistema



Personalizaç
ão



Ger. dados









Controle
acesso


Ger. pen
drive


Proc.
registros


Auto teste



Info.
sistema


Auto teste	
	Testar todos
	Teste LCD
	Teste áudio
	Teste teclado
	Teste sensor Imp. Dig.
	Teste câmera
	Teste relógio


Autoteste


6.10. Informações do sistema


Consulta das informações do sistema, desde versão de firmware e fabricante até a capacidade de armazenamento de dados:



UsuarioAdm



Privilégio
Usr



Conf. Com.



Sistema



Personalizaç
ão



Ger. dados





Controle
acesso


Ger. pen
drive


Proc.
registros


Auto teste


Info.
sistema

Info. sistema	
	Capacidade
	Inf. dispositivo
	Inf. Firmware


Consulta das informações do equipamento


6.11. Gerenciamento pen drive


Para realizar as funções que utilizam o pen drive (download e upload de dados), este deve estar conectado no equipamento.


Baixar


Baixar informações do equipamento para o pen drive.



UsuarioAdm



Privilégio
Usr



Conf. Com.



Sistema



Personalizaç
ão



Ger. dados


Controle
acesso



Ger. pen
drive



Proc.
registros



Auto teste


Info.
sistema

Ger. pen drive

 Baixar

 Enviar

 Configuração

Baixar

Baixar reg. Evento

Baixar usuários


Baixar fotos usr.


Baixar dados do equipamento para o pen drive


- » **Baixar eventos:** baixar eventos de acesso.
- » **Baixar usuários:** baixar para o pen drive os usuários cadastrados no equipamento.
- » **Baixar fotos usuários:** baixar para o pen drive as fotos dos acessos liberados.


Enviar


Enviar dados do pen drive para o equipamento.



UsuarioAdm



Privilégio
Usr



Conf. Com.



Sistema



Personalizaç
ão



Ger. dados


Controle
acesso



Ger. pen
drive



Proc.
registros



Auto teste


Info.
sistema

Ger. pen drive

 Baixar

 Enviar

 Configuração

Enviar

Enviar dados usr.

Enviar foto

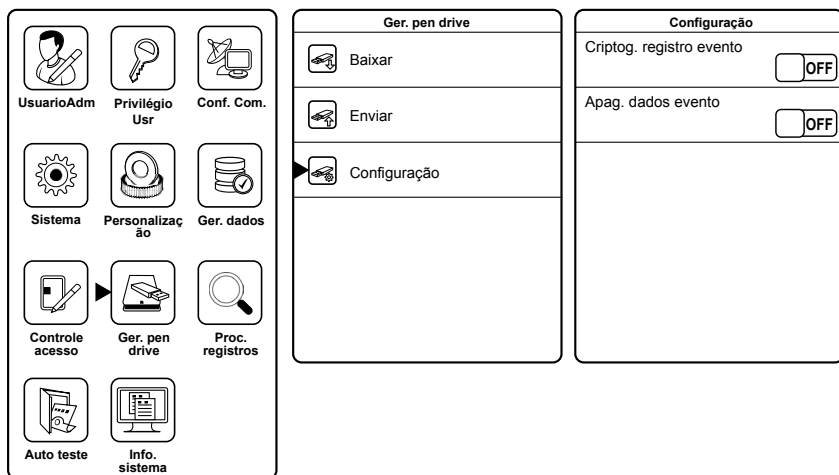
Proteção de tela

Papel de parede

Enviar dados do pen drive para o equipamento

- » **Enviar dados dos usuários:** envia para o equipamento os usuários armazenados no pen drive.
- » **Enviar foto:** envia para o equipamento as fotos dos usuários.
Obs.: é necessário criar uma pasta com o nome Photo e inserir os arquivos de imagem nela. Cada imagem deve conter o número de ID do usuário ao qual está ou estará associada. É permitido até oito mil fotos e cada foto não poderá exceder o tamanho de 15 kB.
- » **Proteção de tela:** envia para o equipamento as fotos de proteção de tela armazenadas no pen drive. É possível selecionar ou enviar todas as fotos do pen drive.
Obs.: é necessário criar uma pasta com o nome Advertise e inserir os arquivos de imagem nela. É permitido até vinte fotos e cada foto não poderá exceder o tamanho de 30 kB.
- » **Papel de parede:** envia para o equipamento as fotos de papel de parede armazenadas no pen drive. É possível selecionar ou enviar todas as fotos do pen drive.
Obs.: é necessário criar uma pasta com o nome wallpaper e inserir os arquivos de imagem nela. É permitido até vinte fotos e cada foto não poderá exceder o tamanho de 30 kB.

Configuração



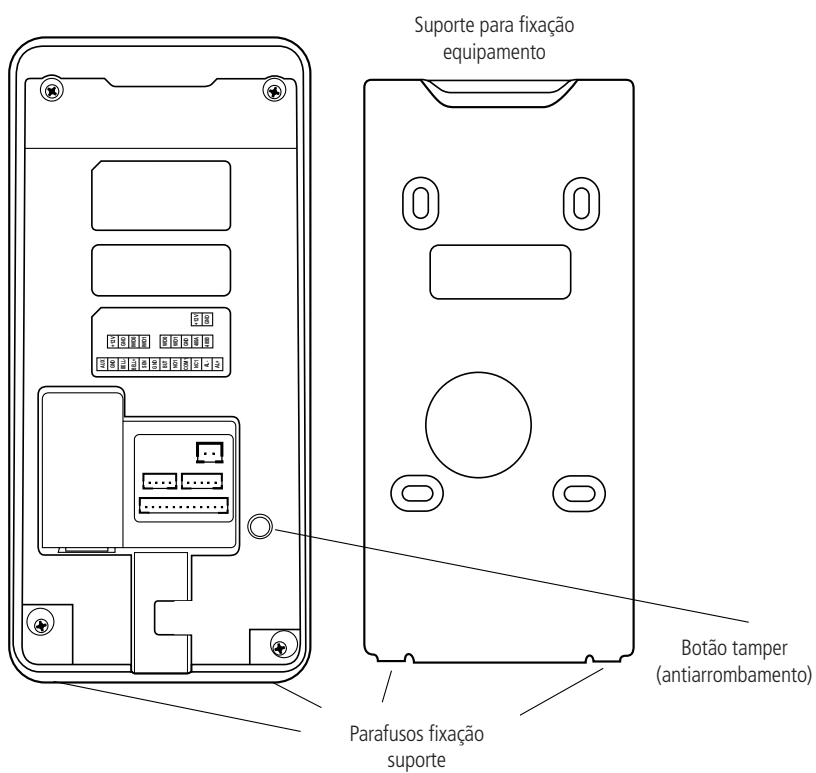
Configurações de gerenciamento

- » **Criptografia registro evento:** função indisponível.
- » **Apagar dados evento:** apagar dados de acesso ao ser transferidos para o pen drive.

6.12. Reset administrador

Caso o usuário administrador seja esquecido, ou tenha sua chave perdida, realize o seguinte processo para acessar o menu do equipamento e reconfigurar o usuário administrador:

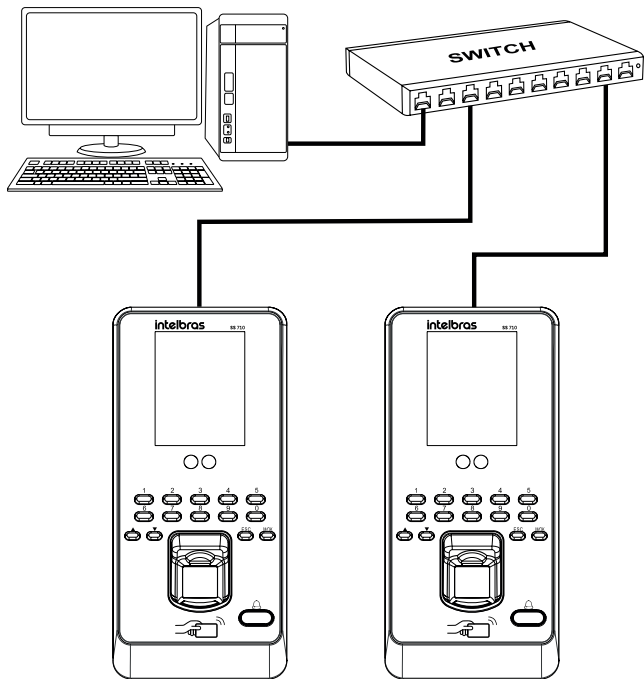
1. Desligue o equipamento;
2. Retire o suporte de fixação do equipamento da parede;
3. Mantenha o botão *Tamper* pressionado e ligue o dispositivo;
4. Após o equipamento iniciar (tela principal), solte o botão *Tamper* e aguarde trinta segundos;
5. Após trinta segundos acesse o menu de programação e reconfigure o usuário administrador conforme o item 6.2 do manual do usuário. Com o usuário administrador restabelecido as demais configurações podem ser alteradas.



7. Comunicação do equipamento

7.1. Configurar comunicação

TCP/IP



Ligação Ethernet

Configurar parâmetros de rede Ethernet

UsuarioAdm

Privilegio
Usr

Conf. Com.

Sistema

Personaliza
ção

Ger. dados

Controle
acesso

Ger. pen
drive

Proc.
registros

Auto teste

Info.
sistema

Conf. Com.

TCP/IP

Serial Comm

Conf. Comunic.

Conf. wiegand

TCP/IP

Ender.IP

192.168.1.201

Masc. Rede

255.255.255.0

Gateway

192.168.1.254

DNS

0.0.0.0

Porta de comu.TCP

4370

DHCP

OFF

Mostrar na barra status

ON

Configurar parâmetros Ethernet

- » **Ender. IP:** configurar endereço de IP do dispositivo.
- » **Masc. Rede:** configurar a máscara de rede.
- » **Gateway:** configurar gateway da rede do equipamento.
- » **DNS:** configurar endereço DNS. Esta função está indisponível.
- » **Porta de comunicação TCP:** número da porta de comunicação TCP. Após alterar o número do TCP, reiniciar o equipamento para que a nova configuração seja validada.
- » **DHCP:** para que o IP do equipamento seja definido dinamicamente via servidor. Esta função está indisponível.
- » **Mostrar na barra status:** para mostrar no display da tela inicial o status da rede Ethernet.

Serial comunicação

Esta função está indisponível.

Configurar comunicação

Para segurança na comunicação do dispositivo na rede, é possível atribuir um ID do dispositivo e uma senha. Assim o equipamento estabelece comunicação apenas com a apresentação dos mesmos:

UsuarioAdm

Privilegio
Usr

Conf. Com.

Sistema

Personalizaç
ão

Ger. dados

Controle
acesso

Ger. pen
drive

Proc.
registros

Auto teste

Info.
sistema

Conf. Com.

TCP/IP

Serial Comm

Conf. Comunic.

Conf. wiegand

Conf. Comunic.

Senha com.

0

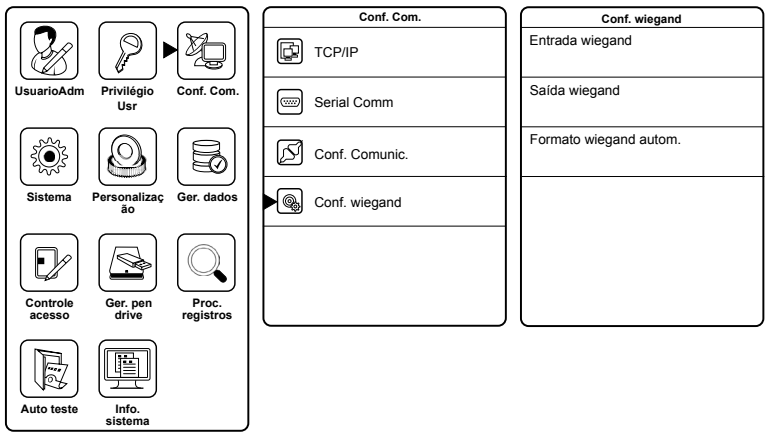
ID Equip.

8

Configurar senha para comunicação Ethernet

Configuração Wiegand

Configuração dos parâmetros Wiegand de entrada e saída.



Configurar Wiegand

- » **Entrada Wiegand:** configurar parâmetros do leitor Wiegand auxiliar.
 - » **Formato Wiegand:** usado para definir o tamanho de bits da chave do cartão de proximidade.
 - » **Largura pulso (us):** usado para definir a largura de pulso do protocolo Wiegand.
 - » **Intervalo pulso (us):** usado para definir o intervalo de pulso do protocolo Wiegand.
 - » **Tipo:** usado para definir se o que está sendo enviado para o equipamento é o ID do usuário ou o número do cartão.
- » **Saída Wiegand:** configurar parâmetros de saída de dados Wiegand.
 - » **SRB:** função indisponível.
 - » **Formato Wiegand:** usado para definir o tamanho de bits da chave do cartão de proximidade.
 - » **Bits de saída Wiegand:** quantidade de bits definidos para saída Wiegand.
 - » **Falha ID**
 - » **Site Code:** inserir manualmente o Site code da chave a ser enviada.
 - » **Largura pulso (us):** usado para definir a largura de pulso do protocolo Wiegand.
 - » **Intervalo pulso (us):** usado para definir o intervalo de pulso do protocolo Wiegand.
 - » **Tipo:** usado para definir se o que está sendo enviado para o equipamento é o ID do usuário ou o número do cartão.
- » **Formato Wiegand automático**

8. Detalhes e cuidados com o leitor biométrico

Dependendo do tempo de uso do equipamento, a lente do sensor biométrico fica suja, o que pode implicar na diminuição de eficiência de leitura. Para resolver esse problema basta limpar o acrílico com fita adesiva. Realize o seguinte procedimento:

1. Aplique a fita adesiva no acrílico, de forma que cubra toda a lente;
2. Puxe lentamente a fita, até remover por completo.

Evite o excesso de incidência de luz diretamente sobre o leitor. Os leitores biométricos ópticos são sensíveis à incidência direta da luz ambiente sobre a sua superfície, principalmente luz fluorescente branca ou luz solar. O equipamento nessas condições poderá gerar falsas tentativas de acesso ou até mesmo falhas na leitura da biometria.

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.

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.

O processo de fabricação deste produto não é coberto pelos requisitos da ISO 14001.

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: intelbras.com.br/suporte-tecnico

Suporte via e-mail: suporte@intelbras.com.br

SAC: 0800 7042767

Onde comprar? Quem instala?: 0800 7245115

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

03.18
Origem: China