

intelbras

Manual do usuário

SS 610

intelbras

SS 610

Controlador de acesso

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

O SS 610 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 e o cartão de proximidade.



03624-16-00160



(01)07896637674232

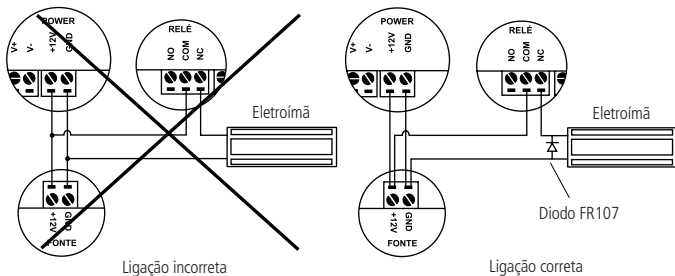
Este equipamento opera em caráter secundário, isto é, não tem direito à proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

Cuidados e segurança

- » É obrigatório o uso de fontes de alimentação estabilizadas ou lineares que protejam o equipamento contra surtos da rede.
- » 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 exibe a imagem a seguir:



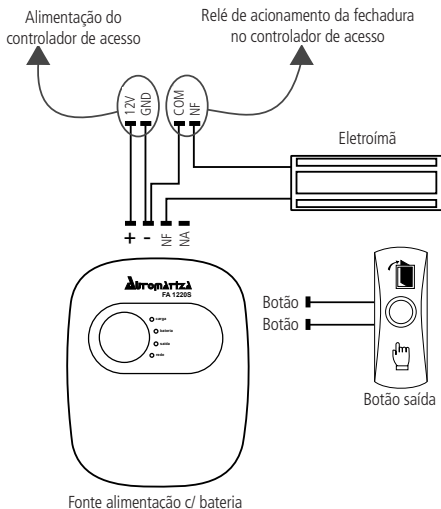
Recomendação de instalação

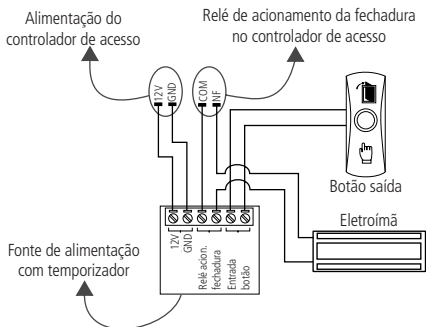
- » Use o diodo FR107 nas fechaduras-eletrôimã que não são da marca Automatiza, como demonstrado na figura acima.
- » Use o circuito desmagnetizante fornecido junto com a fechadura-eletrôimã Automatiza.
- » Não instale o produto em locais sujeitos a extremo calor ou umidade.
- » Recomenda-se utilizar 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

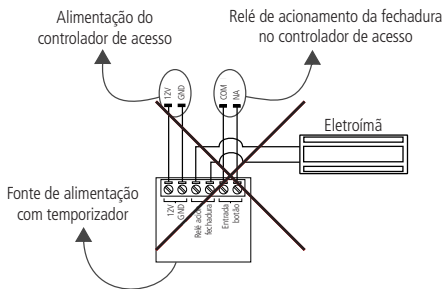
Para acionar a fechadura, utilize diretamente o relé do controlador de acesso. Ao utilizar uma placa temporizadora ou uma fonte com temporizador, utilize uma ligação em série entre os relés de acionamento, como está representado abaixo:





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	8
2. Características	8
3. Conteúdo da embalagem	9
4. Produto	10
5. Esquemas de ligação	11
5.1. Fonte de alimentação	11
5.2. Fechadura-eletróimã	13
5.3. Fechadura elétrica	14
5.4. Fechadura solenoide	15
5.5. Botão de saída	16
5.6. Saída alarme 12 V	17
5.7. Campainha	18
5.8. Leitor auxiliar	19
5.9. Leitor LE 311	20
5.10. Entrada auxiliar	21

6. Operações do sistema	22
6.1. Menu de programação	22
6.2. Usuário-adm	23
6.3. Privilégios usuário	27
6.4. Sistema	27
6.5. Personalização	31
6.6. Gerenciamento de dados	33
6.7. Controle acesso	35
6.8. Procurar registros	41
6.9. Autoteste	42
6.10. Informações do sistema	42
6.11. Gerenciamento pen drive	43
6.12. Reset administrador	45
7. Comunicação do equipamento	46
7.1. Configurar comunicação	46
8. Detalhes e cuidados com o leitor biométrico	49
Termo de garantia	50

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 e biometria digital
Modulação	ASK
Frequência de operação	125 kHz
Taxa de transmissão	3,906 kbps
Código de emissão	125KA2DCN
Tipo antena	Interna
Capacidade máxima de cartões	10.000
Capacidade máxima de biometrias	1.500
Interface de comunicação	Ethernet
Dimensões (L x A x P)	86 x 205 x 45 mm

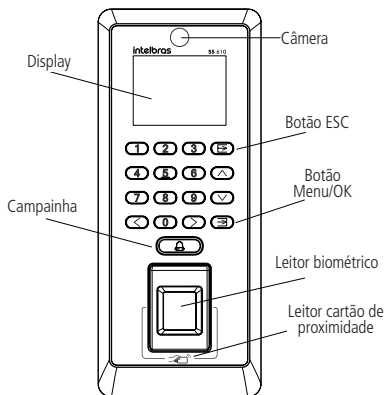
2. Características

- » 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.

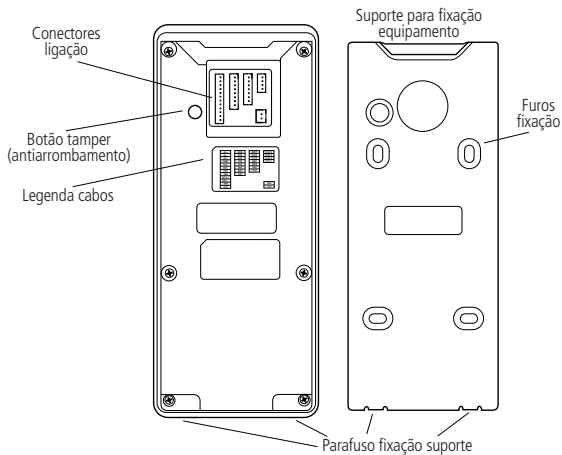
3. Conteúdo da embalagem

- » 1 controlador de acesso SS 610
- » 1 manual de instruções
- » 1 conjunto de cabos para ligação
- » 1 chave Tork
- » 6 parafusos
- » 4 buchas
- » 1 diodo FR107

4. Produto



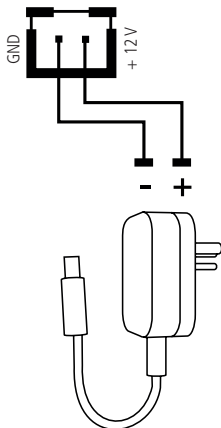
Vista frontal SS 610



Fixação SS 610

5. Esquemas de ligação

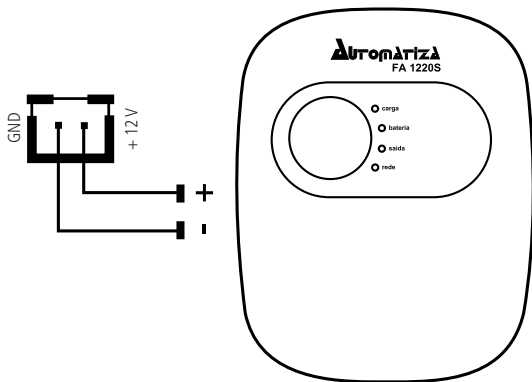
5.1. Fonte de alimentação



Fonte de alimentação

Ligação da fonte de alimentação

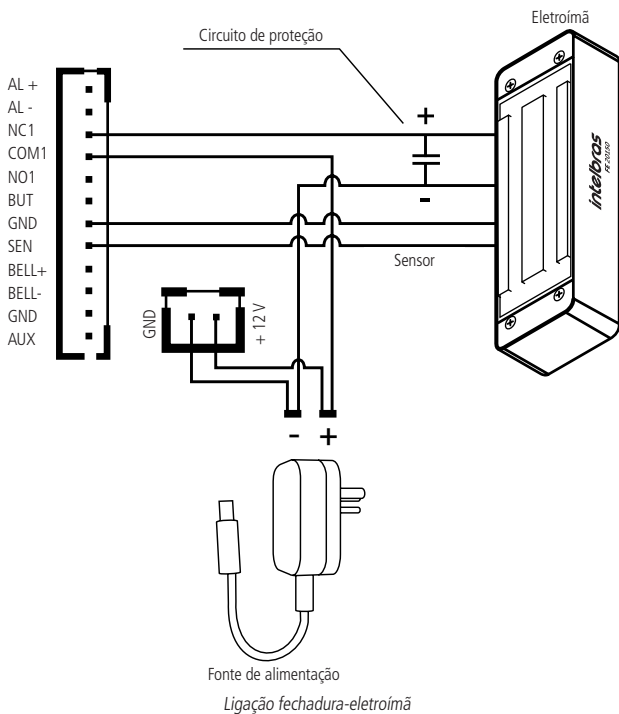
Obs.: caso não haja nobreak para alimentar o equipamento em situações de queda de energia, é recomendável a instalação de uma fonte de alimentação que possua bateria.



Fonte de alimentação com bateria

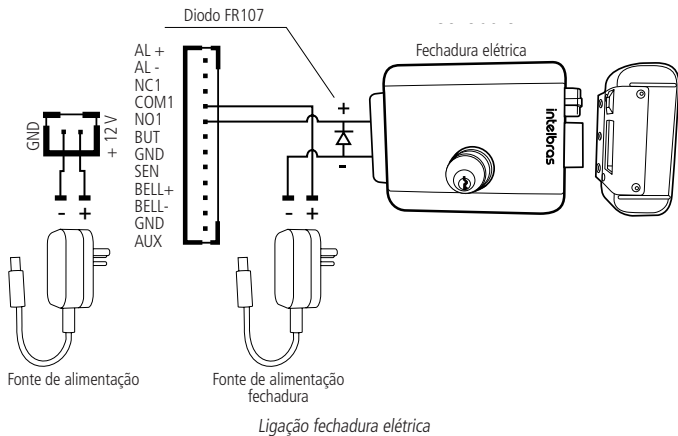
Ligação da fonte de alimentação FA 1220S

5.2. Fechadura-eletrôimã

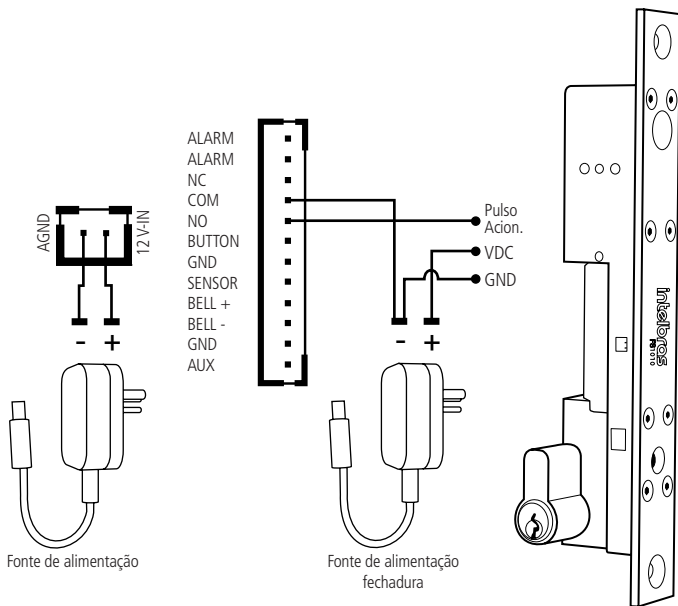


- Obs.:** » Caso a fechadura não possua sensor, desconsidere a ligação deste.
» Ao utilizar fechadura-eletrôimã de outro fabricante, utilize o diodo FR107 na ligação dela.

5.3. Fechadura elétrica

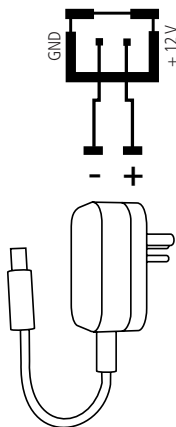


5.4. Fechadura solenoide



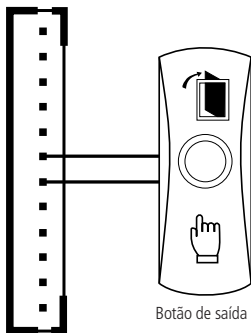
Ligação fechadura solenoide

5.5. Botão de saída



Fonte de alimentação

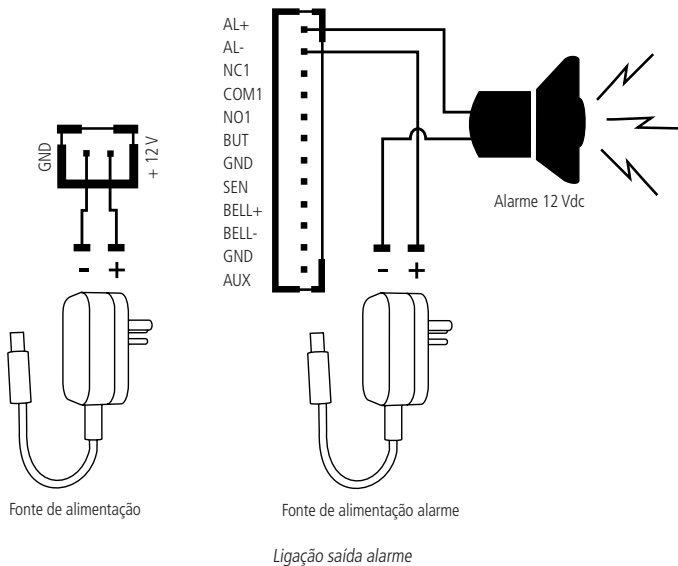
AL+
AL-
COM1
NO1
BUT
GND
SEN
BELL+
BELL-
GND
AUX



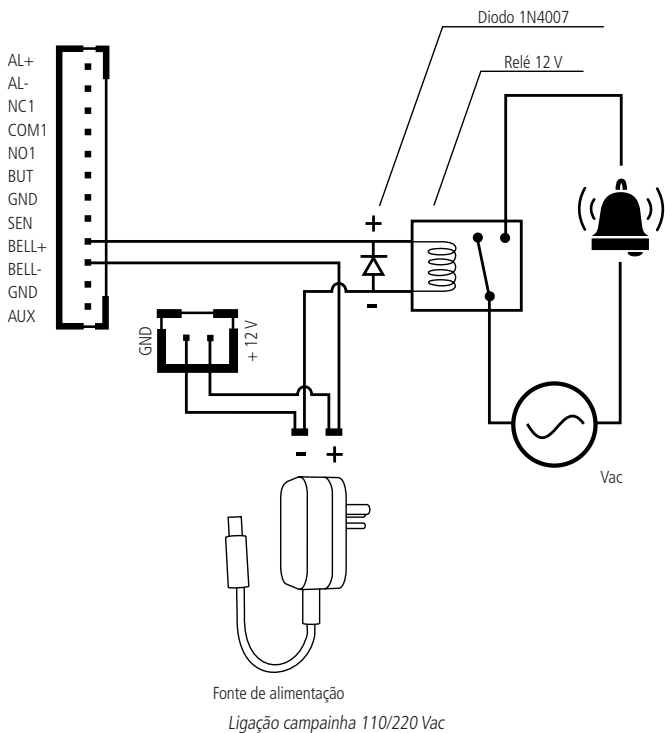
Botão de saída

Ligação botão de saída

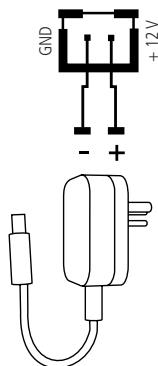
5.6. Saída alarme 12 V



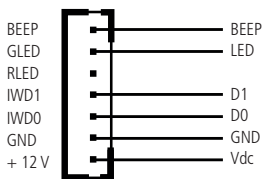
5.7. Campainha



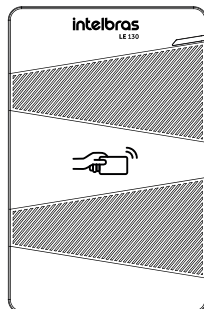
5.8. Leitor auxiliar



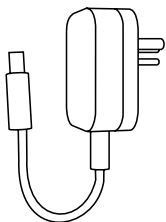
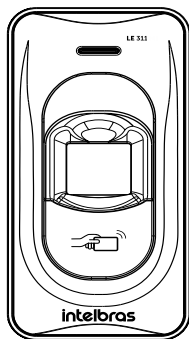
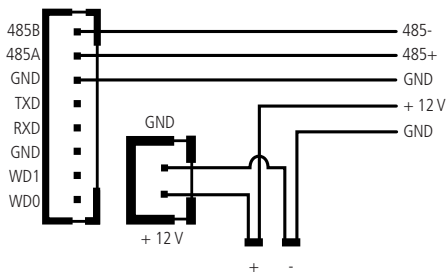
Fonte de alimentação



Ligação leitor auxiliar



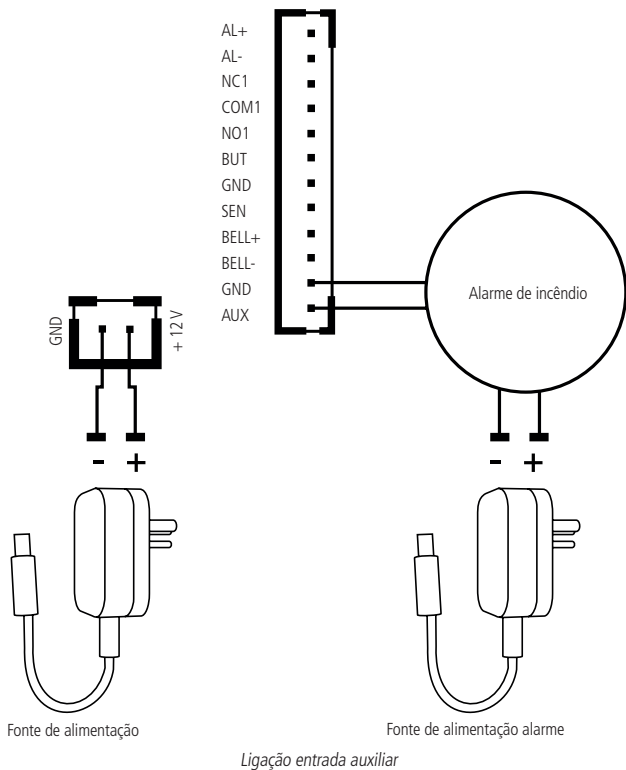
5.9. Leitor LE 311



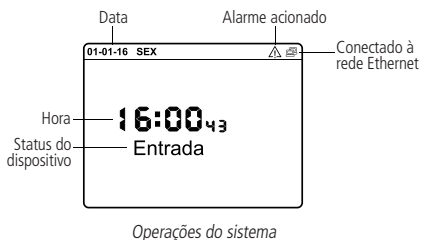
Fonte de alimentação

Ligação leitor LE 311

5.10. Entrada auxiliar

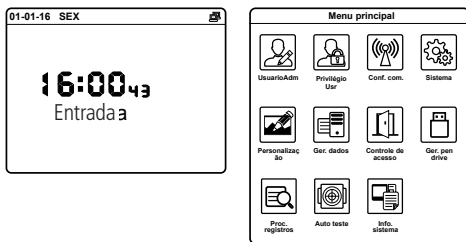


6. Operações do sistema



6.1. Menu de programação

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



Acessar o menu de programação

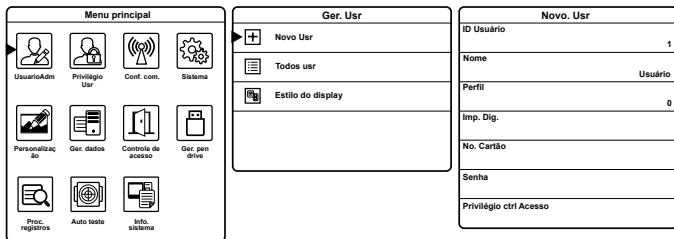
Atenção: para segurança do sistema de controle de acesso, é altamente recomendável o cadastro de uma senha ou cartão-administrador para acesso ao menu de programação.

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.

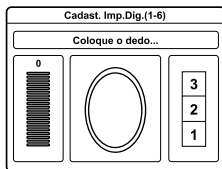
» **Nome:** vinculado ao número de identificação (não alterável).

Obs.: é possível alterar o nome através do software SoapAdmin3.5.

» **Perfil:** definir se o usuário terá perfil de usuário normal ou de administrador.

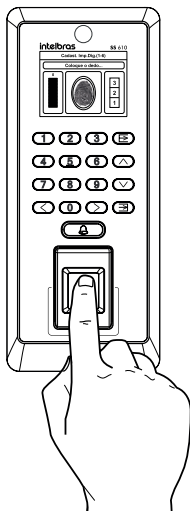
Um administrador é essencial no equipamento pois limita o acesso ao menu de programação. Apenas o administrador será responsável por cadastrar usuários e configurar o equipamento.

» **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.



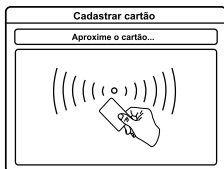
- » Não pressione demasiadamente o dedo no sensor biométrico, isso distorce a imagem da digital, não permitindo que o aparelho identifique os pontos formados pelas intersecções das linhas (cristas e vales) que compõem a digital.
- » Não posicione o dedo torto ou apenas a ponta do dedo no sensor biométrico. 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.
- » **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.
- » **Priv. controle acesso:** definição do grupo, horário de acesso, modo de verificação e coação.

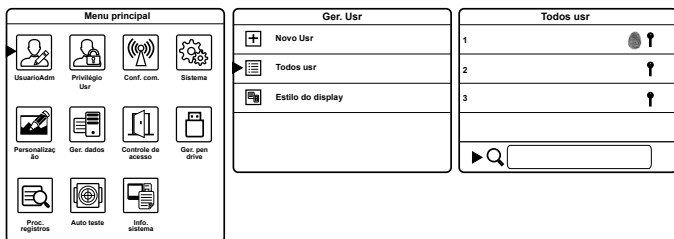
Controle acesso	
No. Grupo	1
Modo de verific.	Aplicar config. do grupo
Imp.Dig. Coação	Indefinido
Aplicar hr. do grupo	<input checked="" type="checkbox"/> ON <input type="checkbox"/>

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

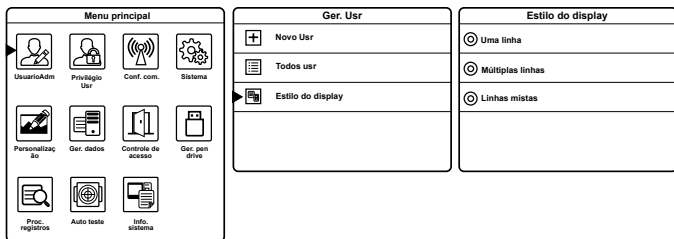
Listar todos os usuários cadastrados no dispositivo, assim, é possível selecionar e editar ou excluir o usuário.



Editar ou excluir usuário

Estilo do display

Definir estilo do display ao listar os usuários.



Definir estilo do display ao listar usuários

6.3. Privilégios usuário

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

Menu principal			
UsuarioAdm	Privilégio Usr	Conf. com.	Sistema
Personaliza- ção	Ger. dados	Controle de acesso	Ger. pen drive
Proc. registros	Auto teste	Info. sistema	

Priv. usuário	
	Usuário personalizado 1
	Usuário personalizado 2
	Usuário personalizado 3

Usuário personalizado 1	
Habilitar atribuir permissões	<input checked="" type="checkbox"/> ON
Nome	Usuário personalizado 1
Atribuir permissões	

Definir privilégios do usuário-administrador

- » **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 acesso ao conteúdo que o usuário-administrador terá sobre o equipamento.

6.4. Sistema

Data e hora

Configurações de data, hora e horário de verão.

Menu principal			
UsuarioAdm	Privilégio Usr	Conf. com.	Sistema
Personaliza- ção	Ger. dados	Controle de acesso	Ger. pen drive
Proc. registros	Auto teste	Info. sistema	

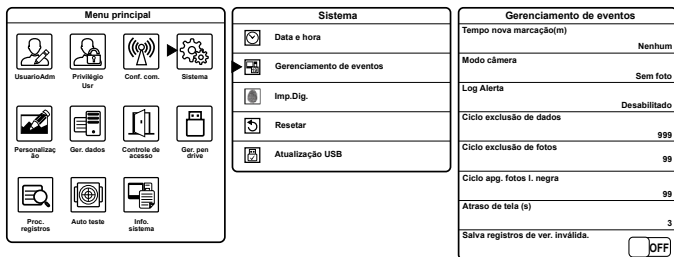
Sistema	
	Data e hora
	Gerenciamento de eventos
	Imp. Dig.
	Resetar
	Atualização USB

Data e hora	
Conf. Data	01.01.16
Conf. Hora	16:00:43
Formato 24h	<input checked="" type="checkbox"/> ON
Formato data	DD.MM.YY
Horário verão	<input type="checkbox"/> OFF

Configuração de data e hora

Configuração de registro de eventos

Nesta função é possível configurar os eventos gerados pelos usuários.



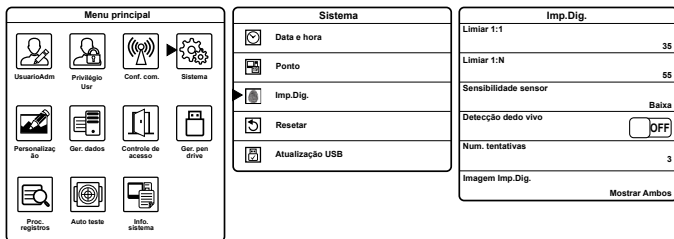
Configuração de registro de eventos

- » **Tempo nova marcação (m):** definir tempo, em minutos, em que o equipamento não irá registrar eventos duplicados.
- » **Modo Câmera:** o modo *Câmera* irá registrar uma foto ao realizar o acesso. O ângulo de visão da câmera é de $60^\circ \times 90^\circ$. Possui cinco opções de funcionamento.
 - » **Sem foto:** não registra nem captura foto.
 - » **Capturar, não salvar:** captura uma foto, porém não armazena.
 - » **Capturar e salvar:** captura e armazena uma foto, independentemente do tipo de evento (liberado ou negado).
 - » **Salva após verificação OK:** captura e armazena uma foto dos eventos de acessos liberados.
 - » **Salva após verificação inválida:** captura e armazena uma foto dos eventos de acessos negados.
- » **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.
- » **Ciclo de exclusão de fotos:** número de fotos que será permitido excluir quando o número armazenado alcançar seu valor máximo.
- » **Ciclo apagar fotos lista negra:** número de fotos da lista negra que será permitido excluir quando o número armazenado alcançar seu valor máximo.
- » **Atraso de tela:** tempo em segundos em que um evento do tipo acesso liberado permanecerá na tela.

- » **Salva registros de verificação inválida:** armazenar, ou não, os eventos de acesso negado.

Impressão digital

Configurações da leitura da impressão digital.



Configuração da leitura biometria digital

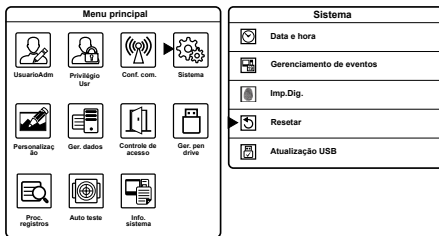
- » **Limiar¹ 1:1:** na verificação 1:1, o acesso liberado acontecerá somente quando a digital verificada e a digital do usuário forem maiores do que o valor inserido.
- » **Limiar¹ 1:N:** na verificação 1:1, o acesso liberado acontecerá somente quando a digital verificada e a digital de todos os usuários 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, tornado uma captura difícil, recomenda-se o valor baixo.
- » **Detecção dedo vivo:** esta função habilita no produto um complemento da segurança biométrica do dispositivo, ou seja, uma vez habilitada (On), apenas dedos vivos poderão ter acesso pela modalidade biométrica, impossibilitando o acesso de dedos de silicone ou outras formas de clonagem de impressão digital.
Obs.: esta função vem desabilitada (Off) de fábrica, recomenda-se sua habilitação (On), para usufruir do máximo de segurança disponível no produto.
- » **Número de tentativas:** para diminuir o processo de reinserir 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 onde o equipamento copiará este 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 retornar 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).

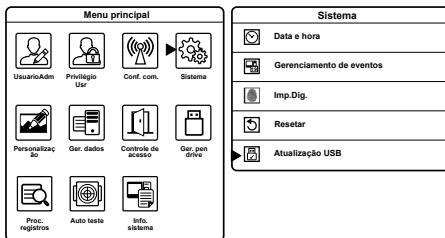
Obs.: esta função não afeta usuário cadastrado, data e hora.



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.

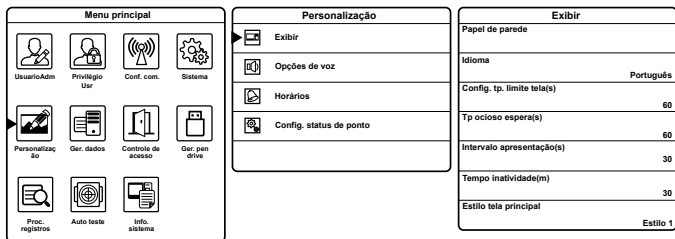


Atualização firmware

6.5. Personalização

Exibir

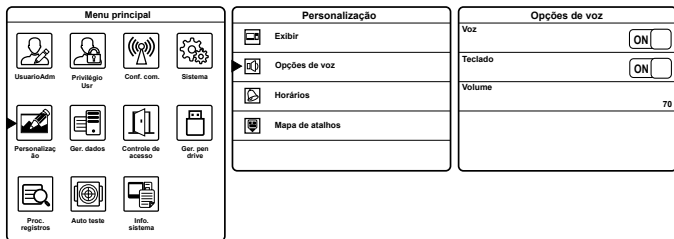
Configurações de tela.



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

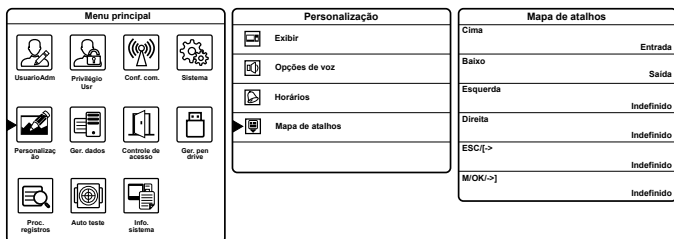
Esta função está indisponível.

Configurar status de evento

Esta função está indisponível.

Mapa de atalhos

Nesta função é permitido definir atalhos para as teclas de navegação:



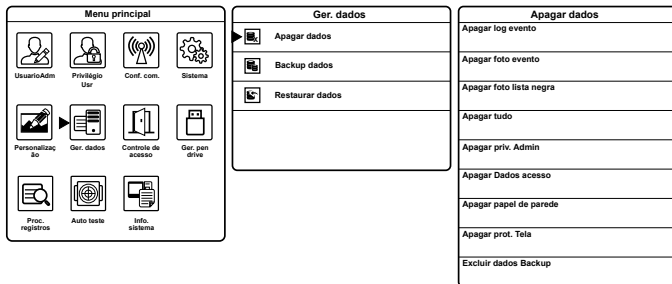
Definir atalhos para teclas

6.6. Gerenciamento de dados

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

Apagar dados

Função utilizada para excluir registros.

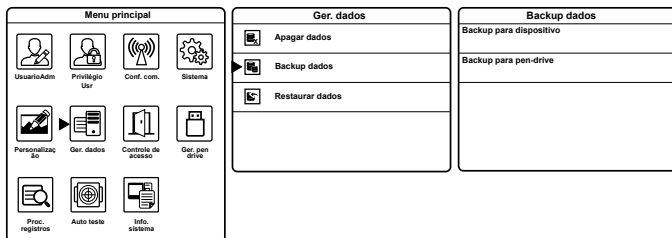


Apagar dados

- » **Apagar log evento:** exclui eventos dos usuários.
- » **Apagar foto evento:** exclui as fotos capturadas nos eventos.
- » **Apagar foto lista negra:** exclui as fotos capturadas com acessos negados.
- » **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 o ele se torne um usuário comum.
- » **Apagar dados acesso:** exclui as opções de acesso (grupos, zonas de horário, configuração coação).
- » **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.

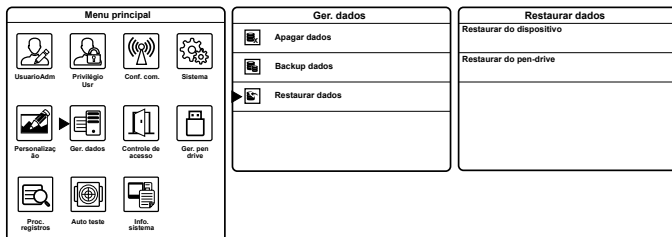


Backup de dados

- » **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.



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.

Menu principal

- UsuarioAdm
- Privilegio Usr
- Conf. com.
- Sistema
- Personalizaçã o
- Ger. dados
- Controle de acesso
- Ger. pen drive
- Proc. registros
- Auto teste
- Info. sistema

Controle Acesso

- Opc. controle acesso
- Conf. zona de tempo
- Conf. feriado
- Conf. grupo
- Aces. Comb. Grupos
- Conf. Anti-passback
- Alarme coação

Opc. controle acesso

Tempo abertura porta(s)	10
Atraso do Sensor(s)	10
Tipo de sensor	Normal aberto(NA)
Atraso alarme(s)	30
Recorrência de negação	3
Tempo NF	Nenhum
Tempo NA	Nenhum
Config. de entrada auxiliar	
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 a configuração da entrada auxiliar no equipamento.
 - » **Saída auxiliar/tempo de abertura (s):** tempo em que permanecerá acionado.
 - » **Configurar tipos de abertura:** tipos de abertura.
- » **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.

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

Buscar horários (1-50)

Configurações de zonas de tempo

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

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 seja frequentado.

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 associá-los 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).

The screenshot displays the 'Configurações de grupo de usuário' interface. It is divided into three main sections:

- Menu principal:** A grid of 12 icons for system functions: UsuarioAdm, Privilegio User, Conf. com., Sistema, Personalizaçã, Ger. dados, Controle de acesso, Ger. pen drive, Proc. registros, Auto teste, and Info. sistema.
- Controle acess:** A vertical list of settings: Opc. controle acesso, Conf. Zona de tempo, Conf. feriado, Conf. grupo (highlighted with a black arrow), Aces.Comb.Grupos, Conf. Anti-passback, and Alarme coação.
- Conf. grupo:** A table for configuring a specific group. The table has a header row 'Adic. grupo' and a body row '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.

Acesso combinado por grupo (entre usuários)

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

The screenshot displays the 'Acesso combinado por grupo (entre usuários)' interface. It is divided into three main sections:

- Menu principal:** Identical to the previous screenshot, showing system navigation icons.
- Controle acess:** Identical to the previous screenshot, showing the list of settings.
- Aces.Comb.Grupo:** A table for defining access combinations for a group. The table has a header row 'Aces.Comb.Grupo' and four data rows (1-4) with columns for user selection and time zones. Row 1 shows '01 00 00 00 00'. Row 2 shows '00 00 00 00 00'. Row 3 shows '00 00 00 00 00'. Row 4 shows '00 00 00 00 00'. Below the table is a search icon and an input field.

Acesso combinado por grupo (entre usuários)

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

Exemplo 1:

Aces.Comb.Grupos	
1	01 00 00 00 00
▶ 🔍	1

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

Aces.Comb.Grupos				
▲	▲	▲	▲	▲
2	0	0	0	0
▼	▼	▼	▼	▼
1	2	3	4	5
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		Aces.Comb.Grupos				
3	03 03 02 01 00	▲ 3 ▼	▲ 3 ▼	▲ 2 ▼	▲ 1 ▼	▲ 0 ▼
▶ 🔍 3		1	2	3	4	5
		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 610 com um leitor escravo.












Menu principal	Controle acesso	Conf. Anti-passback
UsuarioAdm	Opc. controle de acesso	Sentido Anti-passback
Privilégio User	Conf. Zona de tempo	Sem Anti-passback
Conf. com. Sistema	Conf. feriado	Status dispos.
Personalização	Conf. grupo	Saída
Ger. dados	Aces.Comb.Grupos	
Controle de acesso	Conf. Anti-passback	
Ger. pen drive	Alarme coação	
Proc. registros		
Auto teste		
Info. sistema		








Configurar anti-passback

- » **Sentido anti-passback:** definir sentido 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.

Menu principal			
			
UsuarioAdm	Privilégio Uzr	Conf. com.	Sistema
			
Personalizaç ão	Ger. dados	Controle de acesso	Ger. pen drive
			
Proc. registros	Auto teste	Info. sistema	

Controle acess	
	Opc. controle acesso
	Conf. Zona de tempo
	Conf. feriado
	Conf. grupo
	Aces.Comb.Grupos
	Conf. Anti-passback
	Alarme coação

Alarme coação	
Função coação	<input type="checkbox"/> OFF
1:1 Gatilho	<input type="checkbox"/> OFF
1:N Gatilho	<input type="checkbox"/> OFF
Senha de alarme	<input type="checkbox"/> OFF
Atraso alarme(s)	

Configurar alarme coação

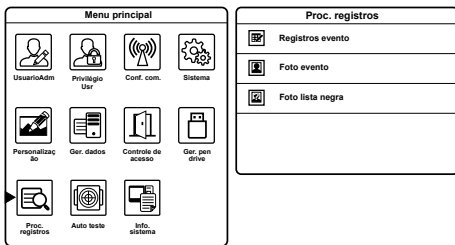
- » **Função Coação:** ativar alarme de coação através da tecla menu (->]) de coação mais a autenticação com biometria. Para isso ative a função coação, em seguida vá ao menu *Mapa de atalhos* (ver item 6.5. *Personalização>Mapa de atalhos*) e defina a tecla M/OK[->] para coação. Assim, para acionar 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 pressionada 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.

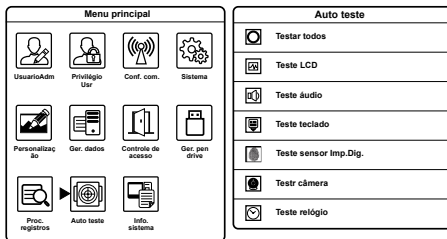


Consulta de eventos

- » **Registros evento:** consulta dos eventos de acesso no equipamento.
Obs.: ao confirmar sem inserir o número do usuário, o evento de todos os usuários será listado.
- » **Foto evento:** consultar fotos dos usuários cadastrados que realizaram acesso no dispositivo.
- » **Foto lista negra:** consultar fotos dos usuários não cadastrados que realizaram acesso no dispositivo e não obtiveram acesso.

6.9. Autoteste

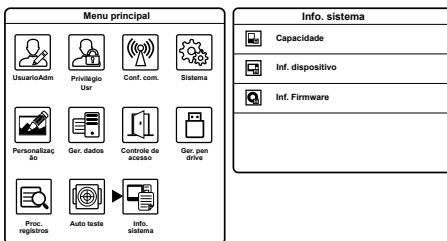
O equipamento realiza um autoteste para conferir sua tela, seus áudios, câmera, sensor biométrico, entre outros.



Autoteste

6.10. Informações do sistema

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



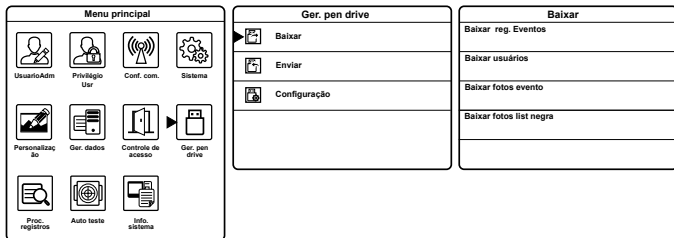
Consulta das informações do equipamento

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.

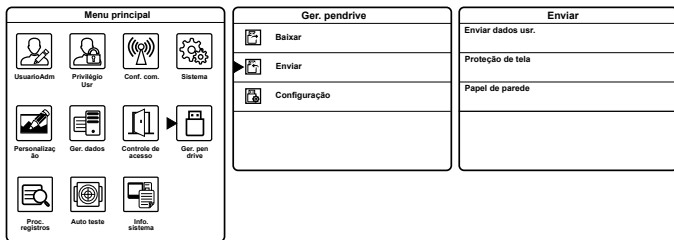


Baixar dados do equipamento para o pen drive

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

Enviar

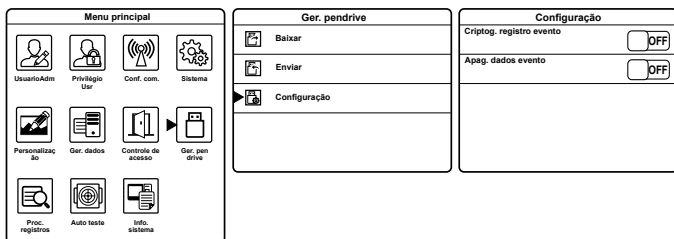
Enviar dados do pen drive para o equipamento.



Enviar dados do pen drive para o equipamento

- » **Enviar dados dos usuários:** enviar para o equipamento os usuários armazenados no pen drive.
- » **Proteção de tela:** enviar 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 no pen drive com o nome Advertise e inserir os arquivos de imagem nela. A capacidade máxima é de 20 imagens, e nenhuma delas deve exceder o tamanho de 30 kB. O nome da imagem não possui restrição, porém, o formato deve ser JPG, PNG ou BMP.
- » **Papel de parede:** enviar 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 no pen drive com o nome Wallpaper e inserir os arquivos de imagem nela. A capacidade máxima é de 20 imagens, e nenhuma delas deve exceder o tamanho de 30 kB. O nome da imagem não possui restrição, porém, o formato deve ser JPG, PNG ou BMP.

Configuração



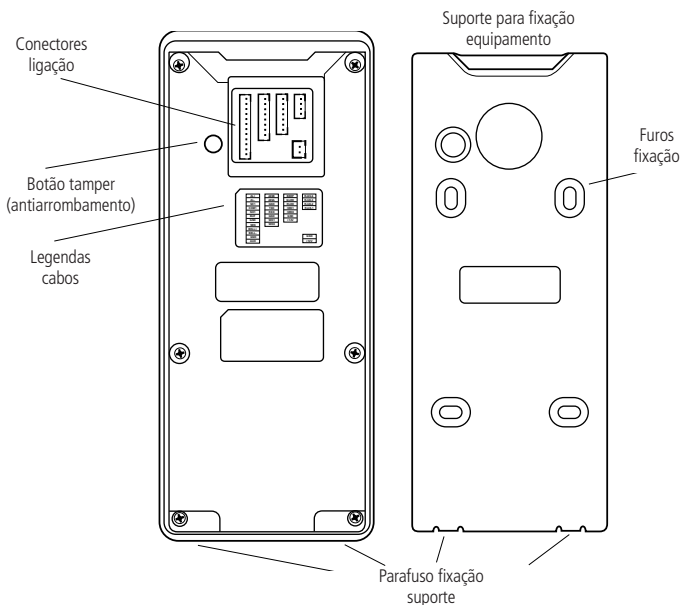
Configurações de gerenciamento

- » **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:

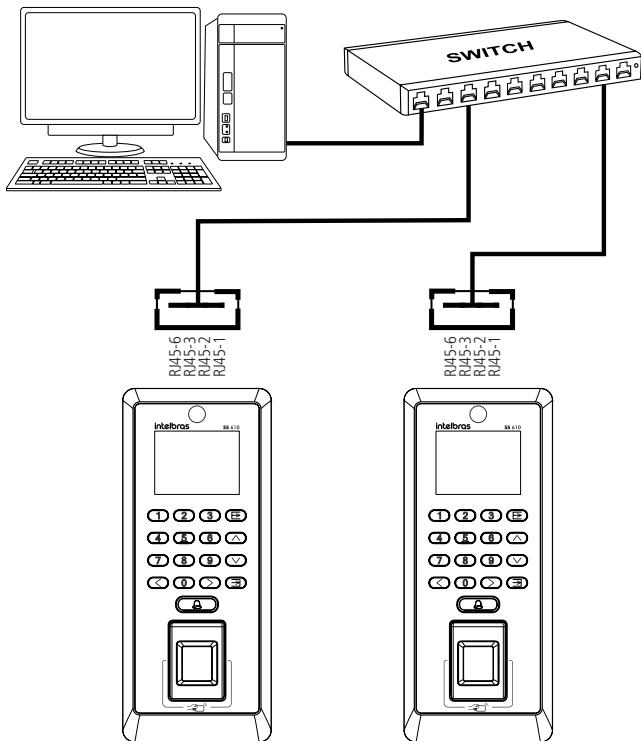
1. Desligue o equipamento;
2. Retire o suporte de fixação do equipamento da parede;
3. Mantenha o botão *Tamper* pressionado e ligue o dispositivo;
4. Após o equipamento iniciar (tela principal), solte o botão *Tamper* e aguarde trinta segundos;
5. Após trinta segundos acesse o menu de programação e 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

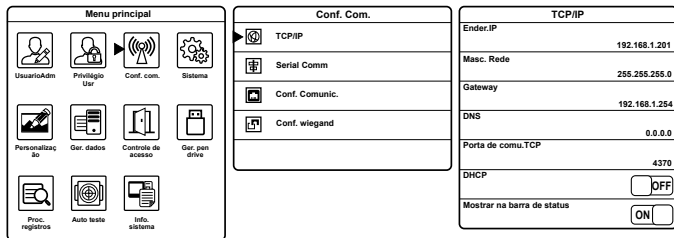
7.1. Configurar comunicação

TCP/IP



Ligação Ethernet

Configurar parâmetros de rede Ethernet



Configurar parâmetros Ethernet

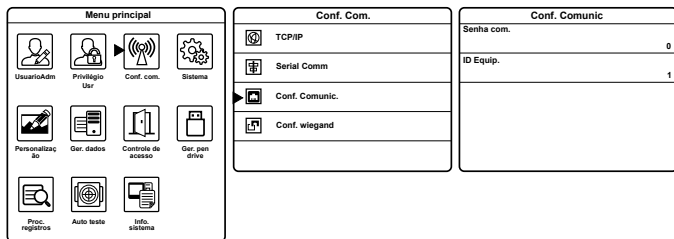
- » **Ender. IP:** configurar endereço de IP do dispositivo.
- » **Masc. rede:** configurar a máscara de rede.
- » **Gateway:** configurar gateway da rede do equipamento.
- » **DNS:** configurar endereço DNS. Esta função está indisponível.
- » **Porta de comunicação TCP:** número da porta de comunicação 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

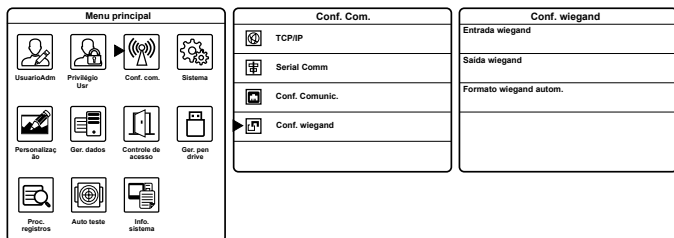
Para segurança na comunicação do dispositivo na rede, é possível atribuir um ID do dispositivo e uma senha. Assim o equipamento estabelece comunicação apenas com a apresentação destes.



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

02.18
Origem: China