AUTOMATIZA

Uma empresa do **Grupo Intelbras**

BIO INOX PLUS

SS311E (125KHZ/WD26/BIO/TCP)

Versão 3.0

12/08/2015

Sumário

1. Apresentação

O BIO INOX PLUS é um dispositivo de controle de acesso de alta segurança que utiliza a biometria ou cartão de proximidade (RFID) como métodos de autenticação de usuários. Sua instalação é fácil e a operação é simples e intuitiva. Dentre suas funções e características, possui sinalização por voz que auxilia no acesso ao menu e cadastros no equipamento.

Possui comunicação Ethernet, possibilitando administração pelo software de gerenciamento de usuários e dispositivos SOAPADMIN

2. Itens que Acompanham

1 Controlador de Acesso BIO INOX PLUS
1 Cabo adaptador de alimentação
1 Cabo USB
1 Chave Torx
1 Membrana de borracha
6 Parafusos
1 Manual do usuário
1 Cabo de dados
1 Cabo de acionamento
1 Cartão RFID
1 Diodo FR107
4 Buchas

3. Especificações Técnicas

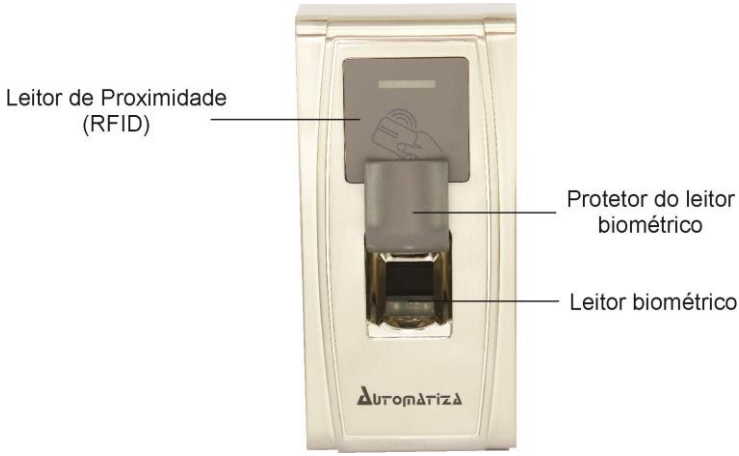
Tensão de alimentação	12VCC
Corrente de operação	250mA
Potência operação	3W
Corrente de chaveamento	1A
Tensão de chaveamento	12VCC
Temperatura de operação	-10 à 60°C
Umidade de operação	10% à 90%
Índice (grau) de proteção	IP65
Frequência de operação	125kHz
Modulação	ASK
Codificação do cartão	Manchester
Método de autenticação	Biometria e cartão de proximidade (RFID)
Capacidade máxima de cartões	10.000
Capacidade máxima de biometria	1.500
Interfaces de comunicação	Ethernet
Dimensões do equipamento	146 x 72 x 34 mm (A x L X P)
Peso	1,15kg

4. Características Gerais

- Possui uma voz que auxilia no acesso ao menu e cadastros do equipamento;
- Capacidade para armazenar até 100.000 eventos;
- Sensor tipo óptico;
- Possui software de gerenciamento;
- Suporta leitor auxiliar para liberar o acesso na saída.

5. Visão geral do Equipamento

5.1. Vista Frontal



5.2. Vista Inferior

6. Recomendações de Instalação

» É obrigatório o uso de fontes de alimentação estabilizadas ou lineares que protejam o equipamento contra surtos da rede.

» Execute toda a instalação com o equipamento desligado da rede elétrica. Após verificar se a instalação está correta, ligue-o.

» Ligue primeiro o cabo terra e depois os outros cabos, isto para prevenir danos causados pela energia estática.

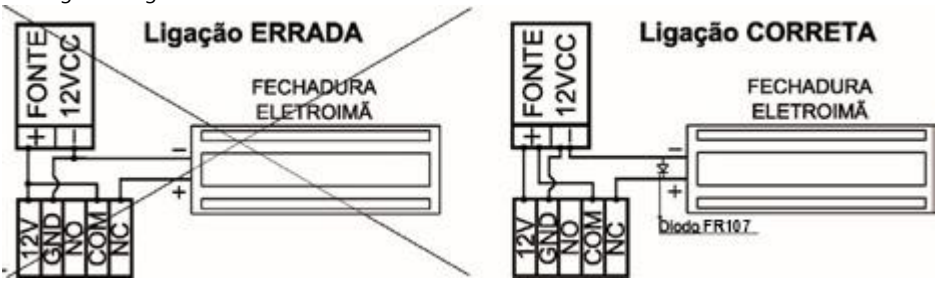
» Utilize cabos manga blindados para fazer ligações de leitores. Recomenda-se o uso de cabos blindados em ambientes que possam sofrer interferência eletromagnética.

» A distância entre o equipamento de controle de acesso e seu leitor auxiliar é de no máximo 10 metros.

» Utilize cabos de bitola de 0,75 mm² ou superior para ligações de alimentação e conexões de equipamentos e para conexões de alimentação das fechaduras.

» Não se devem passar cabos de rede elétrica e cabos de dados na mesma tubulação.

» Não faça derivação dos terminais de alimentação do controle de acesso para os terminais de ligação da fechadura. Devem-se trazer dois fios separados da fonte de alimentação, como mostra a imagem a seguir:



Esquemas de ligação

a) Use o diodo FR107 nas fechaduras-eletroímã, como demonstrado na figura acima.

b) Não instale o produto em locais sujeitos a extremos de calor ou umidade.

» Não instale o produto onde possui luz intensa ou pontos de iluminação diretamente acima do equipamento. A exposição à luz pode resultar no mau funcionamento do equipamento (falhas na identificação) ou até mesmo em acessos tentativas de acesso "fantasma" (sistema acusa tentativa de acesso negado aleatoriamente). ***Detalhes e cuidados no item 11.***

Atenção: Danos causados pelo não cumprimento das recomendações de instalação ou uso inadequado do produto não são cobertos pela garantia, vide Termo de garantia do produto.

!!! ATENÇÃO !!!

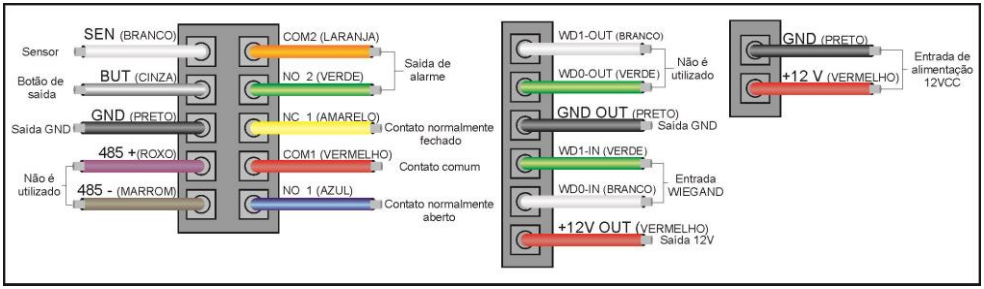
! Não exponha a lente do leitor à luz intensa. A exposição à luz pode resultar no mau funcionamento do equipamento (falhas na identificação) ou até mesmo em tentativas de acessos "fantasma" (sistema acusa tentativa de acesso negado aleatoriamente). Após toda identificação biométrica do usuário, feche novamente a tampa de proteção do sensor. *Detalhes e cuidados no item 11*.

! Não utilize produtos químicos para limpeza do sensor biométrico.

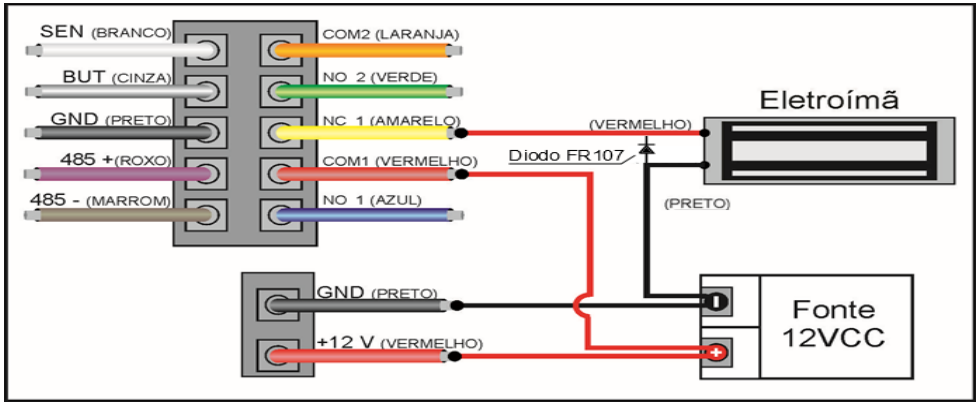
! Recomenda-se a instalação do produto no lado de dentro da porta (com leitor auxiliar do lado externo). No caso de usos externos, recomenda-se o uso da função "Chave de Comunicação" do produto (*mais informações no item 10.0.1*).

7. Esquemas de Ligação

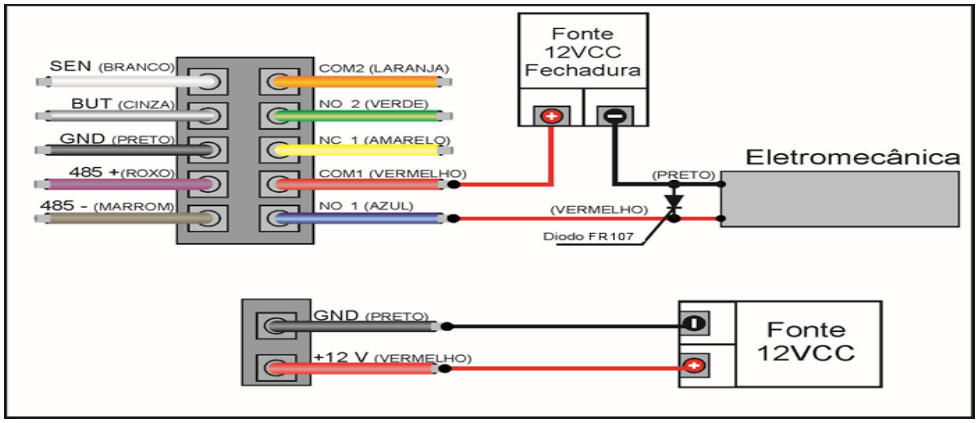
7.1. Conectores



7.2. Fechadura Eletroímã



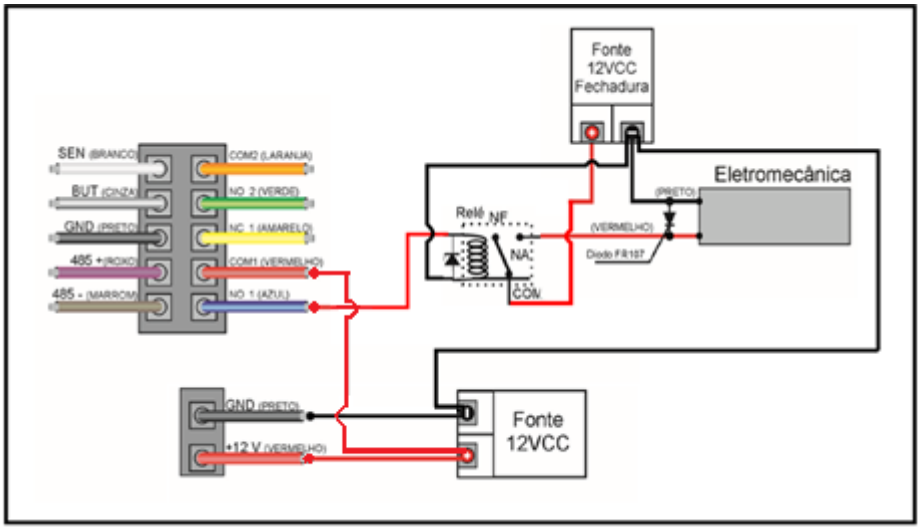
7.3. Fechadura Eletromecânica



Atenção: Deve-se usar uma fonte 12 VCC para a fechadura eletromecânica (separada da fonte do equipamento). Caso a corrente elétrica da fechadura eletromecânica seja maior que 1A deve-se utilizar uma placa do REED para acionar a fechadura. Lembrando que a placa do REED suporta até 5A.

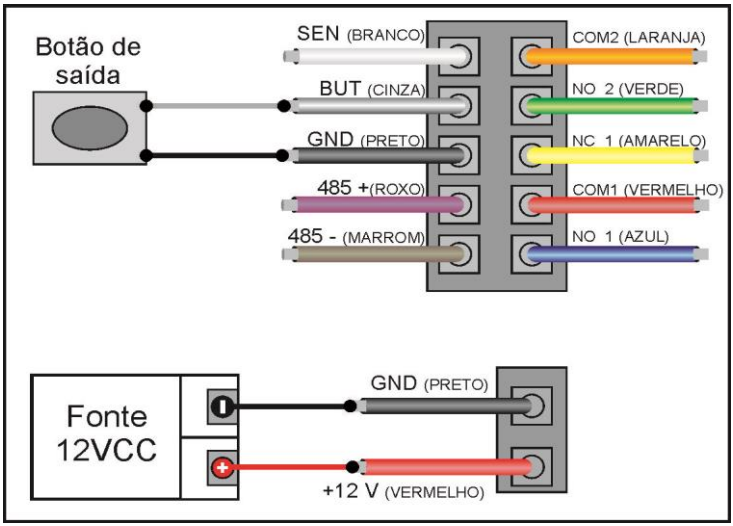
No uso de uma fechadura elétrica de baixo consumo (por exemplo, fechaduras solenoide), não há necessidade do uso de uma placa REED.

7.4. Fechadura Eletromecânica com Relé

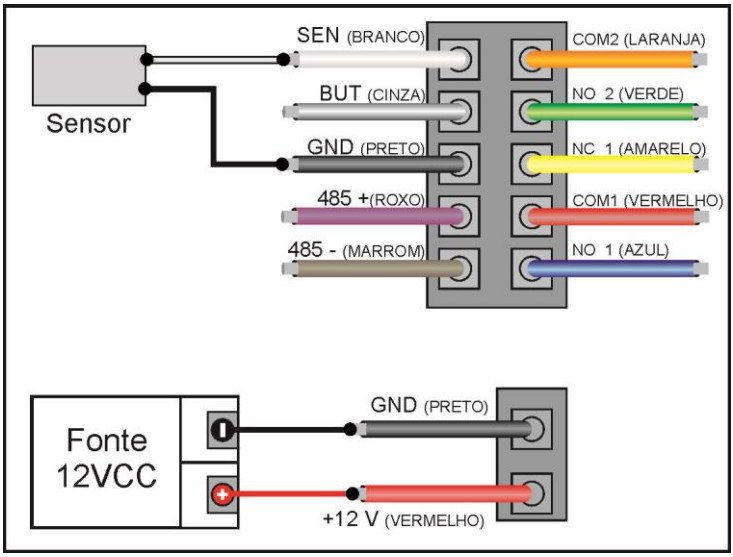


- Usar uma fonte 12Vdc para a fechadura elétrica (separada da fonte do equipamento).
- Sempre usar o diodo (FR107) de proteção entre os terminais da fechadura, como ilustrado na imagem acima.
- Não esqueça de conectar os polos negativos das fontes entre si, como ilustrado na imagem acima.
- A corrente máxima de chaveamento será definida pelas especificações técnicas do relé, portanto certifique-se de obter o relé correto para a fechadura a ser usada.
- Não esqueça de conectar o diodo de proteção entre os polos do relé, como ilustrado na imagem acima.

7.5. Botão de Saída

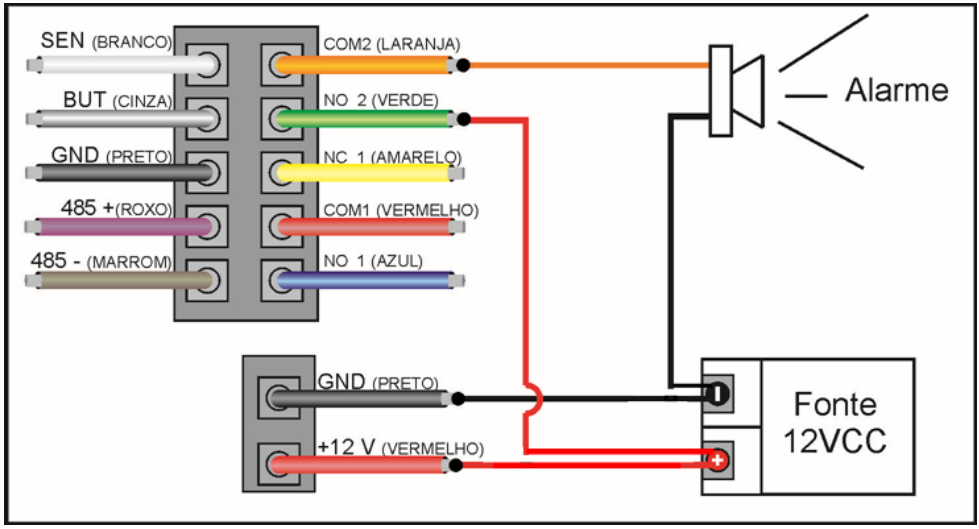


7.6. Sensor de Porta



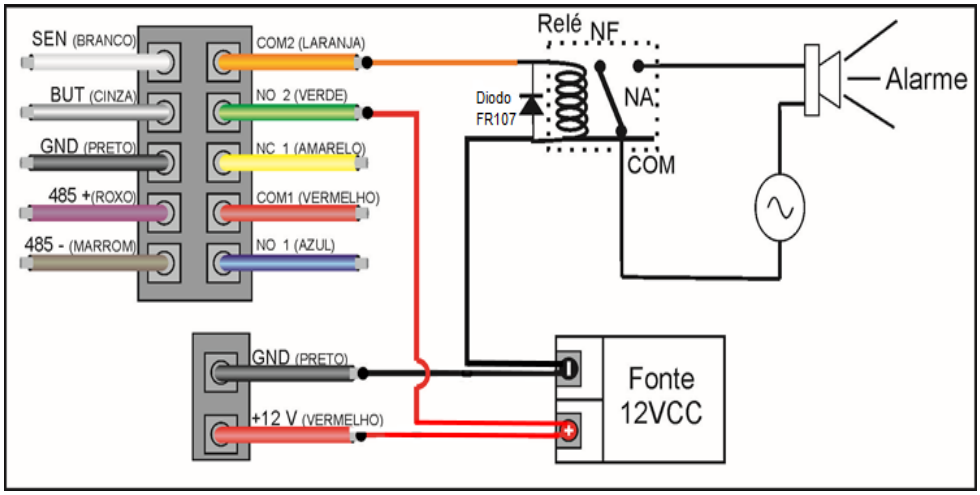
Obs.: O sensor de porta é configurado somente pelo software SoapAdmin.

7.7. Alarme 12VCC



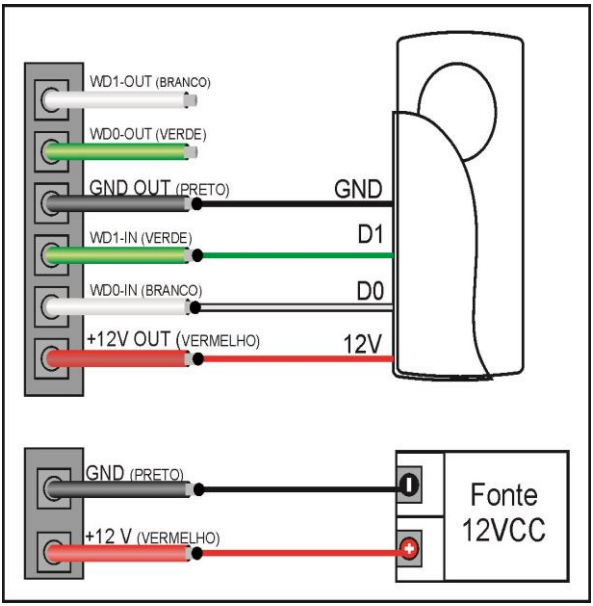
Obs.: O Alarme é configurado somente pelo software SoapAdmin. A saída de alarme (COM2 e NO2) é uma saída de contato seco

7.8. Alarme 110/220VCA



Obs.: O Alarme é configurado somente pelo software SoapAdmin. A saída de alarme (COM2 e NO2) é uma saída de contato seco

7.8. Leitor WIEGAND Auxiliar

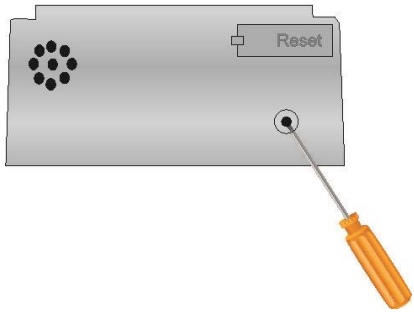


Obs.: O leitor WIEGAND tem como função liberar o acesso com cartão de proximidade na saída.

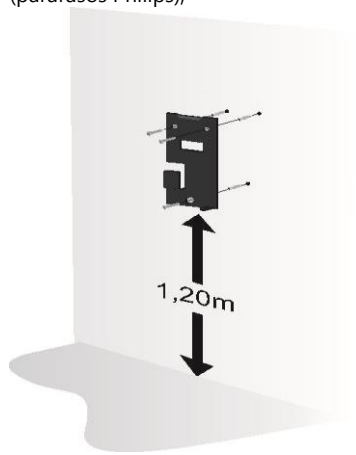
8. Fixação do Equipamento

Para fixar o equipamento deve-se seguir os passos abaixo:

1. Retire o parafuso que fixa a tampa com a chave torx;



2. Faça as marcações na parede com o suporte de fixação. Fure a parede com broca 8 mm, após fazer o furo coloque a bucha e parafuse o suporte com os parafusos de fixação (parafusos Philips);



3. Encaixe o BIO INOX PLUS no suporte de fixação;

4. Parafuse o equipamento no suporte de fixação com o parafuso Torx M4 x 5mm.

9. Operações do Sistema

9.1. Cadastro de Administrador

Para cadastrar um usuário tipo administrador com cartão mestre, deve-se seguir os passos abaixo:

1. Ao iniciar o equipamento, emitirá a mensagem: "por favor, cadastre o cartão mestre'';
2. Aproxime o cartão no dispositivo. Esse cartão será cadastrado como cartão mestre, ou seja, o usuário será do tipo Administrador.

É obrigatório o cadastro do administrador para o equipamento fazer suas operações corretamente. O administrador serve apenas para cadastrar e excluir os demais usuários.

Só é possível ter administrador com CARTÃO, ou seja, não é possível ter um administrador com BIOMETRIA.

9.2. Cadastro de Usuário Comum

9.2.1. Cadastro de Usuário Comum com Cartão de Proximidade (RFID)

Para cadastrar usuário comum com cartão de proximidade (RFID), deve-se seguir os passos abaixo:

1. Aproxime o cartão mestre (administrador);
2. O equipamento irá emitir a seguinte mensagem: '' Usuário cadastrado, por favor, coloque a digital ou aproxime o cartão";
3. Aproxime o cartão que irá ser cadastrado;
4. O equipamento irá emitir a seguinte mensagem: '' ID do usuário n° cadastrado com sucesso'';
5. Aproxime o cartão mestre novamente, para o equipamento voltar ao modo de verificação.

9.2.2. Cadastro de Usuário Comum com Biometria

Para cadastrar um usuário comum com biometria, deve-se seguir os passos abaixo:

1. Aproxime o cartão mestre (administrador);
2. O equipamento irá emitir a seguinte mensagem: '' Usuário cadastrado, por favor, coloque a digital ou aproxime o cartão";
3. Coloque a digital que irá ser cadastrada 3 vezes;
4. O equipamento irá emitir a seguinte mensagem: '' ID do usuário n° cadastrado com sucesso''
5. Aproxime o cartão mestre novamente, para o equipamento voltar ao modo de verificação.

9.2.3. Cadastro de Usuário Comum com Cartão de Proximidade RFID e Biometria

Para cadastrar um usuário tipo comum com cartão de proximidade (RFID) e biometria, deve-se seguir os passos abaixo:

1. Aproxime o cartão mestre (administrador);
2. O equipamento irá emitir a seguinte mensagem: '' Usuário cadastrado, por favor, coloque a digital ou aproxime o cartão";
3. Aproxime o cartão que irá ser cadastrado;
4. O equipamento irá emitir a seguinte mensagem: '' ID do usuário n° cadastrado com sucesso''
5. O equipamento emitirá uma nova mensagem: '' Cadastro, por favor, coloque sua digital''
6. Coloque a digital que irá ser cadastrada 3 vezes;
7. Aproxime o cartão mestre novamente, para o equipamento voltar ao modo de verificação.

9.3. Exclusão de Usuários

9.3.1. Exclusão de Usuário Comum com Cartão de Proximidade (RFID)

Para excluir um usuário comum com cartão, deve-se seguir os passos abaixo:

1. Aproxime o cartão mestre (administrador) por 5 vezes consecutivas (cada uma das 5 aproximações deve fazer um bipe);
2. O equipamento irá emitir a seguinte mensagem: ‘‘Usuário excluído, por favor, aproxime a digital ou aproxime o cartão”;
3. Aproxime o cartão que irá ser excluído;
4. Após isso o equipamento irá emitir a seguinte mensagem: "ID do usuário n° excluído com sucesso”
5. Aproxime o cartão mestre novamente, para o equipamento voltar ao modo de verificação.

9.3.2. Exclusão de Usuário Comum com Biometria

Para excluir um usuário comum com biometria, deve-se seguir os passos abaixo:

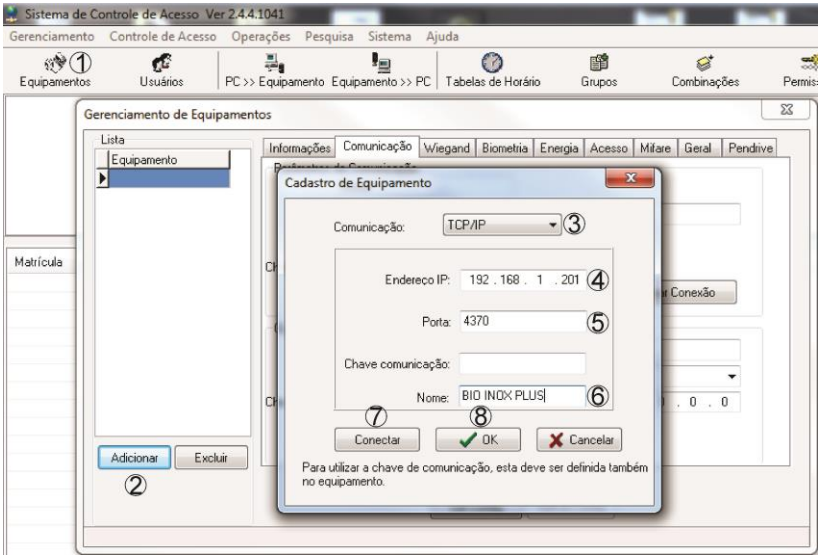
1. Aproxime o cartão mestre (administrador) por 5 vezes consecutivas (cada uma das 5 aproximações deve fazer um bipe);
2. O equipamento irá emitir a seguinte mensagem: ‘‘Usuário excluído, por favor, aproxime a digital ou aproxime o cartão”;
3. Aproxime a digital que irá ser excluída;
4. Após, o produto emitirá a seguinte mensagem: "ID do usuário n° excluído com sucesso”
5. Aproxime o cartão mestre novamente, para o equipamento voltar ao modo de verificação.

10. Comunicação

A comunicação do BIO INOX PLUS com software SoapAdmin é feita via TCP/IP.

Devem-se realizar os seguintes passos para que o equipamento possa se comunicar com o software SoapAdim:

1. Instale o software SoapAdmin em seu computador. O software está disponível no site www.automatiza.com;
2. Mude o endereço de IP de seu computador de acordo com a faixa de IP do Equipamento. O IP de fábrica do BIO INOX PLUS é 192.168.1.201. Recomendamos mudar o IP do computador para 192.168.1.200;
3. Com um cabo crossover ou pacthcord conecte o equipamento ao computador;
4. Abra o software SoapAdmin;
5. Na tela principal do software, clique no botão equipamentos (**1**), ao clicar a janela de gerenciamento de equipamento será aberta;
6. Na janela gerenciamento de equipamentos clique no botão Adicionar (**2**), ao clicar a janela de cadastro de equipamento será aberta;
7. Em comunicação escolha a opção TCP/IP (**3**);
8. Coloque o endereço IP do que equipamento: 192.168.1.201 (**4**);
9. Coloque a Porta: por padrão é 4370 (**5**);
10. Escolha um nome para o equipamento (**6**);
11. Clique em conectar(**7**), uma mensagem de conexão estabelecida deve parecer;
12. Clique em OK (**8**) para salvar e sair.



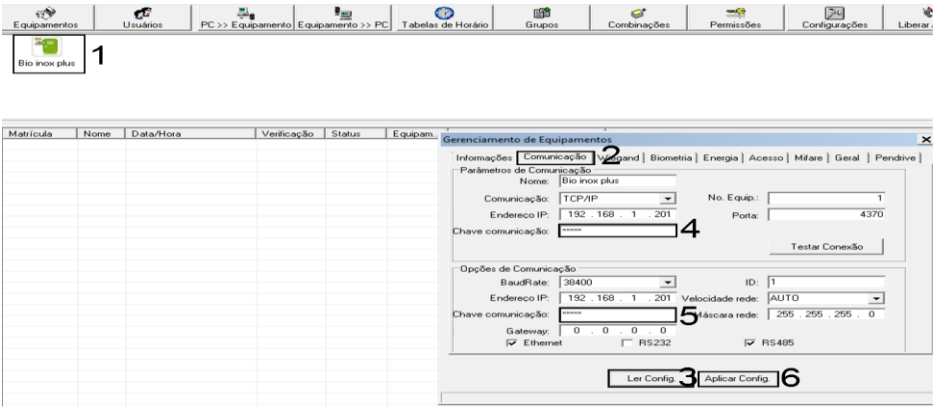
DICA: Para maiores informações sobre o software SOAP Admin entre no site da Automatiza (www.automatiza.com.br) e baixe o manual de instruções.

10.1. Chave de comunicação

O SOAPADMIN possui uma função chamada "Chave de Comunicação", que limita o acesso ao aparelho por conexão tcp/ip para apenas aqueles que conhecem a senha. Para isso, é necessário cadastrar via software uma senha no aparelho, que deverá ser adicionada à configuração do dispositivo no software. Para ativá-la, siga os passos abaixo:

1. Clique com o botão direito do mouse no equipamento cadastrado. Clique em "Propriedades";
2. Na janela "Gerenciamento de Equipamentos" clique na aba "Comunicação";
3. Clique em "Ler Config.";
4. Em "Parâmetros de Comunicação", na caixa "Chave comunicação", insira a senha desejada;
5. Na mesma aba, mas agora em "Opções de comunicação", clique na caixa "Chave comunicação:" e digite a mesma senha do item anterior;
6. Clique em "Aplicar Config.

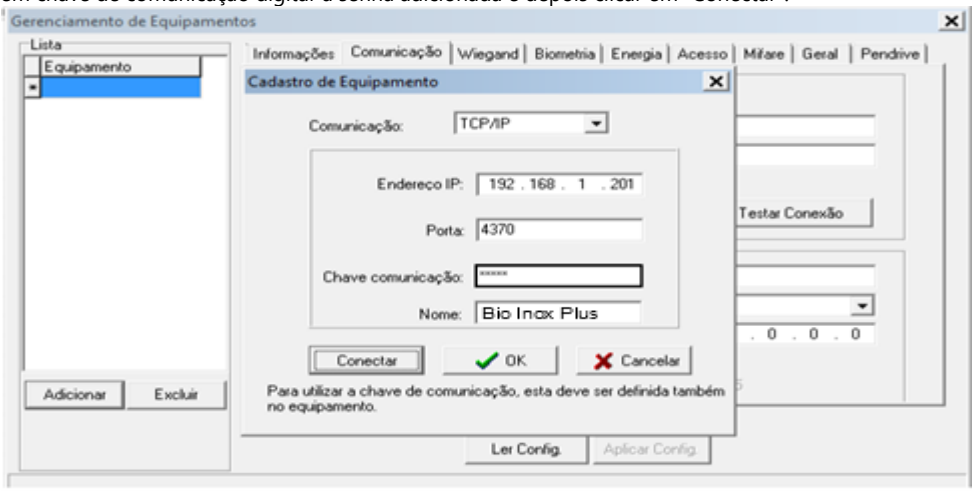
Reinicie o equipamento (propriedades>geral>reiniciar).



Com esta função habilitada, a senha estará salva no equipamento, que poderá se comunicar apenas com computadores que souberem a senha configurada em "Chave de Comunicação".

Observação 1: para retirar a chave de comunicação, é necessário reiniciar o aparelho em **Reset Opções** onde ele retorna para as opções de fábrica (tópico 10.8).

Observação 2: para acessar o aparelho em outro computador basta cadastrar o dispositivo (tópico 10), em chave de comunicação digitar a senha adicionada e depois clicar em "Conectar".



10.2. Download do SoapAdmin

O manual e o software SoapAdmin, está disponível no *link:* *http://www.automatiza.com/produto/software-soapadmin/*.

Clique na aba '' suporte e *download*'' faça download do programa e acesse os manuais.

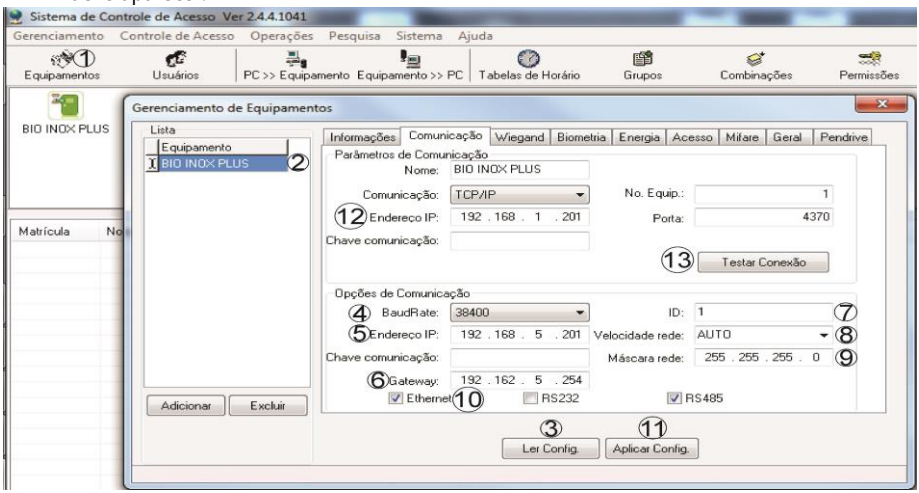
10.3. Mudar o IP do Equipamento

Para mudar o IP do equipamento abra o software SoapAdmin e siga os passos abaixo:

Observação: Antes de mudar o IP veja o item 10. deste manual para que o equipamento possa se comunicar com o software SoapAdmin.

1. Na janela principal do software SoapAdmin clique no botão equipamentos (**1**), ao clicar a janela de gerenciamento de equipamentos será aberta;
2. Clique no equipamento que deseja mudar o IP (**2**);
3. Clique no botão Ler Config. (**3**) para ler as configurações do equipamento;

4. Em BaudRate (**4**) por padrão é 38400;
5. Em endereço IP (**5**) coloque o IP de acordo com a rede ethernet do seu computador;
6. Em gateway (**6**) coloque o gateway de acordo com a rede ethernet do seu computador;
7. Em ID (**7**) coloque um número de identificação para o equipamento;
8. Em velocidade da rede (**8**) por padrão é AUTO;
9. Em máscara rede (**9**) coloque a máscara de acordo com a rede ethernet do seu computador;
10. Selecione a opção ethernet (**10**);
11. Clique no botão Aplicar Config. (**11**) para aplicar as configurações, uma janela de operação concluída será aberta;
12. Reinicie o equipamento;
13. Mude o IP do seu computador de acordo com sua rede ethernet e conecte-o na rede;
14. Conecte o BIO INOX PLUS na rede ethernet;
15. Coloque mesmo endereço de IP (**12**) cadastrado no equipamento no passo **5**;
16. Clique em Testar Conexão (**13**), uma mensagem de conexão com o equipamento estabelecida deve aparecer.



10.4. Opções de Acesso

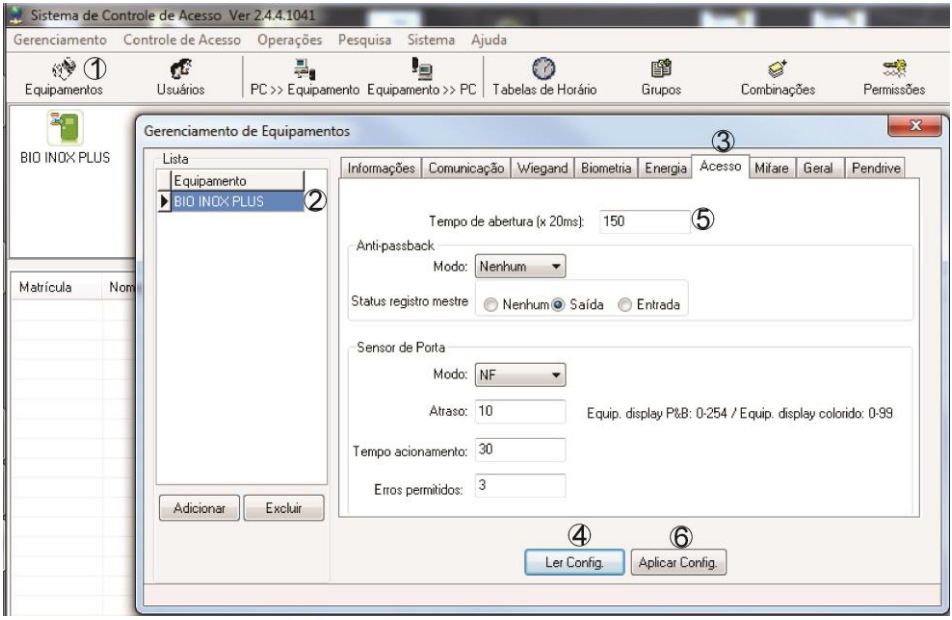
Em gerenciamento de equipamentos é possível configurar as opções de acesso como:

- Alterar o tempo de abertura da porta (item 10.2.1. deste manual);
- Configurar o Anti Pass-Back (item 10.4.2. deste manual);
- Configurar o sensor da porta (item 10.4.3. deste manual);
- Máximos de falhas seguidas em uma identificação ou erros permitidos (10.2.4. deste manual).

10.4.1. Tempo de Abertura da Porta

Para definir o tempo que a porta ficará aberta (tempo que o relé ficará atracado) siga os passos:

1. Na janela principal do software SoapAdmin clique no botão equipamentos(**1**), ao clicar a janela de gerenciamento de equipamentos será aberta;
2. Clique no equipamento que deseja configurar as opções de acesso (**2**);
3. Clique na aba Acesso(**3**);
4. Clique no botão Ler Config. (**4**) para ler as configurações do equipamento;
5. Escolha o tempo que a porta ficará aberta (25=1s, 50=2s, 75=3s, 100=4s, 125=5s, 150=6s, 175=7s, 200=8s, 225=9s, 250=10s) (**5**);
6. Clique no botão Aplicar Config. (**6**) para aplicar as configurações, uma janela de operação concluída será aberta;
7. Reinicie o equipamento;

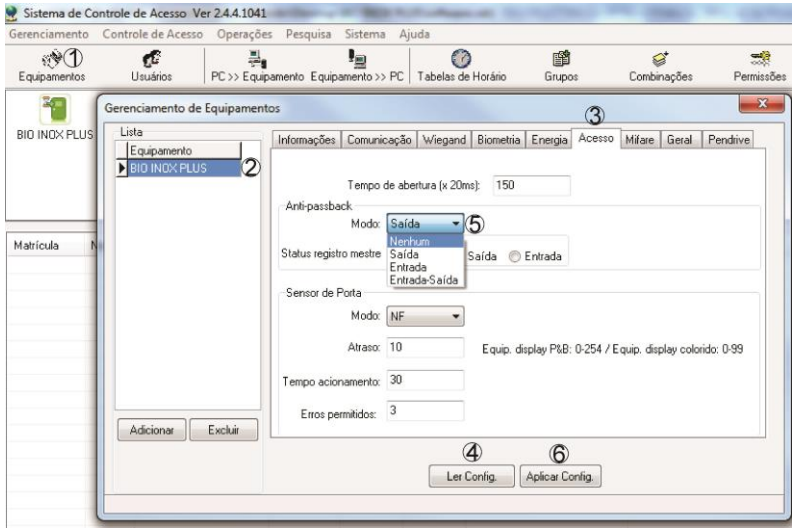


10.4.2. Configurar Anti Pass-Back

O Anti Pass-Back, ou seja, anti dupla entrada ou anti dupla saída. Este recurso é utilizado para que os usuários tenham a responsabilidade de sempre registrarem suas entradas e saídas em cada equipamento. É necessário que exista dois equipamentos, o equipamento 1 (leitor WIEGAND) para saída e equipamento 2 (equipamento BIO INOX PLUS) para entrada. O item 7.8 deste manual mostra o esquema de ligação desses equipamentos.

Para configurar está opção, siga os passos abaixo:

1. Na janela principal do software SoapAdmin clique no botão equipamentos(**1**), ao clicar a janela de gerenciamento de equipamentos será aberta;
2. Clique no equipamento que deseja configurar o Anti Pass-Back (**2**);
3. Clique na aba Acesso(**3**);
4. Clique no botão Ler Config. (**4**) para ler as configurações do equipamento;
5. Selecione uma das opções abaixo(**5**):
   - 4.1. **Nenhum**: Desativa a opção
   - 4.2. **Saída:** o usuário poderá sair livremente (equipamento 1), mas só pode entrar após a verificação do equipamento 2;
   - 4.3. **Entrada**: o usuário poderá entrar livremente, mas só pode sair após a verificação do equipamento 1;
   - 4.4. **Entrada e saída**: a verificação está ativada nos dois equipamentos, para entrada e saída;
5. Clique no botão Aplicar Config. (**6**) para aplicar as configurações, uma janela de operação concluída será aberta;
6. Reinicie o equipamento;



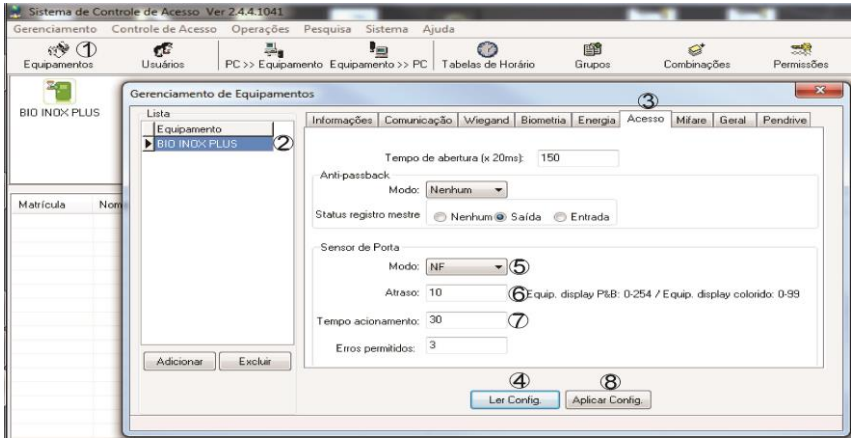
Atenção: O Anti Pass-Back deve ser usado com atenção, pois nenhum usuário tem acesso para liberar APB. Caso o Anti Pass-Back for utilizado incorretamente, o usuário terá seu acesso negado e acionará a saída COM2 e NO2, se tiver instalado um alarme nessa saída, o mesmo será acionado. Para parar o alarme, deve-se acessar a porta.

O único jeito de liberar o acesso é através de um usuário que não tenha utilizado APB incorretamente ou pela abertura remota pelo software.

10.4.3. Configuração do Sensor de Porta

Para configurar o sensor de porta siga os passos:

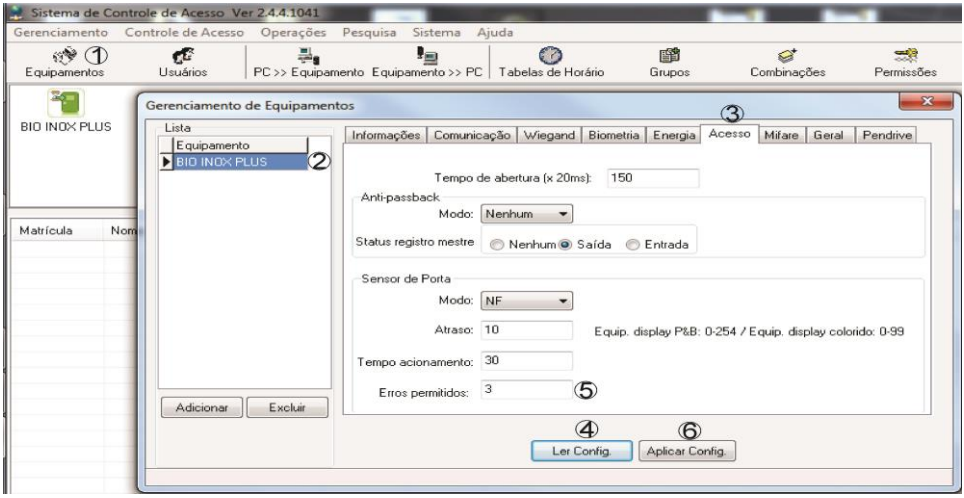
1. Na janela principal do software SoapAdmin clique no botão equipamentos(**1**), ao clicar a janela de gerenciamento de equipamentos será aberta;
2. Clique no equipamento que deseja configurar o sensor de porta (**2**);
3. Clique na aba Acesso(**3**);
4. Clique no botão Ler Config. (**4**) para ler as configurações do equipamento;
5. Configuração do sensor (**5**). Configure o tipo de sensor que está instalado em sua porta:
   5.1. Se for um sensor que tem seu estado normalmente fechado configure opção **NC.**
   5.2. Se for um sensor que tem seu estado normalmente aberto configure a opção **NO**.
   5.3. Se não possuir um sensor configure a opção **NONE**.
   Obs.: Se não utilizar um sensor de porta (**NONE**), as sinalizações de que a porta está aberta não serão acionadas.
6. Tempo atraso é o tempo que o equipamento levará para emitir um sinal que a porta está aberta após o tempo de abertura da porta ter excedido. Este sinal é sonoro e não aciona as saídas **COM2** e **NO2**(saída de alarme). Para configurar, basta escolher o tempo em atraso (**6**).
   Obs.: Caso ele seja acionado basta fechar a porta para que o sinal pare de ser emitido.
7. Tempo de acionamento do alarme é o tempo que o equipamento levará para acionar a saída **COM2** e **NO2** (saída de alarme). O tempo de acionamento do alarme será acionado quando o tempo de atraso for excedido. Para configura, basta escolher o tempo de acionamento(**7**).
   Obs.: Caso o alarme seja acionado para desativa-lo, deve-se passar um cartão cadastrado ou uma digital cadastrada para o alarme parar.
8. Clique no botão Aplicar Config. (**8**) para aplicar as configurações, uma janela de operação concluída será aberta;
9. Reinicie o equipamento;



10.4.4. Máximo de Falhas Seguidas em uma Identificação (Erros Permitidos)

Está opção configura a quantidade máxima de falhas seguidas admissíveis (erros permitidos) em uma operação de identificação de usuário. Por exemplo: se a configuração estiver ativada e um usuário não cadastrado tentar acessar o equipamento por mais vezes que o máximo de falhas admissíveis o equipamento acionará a saída COM2 e NA2 (saída do alarme).

1. Na janela principal do software SoapAdmin clique no botão equipamentos(**1**), ao clicar a janela de gerenciamento de equipamentos será aberta;
2. Clique no equipamento que deseja configurar a quantidade de erros permitidos (**2**);
3. Clique na aba Acesso(**3**);
4. Clique no botão Ler Config. (**4**) para ler as configurações do equipamento;
5. Escolha o máximo de falhas admissíveis em erros permitidos (**5**). Pode ser escolhido de 1 à 9 falhas. Se não quiser utilizar essa configuração, basta colocar 0;
6. Clique no botão Aplicar Config. (**6**) para aplicar a configuração, uma janela de operação concluída será aberta;
7. Reinicie o equipamento;



Atenção: Caso o alarme seja acionado, para desligá-lo, acesse a porta com um usuário cadastrado.
Se utilizar Anti Pass-Back não utilize máximo de falhas seguidas em uma identificação.

10.5. Eventos

O Bio Inox Plus tem um limite máximo de 100.000 eventos para serem armazenados. Quando chega nesse limite ele irá emitir uma mensagem de '' relógio está correndo'', então enquanto essa mensagem for emitida todos os eventos gerados não serão registrados.

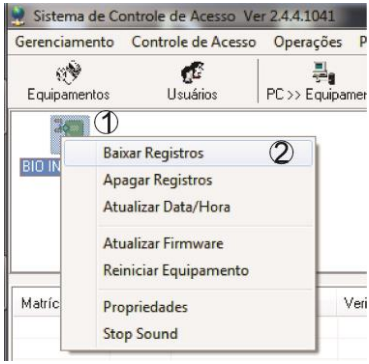
Para monitorar a saída ou a entrada no equipamento é necessário baixar os eventos.

Caso o dispositivo chegue os 100.000 eventos será necessário realizar a exclusão dos eventos armazenados através do software SoapAdmin. Recomendamos não deixar o equipamento chegar ao limite, pois serão perdidos todos registro depois do 100.000° evento.

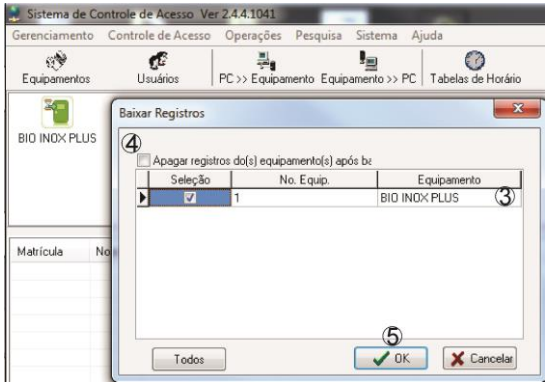
10.5.1. Baixar Eventos

Para baixar os eventos devem-se seguir os passos:

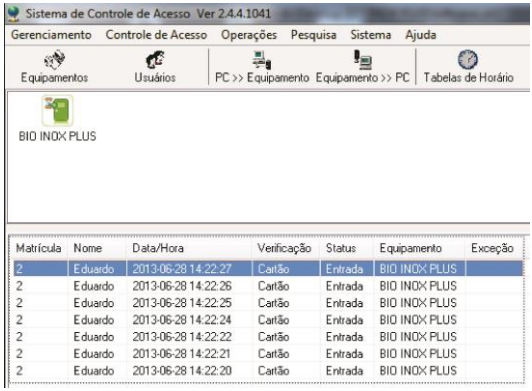
1. Clique com o botão direito do mouse (**1**) no equipamento que deseja baixar os eventos;
2. Clique em baixar registros (**2**), ao clicar a janela baixar registros será aberta;



3. Selecione o equipamento (**3**);
4. Se desejar baixar e excluir os eventos do equipamento, basta selecionar a opção '' apagar registos do(s) equipamento(s)'' (**4**);
5. Clique em OK (**5**) para baixar;



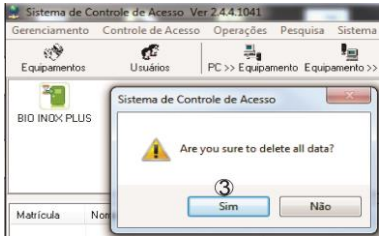
A imagem abaixo mostra os eventos baixados;



10.5.2. Excluir Eventos

Para excluir eventos do equipamento SEM armazená-los no computador, siga os passos:

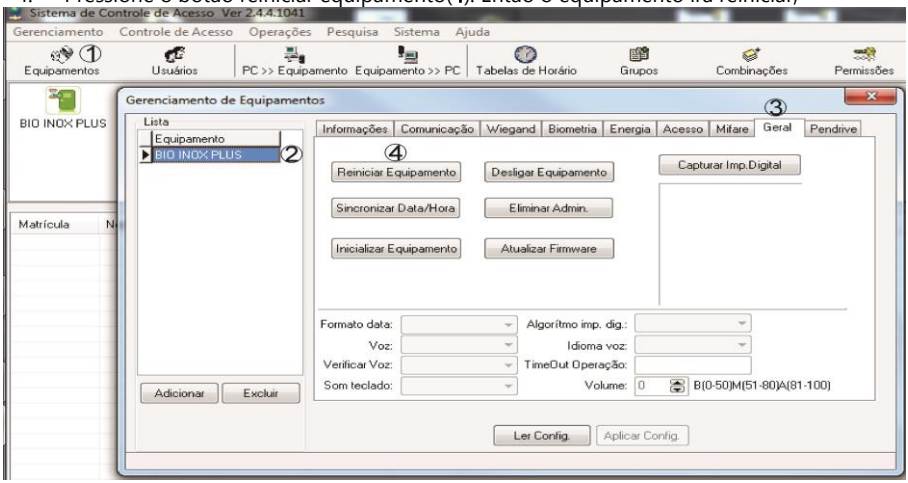
1. Clique com o botão direito do mouse (**1**) no equipamento que deseja excluir os eventos;
2. Clique em apagar registros (**2**), ao clicar a janela sistema de controle de acesso será aberta;
3. Clique em sim (**3**) para confirmar a exclusão.



10.6. Reiniciar o Equipamento

Para reiniciar o equipamento, basta seguir os passos abaixo:

1. Na janela principal do software SoapAdmin clique no botão equipamentos(**1**), ao clicar a janela de gerenciamento de equipamentos será aberta;
2. Clique no equipamento que deseja reiniciar (**2**);
3. Clique na aba Geral(**3**);
4. Pressione o botão reiniciar equipamento(**4**). Então o equipamento irá reiniciar;

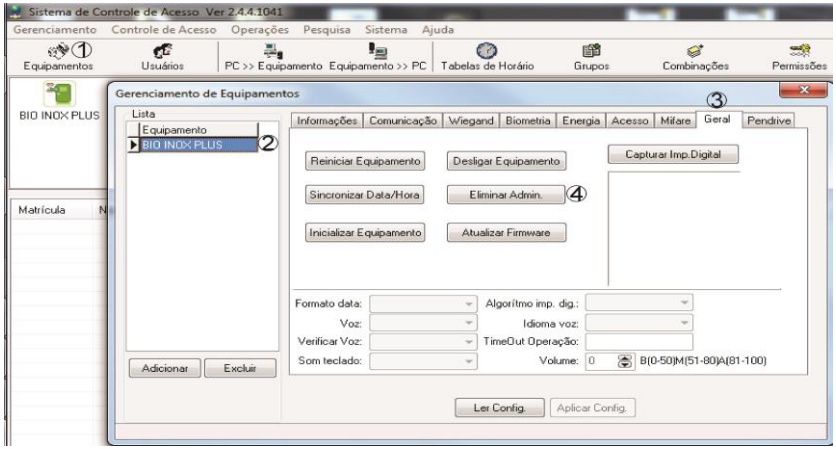


Outra forma de reiniciar o equipamento é apertar o botão de reinicialização no equipamento:

10.7. Retirar Privilégio de Administrador

Para retirar o privilégio de um administrador, ou seja, para transforma o usuário tipo administrador (cartão mestre) em um usuário comum, basta seguir os passos abaixo:

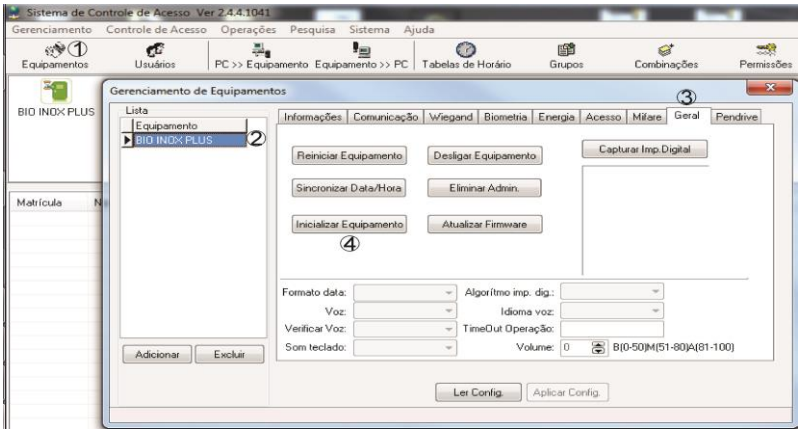
1. Na janela principal do software SoapAdmin clique no botão equipamentos(**1**), ao clicar a janela de gerenciamento de equipamentos será aberta;
2. Clique no equipamento que deseja retirar o privilégio do administrador (**2**);
3. Clique na aba geral (**3**);
4. Pressione o botão eliminar admin(**4**).
5. Reinicie o equipamento;
6. O equipamento irá emitir uma mensagem para cadastrar um novo administrador.



10.8. Reiniciar o Equipamento

Para '' apagar tudo'', ou seja, apagar os log (eventos) realizados, apagar todos os tipos de usuários e reinicia todas as operações do equipamento. Acesse o menu opções avançadas e siga os passos:

1. Na janela principal do software SoapAdmin clique no botão equipamentos(**1**), ao clicar a janela de gerenciamento de equipamentos será aberta;
2. Clique no equipamento que deseja reiniciar (**2**);
3. Clique na aba geral (**3**);
4. Pressione o botão inicializar equipamento (**4**).
5. Reinicie o equipamento;
6. O equipamento irá emitir uma mensagem para cadastrar um novo administrador.



Está opção não restaura as opções que foram modificadas em opções de acesso

10.9. Reset do IP do Equipamento

Para reiniciar o IP do equipamento, ou seja, para que o IP volte a ser o de fábrica 192.168.1.201, basta seguir os passos abaixo:

1. Desligue o equipamento;
2. Retire o suporte de fixação do equipamento da parede;
3. Encaixe o suporte novamente, fazendo que o sensor magnético fique fechado e ligue o dispositivo; (veja a imagem abaixo que mostra onde fica o sensor magnético no equipamento)
4. Depois que a voz começar a falar, retire o suporte do equipamento, fazendo com que o sensor magnético fique aberto;
5. Espere 30 segundos.
6. Ao terminar o tempo, recoloque o suporte, ou seja, aproxime o imã do sensor magnético na sua posição padrão por 3 vezes, cada vez que aproximar deve-se ouvir um "*beep*".
7. Reinicie o equipamento;
8. O IP que estava cadastrado anteriormente não deve funcionar, pois o IP foi restaurado para 192.168.1.201.

11. Detalhes e cuidados com o leitor biométrico

1. Evitar excesso de incidência de luz diretamente sobre o sensor.
Os leitores biométricos óticos são sensíveis à incidência direta da luz ambiente sobre a sua superfície, principalmente luz fluorescente branca ou luz solar.
O que poderá ocorrer é gerar falsas tentativas de acesso ou até mesmo falhas na leitura da biometria. Nesses casos, recomenda-se rever o posicionamento do produto ou dos pontos de entrada de luz e iluminação do ambiente. Procure manter a tampa de proteção sempre fechada, quando não estiver utilizando o leitor biométrico

2. Não pressionar demasiadamente o dedo no sensor do scanner.
Isso distorce a imagem da digital, não permitindo que o sensor biométrico ótico identifique os pontos formados pelas intersecções das linhas (cristas e vales) que compõem a digital.

3. Não posicionar apenas a ponta do dedo no scanner.
Quando isso acontece, em geral é porque o usuário está em pé, ou utiliza um cadastrador de mesa. O uso inadequado do scanner no momento da leitura da digital impede que o sistema transmita uma imagem capaz de ser transformada em um template.

4. **Não alterar o Match Limiar, após cadastrar usuários.**
Ao alterar essa configuração, é modificado o grau de comparação da biometria do usuário com o que está armazenado no equipamento. Isso pode gerar acessos negados ou até mesmo entradas não autorizadas.

!!! ATENÇÃO !!!

- Falta de limpeza adequada da lente aliada à incidência de luz diretamente no sensor ótico, pode gerar acesso indevido.

- SEMPRE posicione o dedo no leitor de forma que o núcleo da impressão digital fique centralizado como na figura da direita.

12. Termo de Garantia

Fica expresso que esta garantia 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 defeitos de fabricação que porventura venham a apresentar, pelo prazo de 90 (noventa) dias de garantia legal, mais 9 (nove) meses de garantia contratual, contados a partir da data da entrega do produto ao Consumidor, conforme consta na Nota Fiscal de compra do produto, que é parte integrante deste Termo em todo território nacional.
2. A Intelbras não se responsabiliza pela instalação deste equipamento, e também por eventuais danos ~~a~~ decorrentes de roubos, furtos, assaltos, tentativas de fraudes e/ou sabotagens pelo uso de seus produtos. É dever do Consumidor acionar um profissional idôneo, capacitado e especializado. O equipamento é garantido contra defeitos 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 interfiram o seu correto funcionamento.
3. Constatado o defeito no produto, o Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado, por intermédio dos meios de contatos divulgados no manual do produto ou através do telefone (48) 2106-0071, ou ainda, através do e-mail suporte@intelbras.com.br, para que possa ser orientado acerca da forma mais ágil de examinar e sanar o defeito durante o prazo de garantia aqui previsto. Caso o Consumidor leve o produto a quem não está autorizado, a garantia perderá sua validade, já que o produto será considerado violado.
4. A garantia perderá ainda sua validade se ocorrer qualquer das hipóteses a seguir: **a)** se o defeito não for decorrente de fabricação; **b)** o defeito ou danos no produto tiver sido causado pelo Consumidor e/ou terceiros estranhos ao fabricante, ou em decorrência de obras de engenharia civil defeituosas; **c)** se os danos ao produto forem oriundos de acidentes, sinistros, agentes da natureza (raios, inundações, desabamentos, etc.), incêndios, umidade, tensão na rede elétrica (sobretensão provocada por acidentes ou flutuações excessivas na rede), instalação/uso em desacordo com o Manual do Usuário ou decorrente do desgaste natural das partes, peças e componentes; **d)** se o produto tiver sofrido influência de natureza química, eletromagnética, elétrica ou animal (insetos, etc.); **e)** se o número de série do produto houver sido adulterado ou rasurado.
5. Na eventualidade do Consumidor solicitar o atendimento domiciliar, deverá contatar o Serviço Autorizado, através dos contatos acima disponibilizados, para que possa ser informado sobre a disponibilidade de atendimento domiciliar em sua região, e caso disponível, quem poderá contatar para consulta da taxa de visita técnica. Caso seja constatada a necessidade da retirada do produto, as despesas decorrentes de transporte, bem como a segurança de ida e volta do produto, ficam sob a responsabilidade do Consumidor.
6. A garantia oferecida através deste termo limita-se ao acima exposto e, com a reparação ou substituição do produto defeituoso a Intelbras satisfaz a garantia integral, não cabendo ao Consumidor pleitear quaisquer outros tipos de indenização ou coberturas, exemplificativamente, porém não limitativos, lucros cessantes, prejuízos originários de paralização do equipamento, danos causados inclusive a terceiros, por acidentes decorrentes do uso do equipamento

Automatiza Ind. e Com. de Equipamentos

R: Albatroz, 35 - Tecnopark Pedra Branca

Palhoça - SC - CEP: 88137-290

PABX + 55 48 2106-0071