



Uma marca do Grupo Intelbras

---

# Manual do usuário

**SoapAdmin 3.5**

# ΑΥΤΟΜΑΤΙΖΑ

## SoapAdmin 3.5

### Software para gerenciamento do sistema de controle de acesso

O SoapAdmin 3.5 é um software de gerenciamento de dispositivos para controle de acesso, entrada/saída de usuários em um ou vários ambientes onde o acesso de pessoas deva ser controlado.

# Índice

1. Apresentação	5
2. Instalação	6
2.1. Especificações de servidor	6
2.2. Processo de instalação	7
2.3. Pré-requisitos e requisitos recomendados	13
3. Iniciando o software SoapAdmin 3.5	13
4. Adicionando áreas	15
5. Adicionando dispositivos	19
5.1. Adicionar dispositivos STDSKD	19
5.2. Adicionar dispositivos Pull SDK	21
5.3. Demais configurações comuns a ambos os tipos de dispositivos	23
6. Controle de acesso	28
6.1. Zona de tempo	28
6.2. Feriados	29
6.3. Perfil de acesso	31
6.4. Configuração de portas	34
6.5. Intertravamento	37
6.6. Anti-passback	39
6.7. Ações vinculadas a eventos	41
6.8. Abertura temporizada	42
6.9. Acesso combinado	45
6.10. Monitoramento	48
6.11. Planta baixa	49
6.12. Nome da leitora	51
6.13. Entradas e saídas auxiliares	52
7. Usuários	53
7.1. Departamentos	53
7.2. Sétimo passo usuários	55
7.3. Cadastro de usuários em lote	57
8. Relatórios	64
9. Sistema	69
9.1. Permissão de operador	69
9.2. Operador	70
9.3. Trocar senha de operador	72
9.4. Gerenciamento do banco de dados	73
9.5. Configurações do sistema	76
9.6. Navegação	77
9.7. Seleção de idioma	77
9.8. Módulos opcionais	78

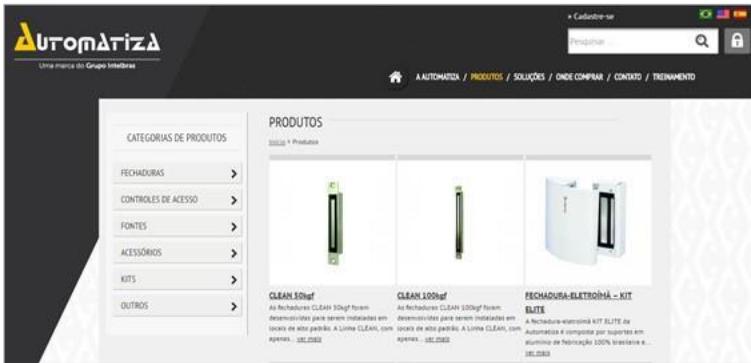
10. Ajuda	78
Termo de uso do software Soapadmin 3.5	79
1.1. ACEITAÇÃO.....	79
1.2. LICENÇA LIMITADA .....	79
1.3. ALTERAÇÕES, MODIFICAÇÕES E RESCISÃO .....	79
1.4. CONSENTIMENTO PARA COLETA E USO DE DADOS.....	79
1.5. ISENÇÃO DE GARANTIAS E LIMITAÇÕES DE RESPONSABILIDADE .....	79
1.6. FORO PARA DIRIMIR CONTROVÉRSIAS .....	80

# 1. Apresentação

Com o SoapAdmin 3.5, é possível configurar privilégios e permissões diferentes para cada perfil de pessoa, tornando o sistema versátil e adequado à realidade de sua empresa. No software, estão disponíveis várias modalidades de relatórios gerenciais, cujos dados podem ser agrupados por dia, semana e mês.

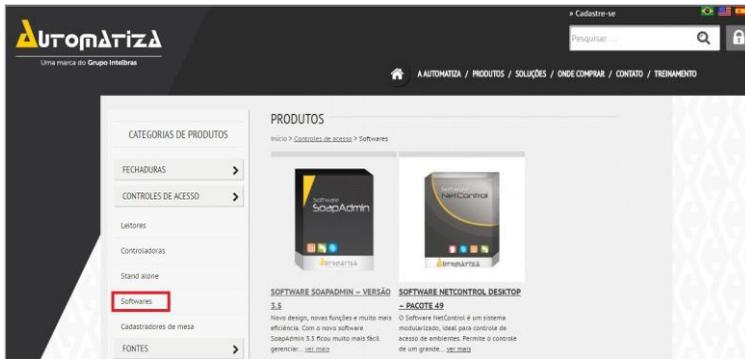
Todo esse controle e gerenciamento está a sua disposição gratuitamente através do site da Automatiza [www.automatiza.com.br](http://www.automatiza.com.br) / [www.intelbras.com.br](http://www.intelbras.com.br). Basta observar os passos descritos a seguir para poder desfrutar do máximo de controle e segurança oferecido pelo software SoapAdmin 3.5.

1. No seu navegador web, digite o endereço [www.automatiza.com.br](http://www.automatiza.com.br);
2. Na página principal, selecione a opção Produtos;



Opção Produtos site Automatiza

3. Na nova tela de Produtos selecione a guia Controle de acesso/Software;



Opção Softwares na guia Controle de acesso

4. Por fim, clique sobre a opção Software SoapAdmin - versão 3.5 e na nova tela, na guia Suporte e download, clique sobre o link Software e instalação e aguarde o processo de download terminar.



Download do pacote para instalação do software SoapAdmin 3.5

O software SoapAdmin 3.5 é habilitado a gerenciar controladoras da linha CT 500 e os dispositivos stand alone NEO, DUO, Bio Inox Plus e SS 411E, divididos por tipo de SDK, exemplificados na tabela a seguir:

Nome do dispositivo	Tipo de SDK
NEO SS 410 / NEO SS 420	Disp. STDSKD
DUO SS 210 / SS 220	Disp. STDSKD
Bio Inox Plus SS 311E	Disp. STDSKD
SS 420 / SS 420 MF	Disp. STDSKD
DUO SS 230 / DUO SS 230 MF	Disp. STDSKD
IBPROX SS 120	Disp. STDSKD
Bio Inox Plus SS 311 MF	Disp. STDSKD
SS 610	Disp. STDSKD
SS 710	Disp. STDSKD
SS 411E	Disp. Pull SDK
SS 320 / SS 320 MF	Disp. Pull SDK
SS 411E	Disp. Pull SDK
Série CT 500 (1P/1PB, 2P/2PB, 4P/4PB)	Controladora para 1 porta, 2 portas e 4 portas

Tipos de dispositivos de controle de acesso

Após o download do software, acompanhe as orientações de instalação disponíveis no tópico a seguir.

## 2. Instalação

### 2.1. Especificações de servidor

Observe a seguir as especificações mínimas de configuração que o servidor que irá armazenar o banco de dados do software SoapAdmin 3.5 deverá ter para seu correto funcionamento e para o correto funcionamento do software. No caso de estarem sendo utilizados processadores mais antigos, o software pode apresentar lentidão.

Quantidade de dispositivos	Configuração do servidor
Até 50	4 GB de memória RAM ou mais
	Processador de 3 GHz ou superior, preferencialmente Dual Core
	10 GB de espaço livre em disco (para instalação, não considerando o crescimento da base de dados)
	Placa de rede com capacidade de 100 Mbps ou mais
	Net Framework 3.0 / 3.5

Configurações do servidor

**Obs.:** para processadores mais antigos este produto não funciona de maneira estável e pode apresentar lentidão ou travamento.

**Importante:** o espaço de 10 GB livres necessário refere-se apenas ao espaço ocupado pela instalação do software, não considerando o tamanho do banco de dados utilizado.

## 2.2. Processo de instalação

Após a conclusão do download do software, executado no tópico 1. Apresentação anterior, é necessário instalar o pacote no servidor. Para isso, execute o processo descrito a seguir:

1. Dê um duplo clique sobre o ícone executável do software Setup.exe;
2. Na nova tela, escolha o idioma para instalação e clique em Ok;



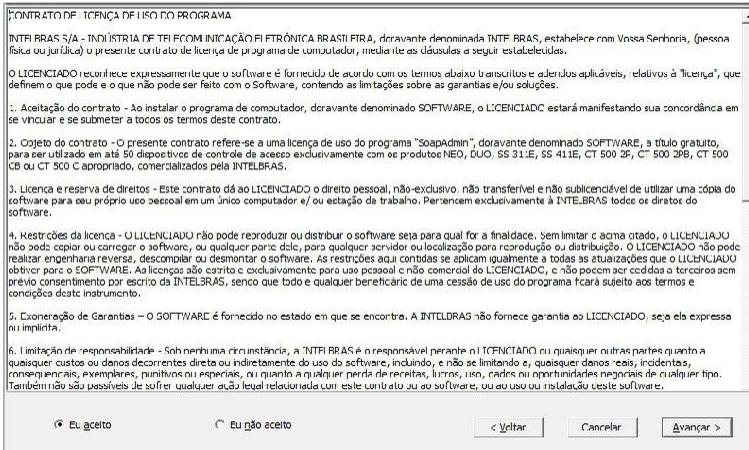
Setup de instalação

3. Uma nova tela surgirá. Nesta tela, clique em Avançar;



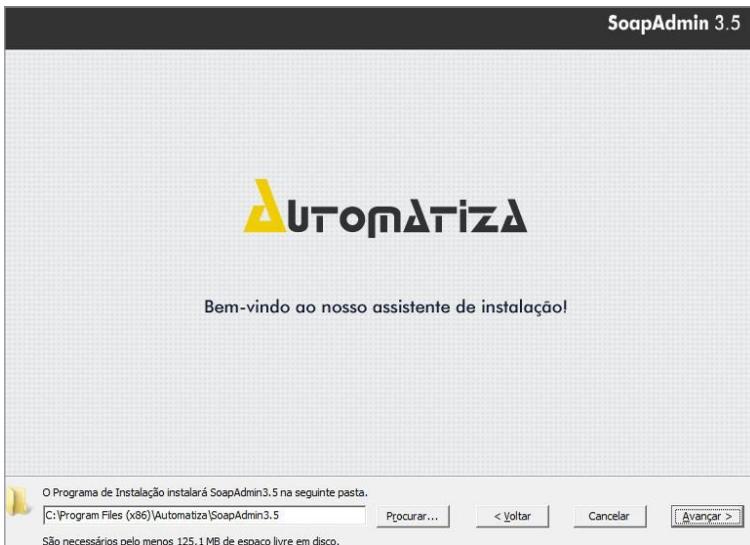
Tela inicial do assistente de instalação

4. No passo seguinte é necessário aceitar os termos Contrato de Licença do software. Após a leitura, clique na opção Eu aceito e na sequência em Avançar;



Contrato de licença do software

5. Na tela a seguir, é exibido o local em que os arquivos do pacote de instalação serão instalados. Nessa tela, clique em Avançar;



Local de instalação do software

6. Na nova tela, o assistente de instalação irá demonstrar o processo de criação do ícone de atalho para o software. Nessa tela clique em Avançar;



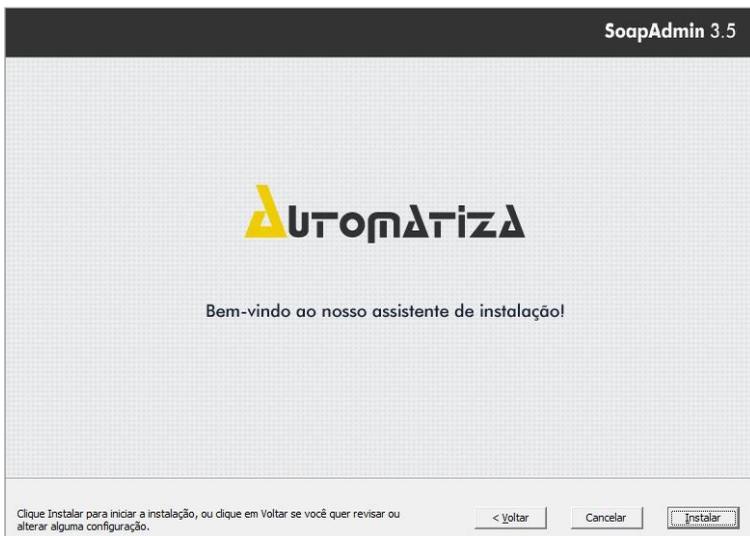
Atalho para o software

7. Na nova tela, é necessário definir onde será armazenado o backup de redundância do banco de dados do software. Este backup é uma cópia duplicada do backup-padrão do software. Após a definição clique em Avançar;



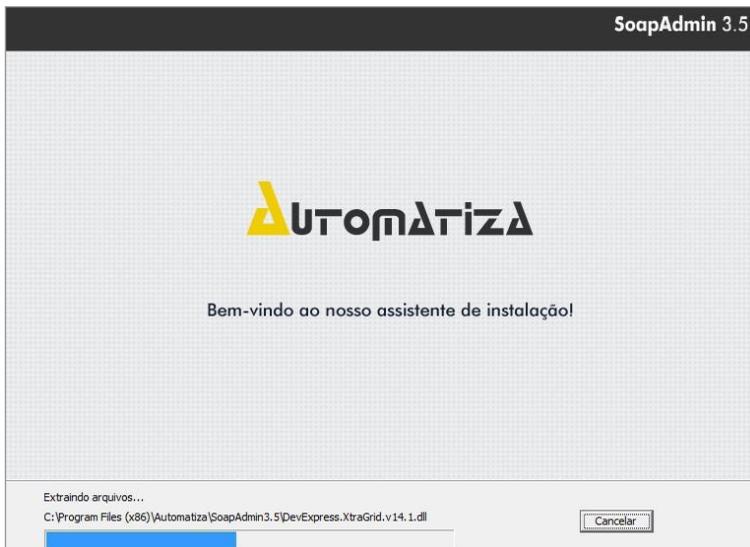
Definição do armazenamento do banco de dados

8. Por fim, clique na opção Instalar na nova tela do assistente de instalação;



Confirmação de instalação do software

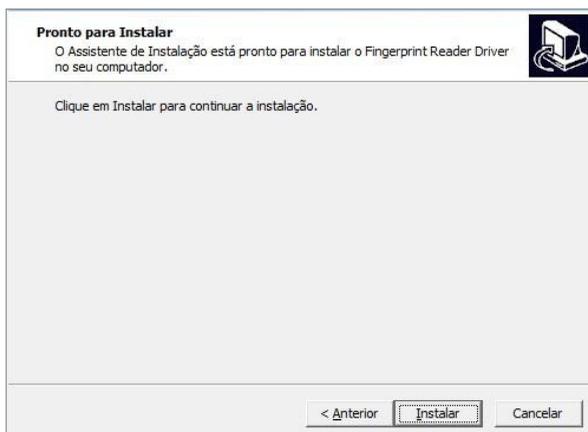
9. Acompanhe os processos abaixo e selecione Avançar, Instalar e Concluir nas novas telas que surgirem;



Progresso de instalação



Instalação do driver de biometria digital



Instalação do driver de biometria digital



Conclusão de instalação do driver de biometria digital

10. Ao final do processo de instalação, selecione a opção Sim, deseje reiniciar o computador agora e, em seguida, clique em Concluir.

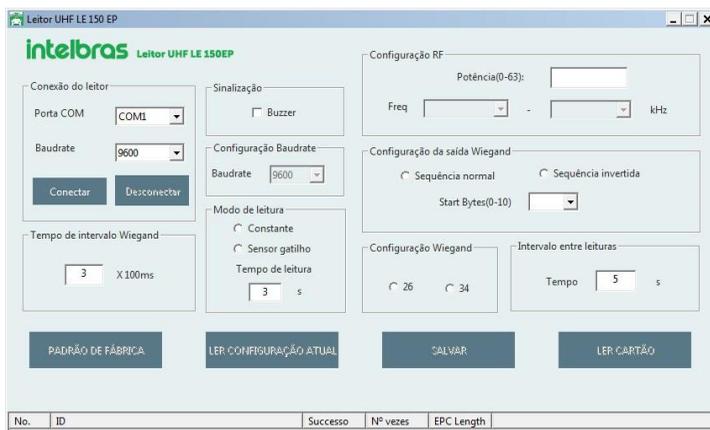


Conclusão de instalação do software SoapAdmin 3.5

- Importante:** » O pacote de instalação também instalará automaticamente o software de configuração da Antena UHF Intelbras LE 150EP, bem como o respectivo ícone de atalho na área de trabalho do computador. Para as informações de configuração da Antena UHF através deste Software, consulte o manual do produto LE 150EP.
- » Após a instalação do software, para sua correta execução e funcionamento, é necessário que o mesmo seja executado em modo Administrador. Caso outros operadores utilizem o mesmo servidor ou máquina cliente, será necessário atribuir a todos o perfil de administrador da máquina servidor ou cliente no sistema operacional.



Ícone de atalho para software Antena UHF



Tela inicial do software de configuração do Leitor UHF 150EP

### 2.3. Pré-requisitos e requisitos recomendados

Para o bom funcionamento do software SoapAdmin 3.5 em conjunto com os dispositivos de controle de acesso, observe as informações a seguir:

- » Configurações recomendadas:
  - » Processador de 3 GHz ou superior, preferencialmente Dual Core.
  - » 1 GB de espaço livre em disco (para instalação, não considerando o crescimento da base de dados).
  - » 4 GB de memória RAM ou mais.
  - » Placa de rede com capacidade de 100 Mbps.
  - » Windows® 7 (32 bits e 64 bits), Windows® 8 (32 bits e 64 bits) e Windows® 10 (32 bits e 64 bits).

**Obs.:** para um melhor desempenho, o ciclo de operação (escrita/leitura) de cada componente deve ser levado em consideração.

- » Pré-requisitos:
  - » O Net Framework deve ser previamente instalado.

## 3. Iniciando o software SoapAdmin 3.5

Após a conclusão do processo de instalação do software, deve-se abri-lo e fazer o login de usuário no dispositivo para iniciar seu gerenciamento. Para isso, execute os passos a seguir:

1. Dê um duplo clique no ícone de atalho criado pelo software SoapAdmin 3.5 na área de trabalho de seu computador, conforme a figura a seguir:



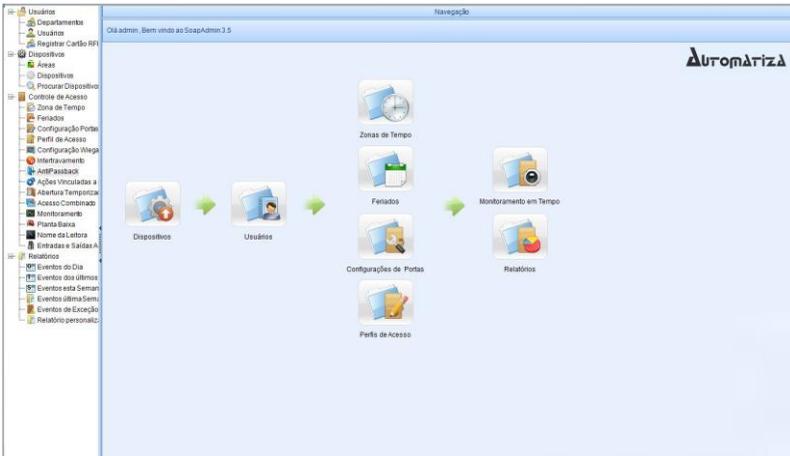
Ícone de atalho do software SoapAdmin 3.5

2. Digite admin para logar como operador-padrão do sistema, nos campos demonstrados na figura a seguir;
  - » Operador-padrão: admin.
  - » Senha-padrão: admin.

Tela de login do software SoapAdmin 3.5. O cabeçalho da janela contém o logotipo "ΑΥΤΟΜΑΤΙΣΤΑ" em amarelo e o texto "SoapAdmin 3.5" em branco. Abaixo, há dois campos de entrada: "Operador:" com o texto "admin" e "Senha:" com caracteres ocultos por asteriscos. Cada campo possui um ícone de olho para alternar a visibilidade e um asterisco vermelho à direita. Na base da janela, há dois botões: "OK" e "Cancela".

Tela de login no software

3. Na tela principal, estão apresentadas em ordem de prioridades, as principais funções que devem ser executadas para a correta configuração do sistema de controle de acesso.



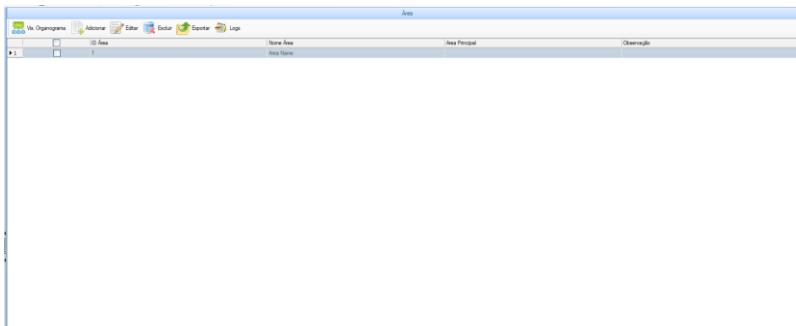
Tela de navegação do software

A ordem de configurações obedece o exposto a seguir. Essa ordem é importante, pois estabelece as condições necessárias para os posteriores vínculos entre as diversas funções do software, tornando assim os relatórios de gerenciamento de controle de acesso mais completos e abrangentes.

- » **Adicionar áreas:** opção disponível em Dispositivos, sua função é mapear as diversas áreas da empresa ou organização que devam ser monitoradas e controladas pelo sistema de controle de acesso.
- » **Adicionar dispositivo:** opção disponível em Dispositivos, sua função é inserir no software o dispositivo ou os dispositivos que serão utilizados pelo sistema de controle de acesso, podendo variar em diferentes tipos, tal qual exemplificado no tópico 1. Apresentação deste manual.
- » **Adicionar zonas de tempo:** opção disponível em Controle de acesso. Sua função é determinar os horários em que o sistema de controle de acesso estará disponível para acesso de usuários dentro de um horizonte semanal, vinculando a esses horários os respectivos dispositivos que compõem o sistema de controle de acesso, bem como seus usuários. O software dispõe de uma zona de tempo-padrão que abrange 24h, disponível semanalmente.
- » **Adicionar feriados:** opção disponível em Controle de acesso, sua função é mapear todos os feriados existentes em um horizonte anual, bem como aqueles que são recorrentes, tais como Natal e ano-novo. Posteriormente, também é possível associar esses feriados aos dispositivos do sistema de controle de acesso, bem como configurar exceções de permissões de acessos entre o banco de usuários.
- » **Configuração de portas:** opção disponível em Controle de acesso, sua função é determinar o modo como a porta controlada irá funcionar através do respectivo dispositivo instalado nela. Parâmetros como tempo de abertura de porta, métodos de autenticação para acesso, zona de tempo habilitada, entre outros, são configurados por meio dessa função.
- » **Perfil de acesso:** opção disponível em Controle de acesso, sua função é criar um perfil de acesso que deverá ser vinculado à zona de tempo criada anteriormente. Nesse momento, serão vinculados também os respectivos dispositivos ao perfil criado, bem como determinados usuários do banco de dados do sistema, essa avaliação é feita pelo operador administrador do sistema, que é quem gerencia o sistema de controle de acesso.
- » **Departamentos:** opção disponível em Usuários, sua função é mapear os diferentes departamentos ou setores da organização, para possibilitar o vínculo de cada usuário cadastrado ao seu respectivo departamento.
- » **Usuários:** opção disponível em Usuários, essa função permite que sejam inseridos os usuários que acessam os ambientes controlados pelo sistema de controle de acessos. Nessa função, também é possível cadastrar os métodos de autenticação preferenciais para cada perfil, bem como vínculos de perfis de acesso criados previamente e informações administrativas do usuário.
- » **Relatórios de eventos:** opção disponível em Relatórios, essa função possibilita criar relatórios dos eventos gerados durante o tempo de operação do sistema de controle de acesso e também possibilita gerar relatórios personalizados de acordo com a necessidade da empresa, bem como os eventos de exceção as regras criadas e configuradas anteriormente.

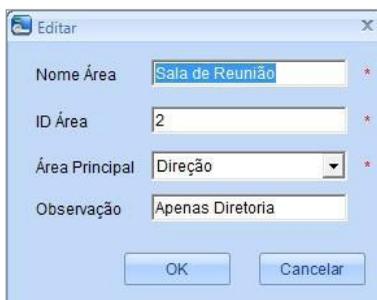
## 4. Adicionando áreas

1. Este é o primeiro passo após a instalação do software SoapAdmin 3.5, aqui serão mapeadas todas as áreas da empresa que se deseja controlar. Após efetuar login no software selecione a opção Áreas, localizada em Dispositivos e selecione Adicionar, como demonstrado na figura a seguir:



Tela de visualização de áreas

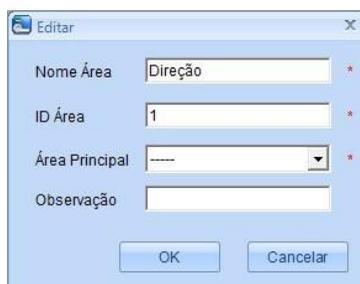
2. Na nova tela, digite o nome da área a ser adicionada e o ID dessa área (numeral sequencial). Deve-se vincular a nova área à área principal já criada anteriormente na metodologia de um organograma. Por fim, clique em Ok para gerar a nova área;

A screenshot of the 'Editar' dialog box in SoapAdmin 3.5. The dialog has a title bar with a close button. It contains four fields: 'Nome Área' with the value 'Sala de Reunião', 'ID Área' with the value '2', 'Área Principal' with a dropdown menu showing 'Direção', and 'Observação' with the value 'Apenas Diretoria'. There are 'OK' and 'Cancelar' buttons at the bottom.

Adicionando áreas

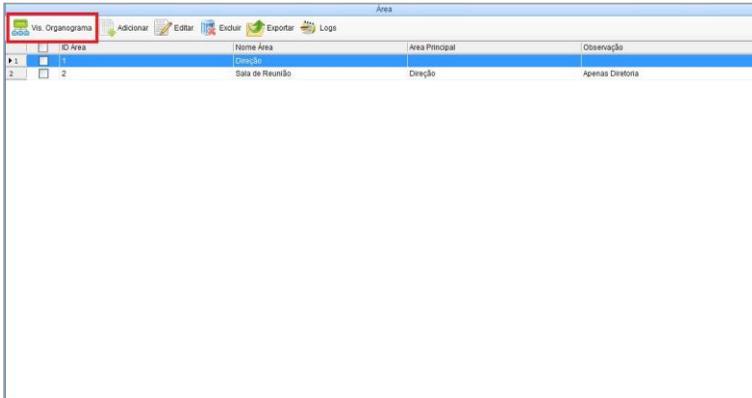
**Obs.:** o software já traz de fábrica uma área raiz cadastrada, de nome Área name, que não pode ser excluída, contudo, é possível editá-la para o nome que faça mais sentido à real necessidade do cliente. Para isso, selecione a área na tela inicial de visualização das áreas, clique em Editar e então repita os passos descritos no tópico anterior.

**Importante:** a área raiz não possui vínculos com nenhuma área principal acima dela, para essa área, o campo Área principal não é preenchido. Nessa área o seu ID-padrão é representado pelo numeral (1). Ao final da edição, clique em Ok para salvar as modificações.

A screenshot of the 'Editar' dialog box in SoapAdmin 3.5, showing the root area. The dialog has a title bar with a close button. It contains four fields: 'Nome Área' with the value 'Direção', 'ID Área' with the value '1', 'Área Principal' with a dropdown menu showing '-----', and 'Observação' which is empty. There are 'OK' and 'Cancelar' buttons at the bottom.

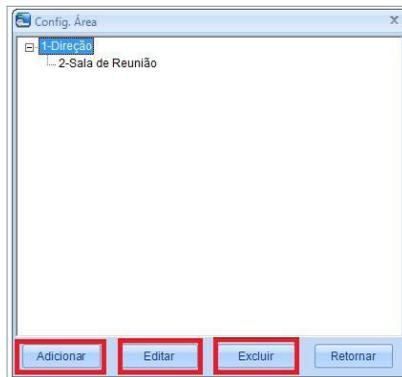
Edição de área raiz

3. Após adicionar e editar todas as áreas necessárias, é possível visualizar o organograma de áreas da empresa ou organização, para isso, na tela de visualização de áreas, clique sobre o botão Vis. organograma;



Visualização de Vis. Organograma

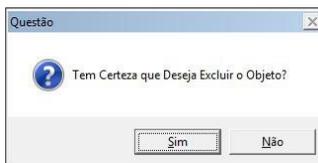
4. Caso necessário, pode-se adicionar, editar ou excluir alguma das áreas por meio da tela que será aberta. Feitos os devidos ajustes, clique no botão Retornar para sair;



Visualização de organograma

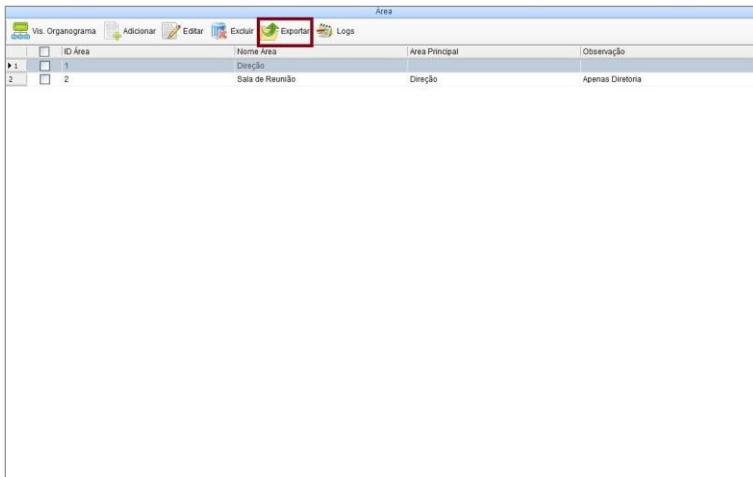
**Obs.:** as áreas são representadas na ordem de vínculos de hierarquia, da mais importante para a menos importante.

**Importante:** para excluir uma das áreas existentes (exceto a área raiz), basta selecionar a área desejada e clicar sobre o botão Excluir na visualização do organograma ou na tela inicial de áreas. Uma mensagem de texto será exibida, perguntando se deseja confirmar a exclusão. Em caso afirmativo, clique em Sim, do contrário clique em Não na caixa de texto.

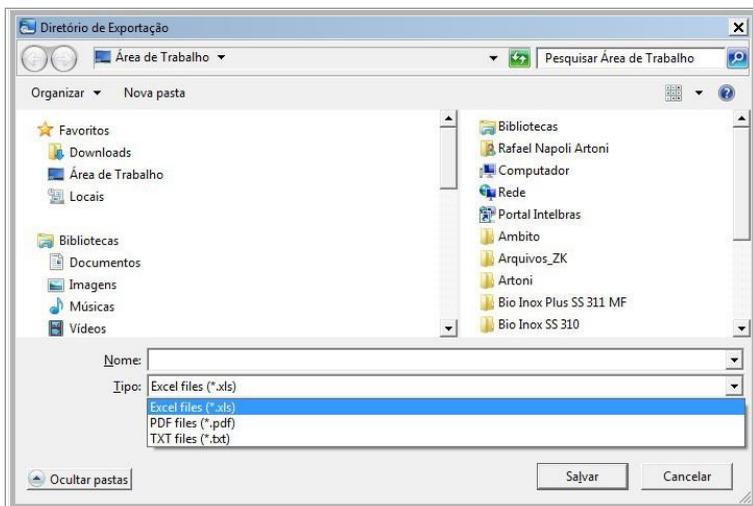


Confirmação de exclusão de área

5. É possível exportar as áreas cadastradas para um arquivo externo nas extensões .xls (Excel), .pdf (PDF) e .txt (Bloco de notas). Para isso, na tela de visualização das áreas, clique sobre o botão Exportar. Na nova tela, selecione o nome, a extensão e o local de armazenamento do arquivo e, por fim, clique em Salvar para concluir ou Cancelar para voltar à tela de visualização de áreas;

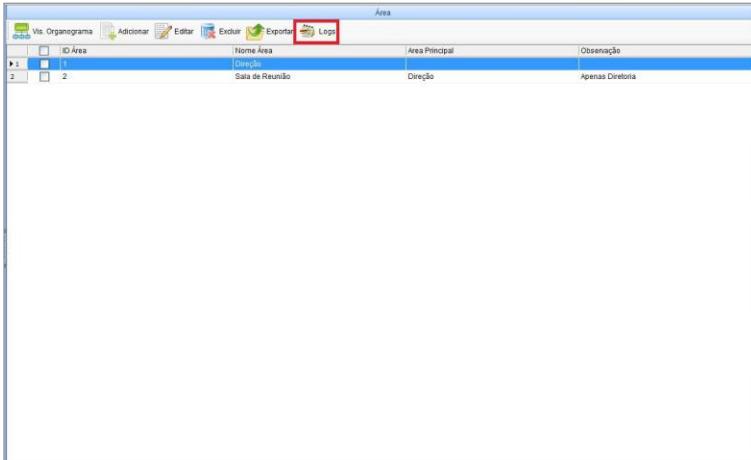


Botão função Exportar

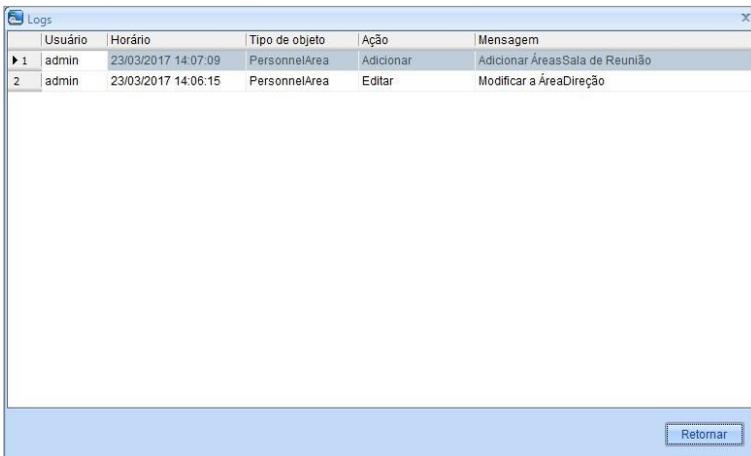


Diretório de exportação de áreas

6. Ainda na função Áreas é possível conferir as últimas movimentações e alterações efetuadas, para isso, clique sobre o botão Logs para verificar a lista de modificações, bem como o usuário no software responsável pela alteração. Para retornar à tela de visualização de áreas, clique no botão Retornar, na nova tela que se abrirá.



Botão Logs



Lista de Logs

## 5. Adicionando dispositivos

Após criar as devidas áreas, deve-se adicionar os dispositivos que farão parte do sistema de acesso. Na tabela a seguir estão listados os modelos de dispositivos e seus respectivos tipos de SDK.

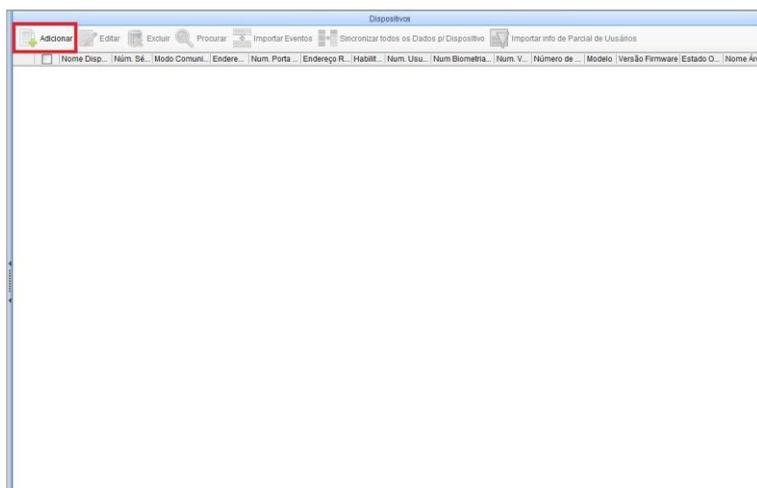
Nome do dispositivo	Tipo de SDK
NEO SS 410 / NEO SS 420	Disp. STDSDK
DUO SS 210 / SS 220	Disp. STDSDK
Bio Inox Plus SS 311E	Disp. STDSDK
SS 420 / SS 420 MF	Disp. STDSDK
DUO SS 230 / DUO SS 230 MF	Disp. STDSDK
IBPROX SS 120	Disp. STDSDK
Bio Inox Plus SS 311 MF	Disp. STDSDK
SS 610	Disp. STDSDK
SS 710	Disp. STDSDK
SS 411E	Disp. Pull SDK
SS 320 / SS 320 MF	Disp. Pull SDK
SS 411E	Disp. Pull SDK
Série CT 500 (1P/1PB, 2P/2PB, 4P/4PB)	Controladora para 1 porta, 2 portas e 4 portas

Tipos de dispositivos compatíveis com o software

Existem duas formas de adicionar os dispositivos no sistema (dispositivos STDSDK e dispositivos Pull SDK). Confira as particularidades de cada uma delas a seguir:

### 5.1. Adicionar dispositivos STDSDK

1. Na tela inicial da função Dispositivos, clique sobre o botão Adicionar para digitar as informações pertinentes ao dispositivo a ser adicionado;



Tela inicial dispositivos

2. Na nova tela, preencha as informações da guia Parâmetros básicos, observando na tabela acima Tipos de dispositivos compatíveis com o software o tipo de controlador de acesso que será adicionado;

Adicionar

Parâmetros Básicos

Nome Dispositivo \*

Senha Comunicação

Tipo de Controlador de Acesso Controladora para 2 Portas

Troca para Duas-Portas Bidirecional

Sincronismo automático de Hora

Área \*

Excluir Dados do Dispositivo ao Adicionar

Modo Comunicação TCP/IP RS485

Endereço IP \*

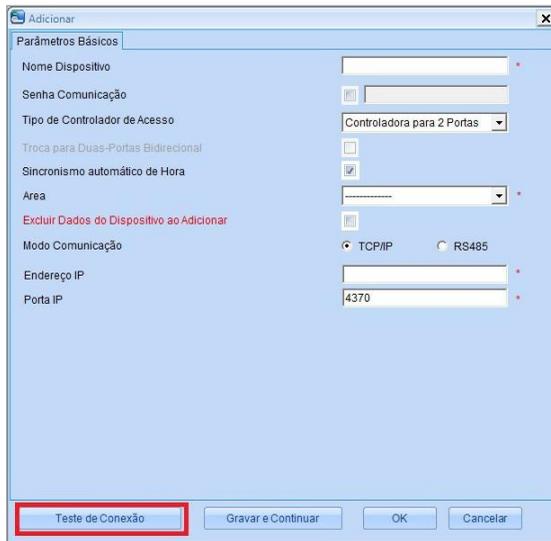
Porta IP 4370 \*

Teste de Conexão Gravar e Continuar OK Cancelar

Adicionando dispositivo

3. Digite o endereço de IP-padrão do equipamento, que pode ser encontrado no respectivo manual do dispositivo que se pretende adicionar, para comunicações TCP/IP, ou o endereço RS485 para dispositivos desse padrão de comunicação. Vincule também a área a que esse dispositivo pertence, cadastrada no tópico 4. Adicionando áreas;  
**Importante:** verifique o padrão de comunicação disponível em seu dispositivo antes de adicioná-lo ao software.
4. Durante o preenchimento, para a garantir o correto funcionamento do dispositivo, marque a opção Excluir dados do dispositivo ao adicionar, que é apresentada com letras na cor vermelha;  
**Importante:** não marque essa opção caso já possua usuários e eventos cadastrados no seu dispositivo, caso contrário, eles serão excluídos.

5. Após o preenchimento das informações, clique no botão Teste de conexão para validar a comunicação com o dispositivo;

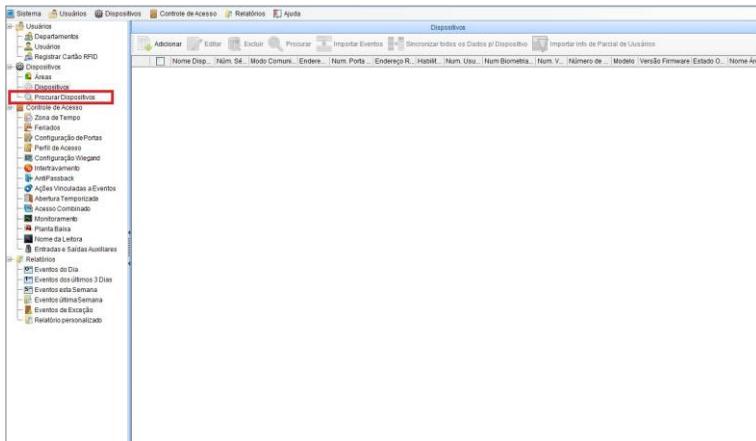


Testando conexão

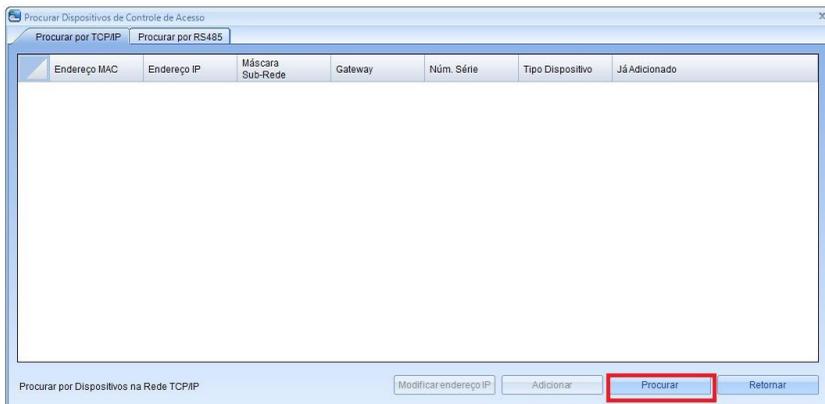
6. Clique no botão Gravar e continuar para adicionar mais de um dispositivo ou clique no botão Ok para salvar o dispositivo e finalizar o processo de cadastro.

## 5.2. Adicionar dispositivos Pull SDK

1. Os equipamentos do tipo Disp. Pull SDK e as controladoras para 1, 2 e 4 portas podem ser encontrados na rede sem a necessidade de inserção manual de seu endereço de IP, através do botão Procurar dispositivos disponível em Dispositivos;



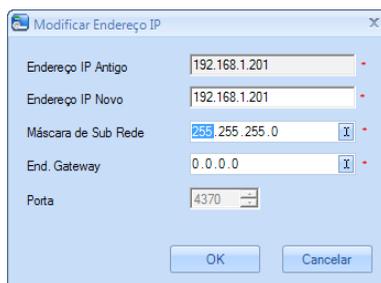
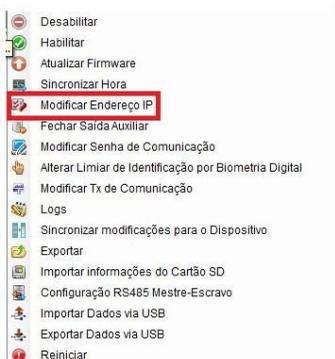
Procurar dispositivos



Procurando dispositivo

A lista de equipamentos será exibida na nona tela acima, basta selecionar o dispositivo e na sequência clicar sobre o botão Adicionar.

**Importante:** caso os dispositivos tenham o mesmo número de IP, é necessário mudar o endereço de IP após adicioná-los, selecionando o dispositivo adicionado e clicando na guia Mais, disponível no canto superior direito da tela de visualização de dispositivos e na sequência, selecionar a opção Modificar endereço IP.



Modificando endereço de IP

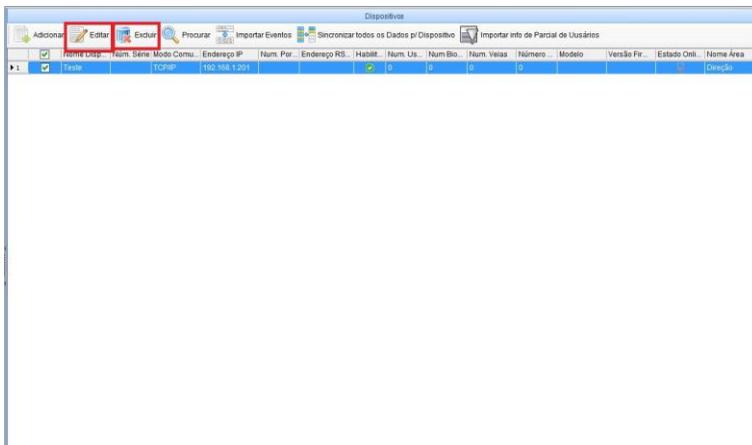
2. Na nova tela, preencha as informações da guia Parâmetros básicos. Vincule também a área a que esse dispositivo pertence, cadastrada no tópico 4. Adicionando áreas;

Adicionando dispositivo Pull SDK

3. Durante o preenchimento, para a garantir o correto funcionamento do dispositivo, marque a opção Excluir dados do dispositivo ao adicionar que é apresentada com letras na cor vermelha;  
**Importante:** não marque essa opção caso já possua usuários e eventos cadastrados no seu dispositivo, caso contrário, serão excluídos.
4. Clique no botão Gravar e continuar para adicionar mais de um dispositivo ou clique no botão Ok para salvar o dispositivo e finalizar o processo de cadastro.

### 5.3. Demais configurações comuns a ambos os tipos de dispositivos

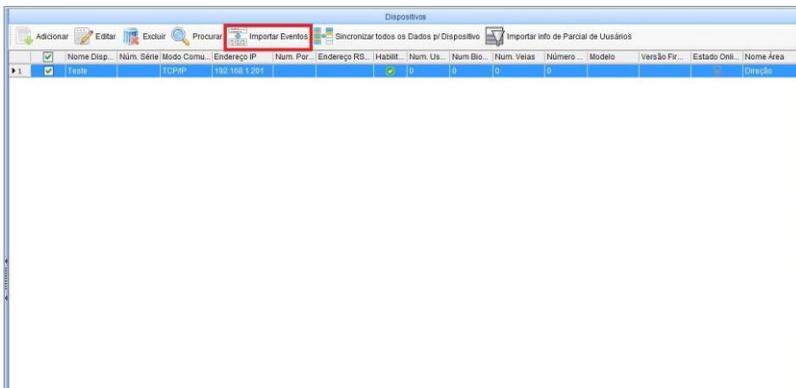
1. Na tela de visualização dos dispositivos é possível editar ou excluir os dispositivos cadastrados. Para isso, basta clicar sobre os respectivos botões após selecionar o dispositivo na tela de visualização;



Editando ou excluindo dispositivos

**Importante:** é possível procurar dispositivos diretamente na tela de visualização deles. Para isso, clique sobre o botão Procurar, logo ao lado do botão Excluir. Contudo, lembre-se de alterar o endereço de IP do dispositivo adicionado, caso ele seja igual ao endereço de IP do dispositivo que se deseja adicionar. Essa função só está disponível para dispositivos tipo Disp. Pull SDK e controladoras de 1, 2 e 4 portas.

2. Na função Dispositivos, é possível importar eventos gerados durante a operação de controle de acesso, ou seja, trazer para o banco de dados do software os eventos que se encontram armazenados nos dispositivos. Para isso, selecione o dispositivo na tela de visualização e clique sobre o botão Importar eventos;



Importação de eventos

**Importante:** essa função funcionará para dispositivos que não tenham sido zerados antes de serem adicionados ao software e já possuam um histórico de eventos.

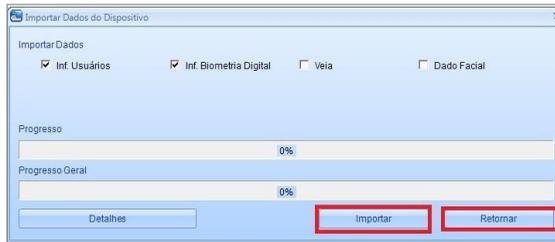
3. Na nova tela, é possível selecionar quais informações devem ser importadas. São elas: Importar registros novos, Importar todos registros ou Excluir registros após importar. Essa última exclui da memória do dispositivo todos os eventos após importá-los para o banco de dados do software. Marque a opção desejada e clique sobre o botão Importar para executá-la e acompanhe o progresso das informações. Ou clique em Retornar para voltar à tela de visualização dos dispositivos;



Importando eventos

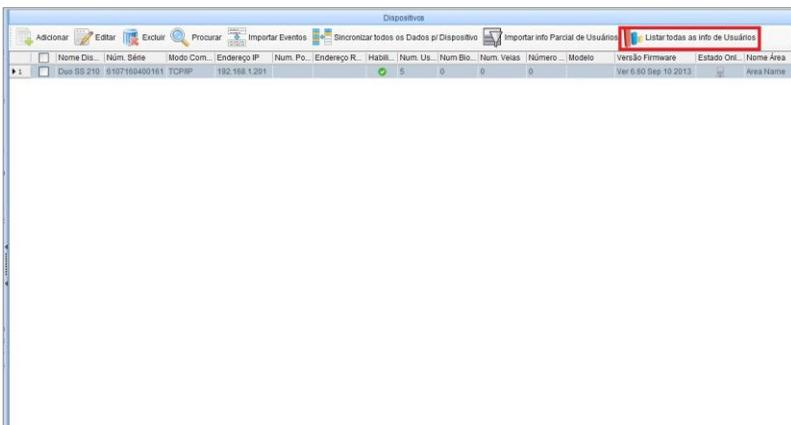


7. Na nova tela, selecione as informações que se deseja importar e na sequência clique sobre o botão Importar e acompanhe o progresso das informações. Ao fim do processo, clique sobre o botão Retornar para voltar à tela de visualização dos dispositivos;



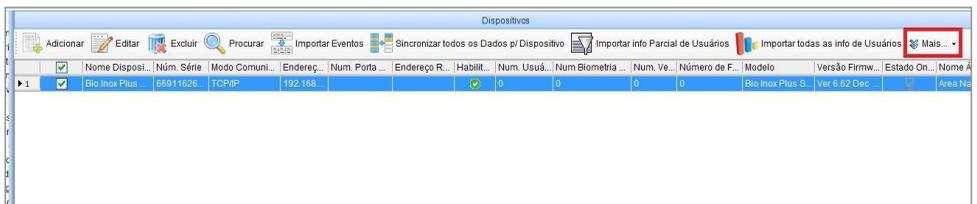
Selecionando informações para importar

**Obs.:** é possível importar todas as informações de usuários do dispositivo. Para isso, clique sobre o botão Importar todas as info de usuários. Acompanhe o progresso das informações e ao final clique em Fechar, para retornar à tela de visualização de dispositivos ou aguarde o tempo decrescente até que a tela feche sozinha.



Importando todas as informações de usuários

8. A função Dispositivos ainda traz a guia Mais, disponível na barra superior de funções à direita, dentro de uma seta indicativa;

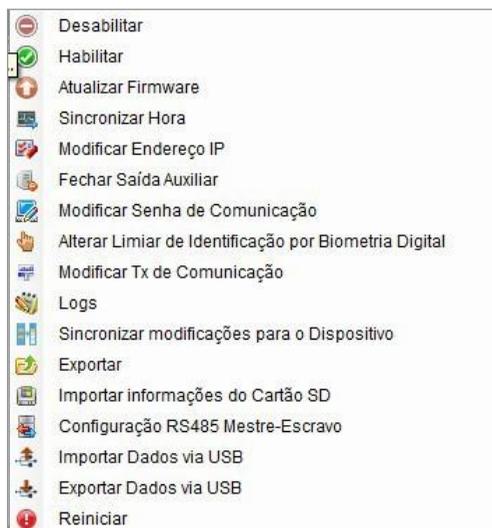


Localização da guia Mais em dispositivos

9. Dentro da guia Mais, uma nova coluna de funções será aberta e a descrição de cada uma delas pode ser verificada pela tabela a seguir:

Função	Descrição
Desabilitar	Torna o dispositivo selecionado inativo
Habilitar	Torna o dispositivo selecionado ativo
Sincronizar hora	Ajusta a hora do dispositivo à hora do software
Modificar endereço de IP	Altera o endereço de IP dos dispositivos já adicionados
Fechar saída auxiliar	Altera de estado as saídas auxiliares do dispositivo
Modificar senha de comunicação	Altera a senha de comunicação do dispositivo com o software
Alterar limiar de identificação por biometria digital	Altera a taxa de falsa aceitação da biometria digital nos dispositivos
Modificar TX de comunicação	Altera o valor dos pacotes de dados trocados entre o dispositivo e o software
Logs	Traz todas as informações de alterações de configurações feita pelo operador no software
Sincronizar modificações para o dispositivo	Ajusta as informações modificadas nos dispositivos
Exportar	Exporta para Excel, PDF ou TXT a lista de dispositivos adicionados.
Importar informações do cartão SD	Traz para o software as informações de dispositivo contidas no cartão de memória SD.
Configuração RS485 mestre-escravo	Configura o mestre e o escravo para dispositivos conectados e interligados por esse padrão de comunicação.
Importar dados via USB	Traz para o banco de dados do software as informações de eventos e usuários do dispositivo através da conexão USB.
Exportar dados via USB	Exporta para um pen drive as informações do banco de dados do software de usuários e eventos dos dispositivos cadastrados.
Reiniciar	Reinicia o dispositivo selecionado.
Reset de fábrica	Volta ao padrão de fábrica todas as configurações do dispositivo, deletando no banco de dados do controlador todas as informações de usuários e perfis de acesso.

Descrição das funções da guia Mais



Funções da guia Mais

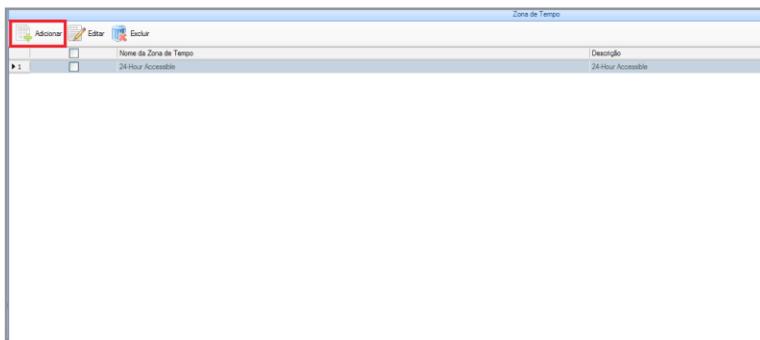
## 6. Controle de acesso

Nesta seção, apresentaremos as funções de configuração do sistema de controle de acesso e abordaremos os tópicos: Zona de tempo, Feriados, Configuração de porta, Perfil de acesso, Configuração Wiegand, Intertravamento, Anti-passback, Ações vinculadas a eventos, Abertura temporizada, Acesso combinado, Monitoramento, Planta baixa, Nome da leitora e Entradas e saídas auxiliares.

### 6.1. Zona de tempo

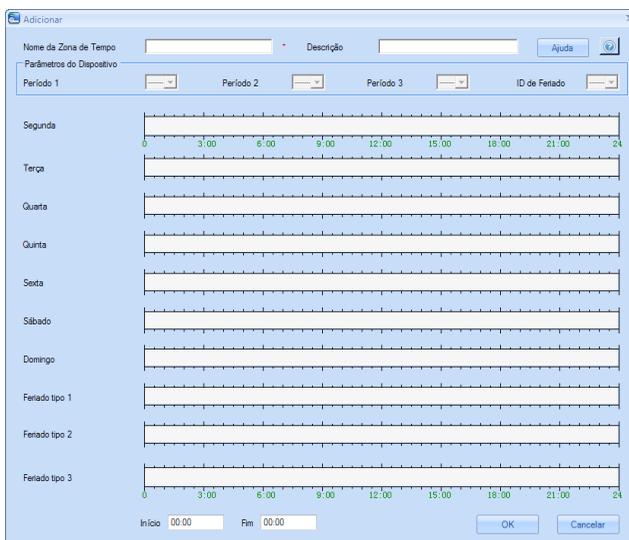
Zona de tempo é o intervalo de tempo no qual os usuários terão acesso ao ambiente controlado pelo dispositivo. O software SoapAdmin 3.5 já traz de uma Zona de tempo padrão de fábrica, que fica acessível 24 horas por dia e que não pode ser excluída. É possível adicionar outras áreas para os devidos vínculos posteriores. Para isso, observe os passos descritos a seguir:

1. Selecione a opção Zona de tempo, disponível em Controle de acesso. Na tela inicial, clique no botão Adicionar;

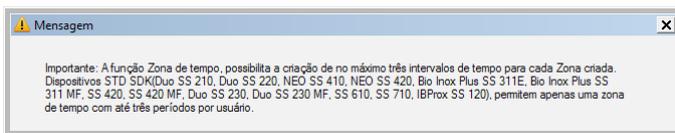


Tela inicial de zona de tempo

2. Na nova tela, insira o Nome da zona de tempo, a Descrição e preencha os tempos distribuídos por cada dia da semana. Também é possível configurar o horário de 3 perfis de feriados na zona de tempo criada. Ao final, clique em OK para criar a Zona de tempo;



Criando zona de tempo



Criando zona de tempo

3. Também é possível Editar ou Excluir as zonas de tempo criadas. Para isso, clique sobre os botões Editar ou Excluir após a seleção da zona de tempo na tela inicial, faça as modificações e clique em OK para confirmar as modificações.

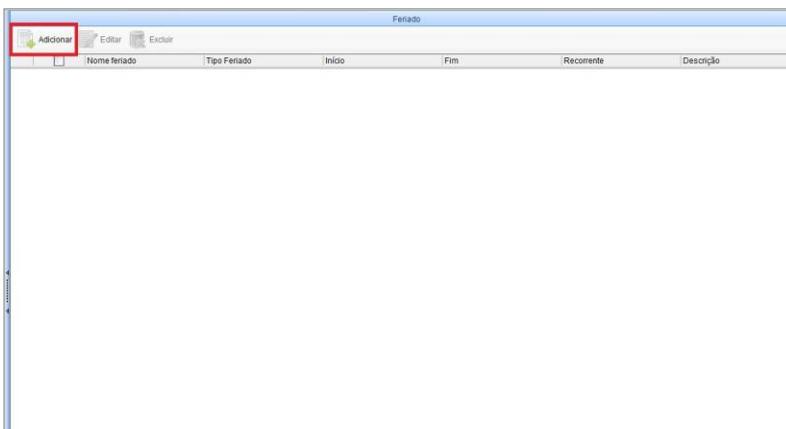
**Importante:** » A função Zona de tempo possibilita a criação de no máximo três intervalos de tempo para cada zona criada. Dispositivos STD SDK (Duo SS 210, Duo SS 220, NEO SS 410, NEO SS 420, Bio Inox Plus SS 311E, Bio Inox Plus SS 311 MF, SS 420, SS 420 MF, Duo SS 230, Duo SS 230 MF, SS 610, SS 710, IBProx SS 120) permitem apenas uma zona de tempo com até três períodos por usuário.

- » Equipamentos Pull SDK, tais como (SS 320, SS 320 MF, SS 411E e a linha de controladoras CT 500), não possuem essa restrição.
- » O limite para cadastro de Zonas de tempo é de 50 zonas de tempo com até um período cada. A medida que são atribuídos mais períodos na zona de tempo o número suportado de zonas de tempo diminui proporcionalmente.

## 6.2. Feriados

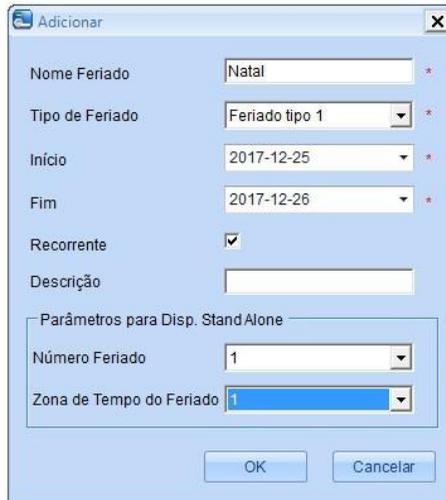
Nesta função, é possível criar os feriados que impactarão o sistema de controle de acesso, bem como vinculá-los ao tipo de feriado que foi criado na zona de tempo (1, 2 ou 3). Para isso, basta executar os passos descritos a seguir:

1. Na tela inicial de visualização dos feriados, clique no botão Adicionar;



Tela inicial de feriados

2. Na nova tela, crie os feriados desejados, sempre os vinculando aos tipos de feriados 1, 2 ou 3, bem como os parâmetros offline para a posterior sincronização com os dispositivos do sistema de controle de acesso;



Criando feriados

**Obs.:** o campo Recorrente deve ser marcado quando o feriado em questão se repete anualmente.

3. Após as devidas configurações, clique em Ok para confirmar ou em Cancelar para retornar à tela de visualização inicial de feriados;

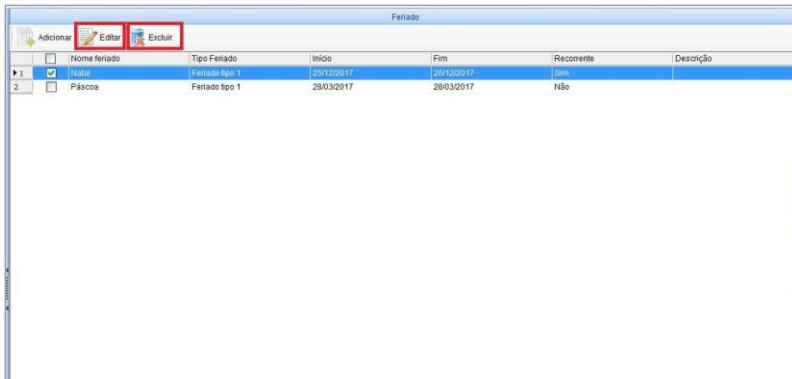
**Importante:** » Após a criação dos feriados faça o sincronismo das informações para os dispositivos que compõem o sistema de controle de acesso. O número máximo de feriados criados é de 24.



Sincronizando informações

- » A função Feriado está disponível apenas para os dispositivos que trabalham com o protocolo Pull SDK, tais como os da série CT 500, o SS 411E, o SS 320 e o SS 320 MF.

4. Também é possível editar ou excluir um dos feriados criados anteriormente, para isso, basta selecionar o feriado em questão e clicar sobre os botões Editar ou Excluir na tela inicial de visualização dos feriados. Sempre lembrando de sincronizar as informações com o dispositivo ao final dos ajustes.

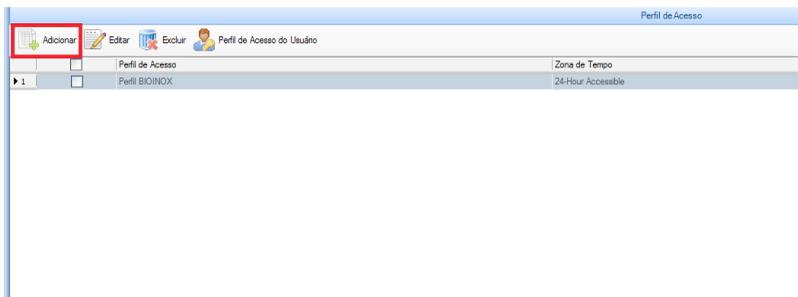


Excluindo ou editando feriados

### 6.3. Perfil de acesso

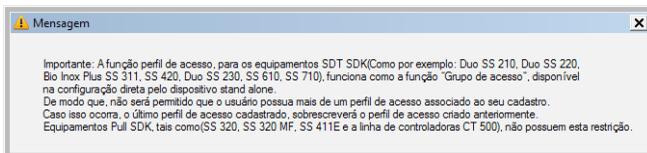
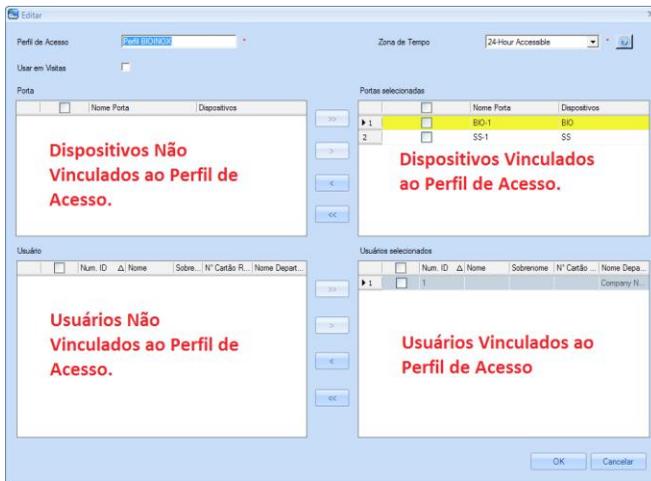
Para que o sistema de controle de acesso funcione corretamente, é necessário adicionar os Perfis de acesso dos dispositivos e usuários. Para isso, observe as instruções descritas a seguir:

1. Na tela de visualização da função Perfil de acesso, clique sobre o botão Adicionar;



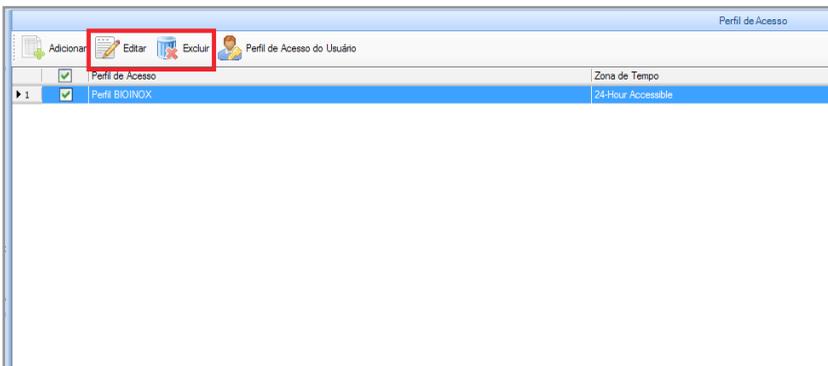
Tela de visualização de perfis de acesso

2. Na nova tela, entre com o nome do novo perfil de acesso a ser criado e, utilizando as Setas centrais de navegação, adicione os dispositivos e usuários que farão parte do perfil de acesso em questão, selecionando-os à esquerda e transferindo-os para o campo da direita. Também é necessário vincular a zona de tempo a que o perfil de acesso pertence. Ao final das configurações clique em Ok e sincronize as informações com os dispositivos do sistema;



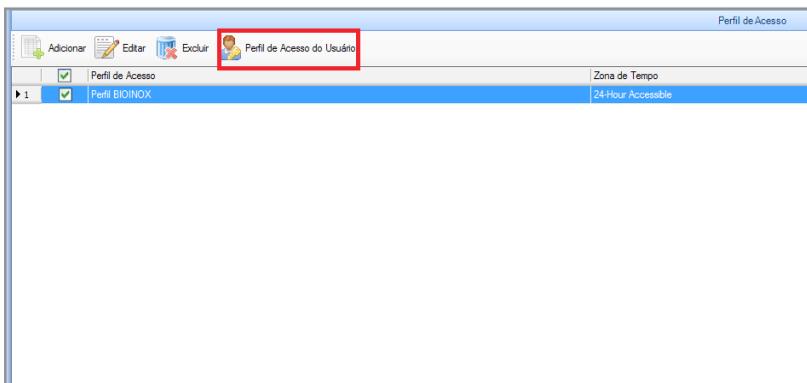
Atribuindo dispositivos e usuários ao perfil de acesso

3. É possível também editar ou excluir os perfis de acesso criados. Para isso, selecione o Perfil de acesso selecionado e clique sobre os botões Editar e Excluir na tela de visualização dos perfis de acesso;

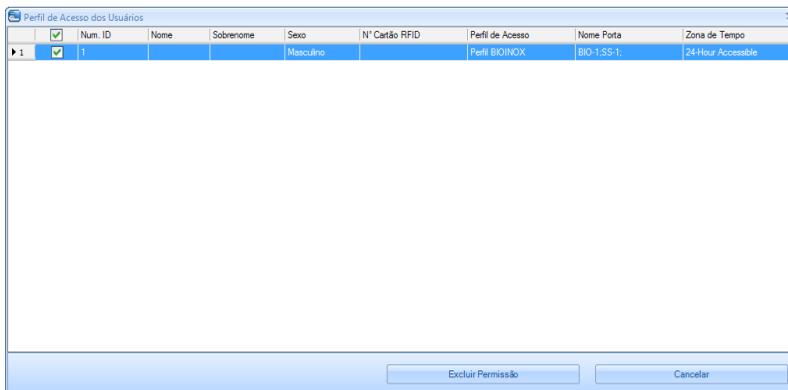


Editando ou excluindo perfil de acesso

4. Ainda na tela de visualização é possível excluir a permissão dos usuários dentro do perfil de acesso criado. Para isso, basta clicar sobre o botão Perfil de acesso do usuário na tela de visualização do Perfil de acesso. Na nova tela selecione os usuários que se deseja excluir e clique no botão Excluir privilégios. Depois será necessário sincronizar as informações com todos os dispositivos pertencentes ao Sistema de controle de acesso.



Perfil de acesso do usuário



Excluindo usuários do perfil de acesso

- Importante:** » A função Perfil de acesso, para os equipamentos SDT SDK (Duo SS 210, Duo SS 220, NEO SS 410, NEO SS 420, Bio Inox Plus SS 311E, Bio Inox Plus SS 311 MF, SS 420, SS 420 MF, Duo SS 230, Duo SS 230 MF, SS 610, SS 710, IBProx SS 120), funciona como a função Grupo de acesso, disponível na configuração direta pelo dispositivo stand alone. De modo que não será permitido que o usuário possua mais de um perfil de acesso associado ao seu cadastro. Caso isso ocorra, o último perfil de acesso cadastrado sobrescreverá o perfil de acesso criado anteriormente.
- » Equipamentos Pull SDK, tais como (SS 320, SS 320 MF, SS 411E e a linha de controladoras CT 500), não possuem essa restrição.

## Perfil de acesso para visitantes

É possível também criar um perfil de acesso para o cadastro de visitantes. Para isso, basta clicar sobre o check-box que marca a opção Usar em visitas, para que este perfil fique visível na tela de cadastro de visitantes para o posterior vínculo dos mesmos.

Perfil de Acesso		Zona de Tempo	
Visitantes		Visitantes	
<input checked="" type="checkbox"/> Usar em Visitas			
Porta			
	Nome Porta	Dispositivos	
1	BP Plus-1	BP Plus	
2	SS 320-1	SS 320	
Portas selecionadas			
	Nome Porta	Dispositivos	
1	CT-1	CT	
2	CT-2	CT	
Usuário			
	Num. ID	Nome	Sobr... N° Cartão... Nome Dep...
1	1	Rafael	8839253 Company N...
2	4	Big Richard	32212531... Company N...
Usuários selecionados			
	Num. ID	Nome	Sobreno... N° Cartã... Nome De...
1	2	João	
2	3	Scarlet	3534045

Perfil de acesso de visitantes

**Importante:** após habilitar o perfil de acesso aos visitantes, associe os dispositivos de controle de acesso que pertencerão a esse perfil de acesso para posteriores vínculos dos cadastros de visitantes.

## 6.4. Configuração de portas

Nesta seção são realizadas algumas configurações de portas do sistema de controle de acesso, tais como: Tempo de abertura, Sensor de fechadura, Método de autenticação, entre outras podem ser configuradas. Para isso, siga os passos descritos a seguir:

1. Na tela inicial de visualização de configuração de porta, serão exibidas todas as portas referentes aos dispositivos previamente adicionados. Para modificar os seus parâmetros, selecione a porta na tela inicial e clique sobre o botão Editar;

	Nome Porta	Num. Porta	Nome Dispositivo	Zona de Tempo para Abrir Porta	Modo de Passagem	Tempo de Abertura	Horário do Sensor	Modo Verificação	Tipo de Sensor	Estado E/S
1	SS-1	1	SS	24-hor Accessible		5	15	Somente Biometria Digital	Nenhum	Estrada
2										Entrada

Lista de portas adicionadas

2. Na nova tela, é possível alterar o Nome da porta, a Zona de tempo padrão, o Período de porta aberta, o Modo de verificação, o Tipo de sensor da fechadura, bem como o Atraso do sensor, que é o tempo que o dispositivo leva para acionar um alarme quando a porta fica aberta, o Tempo de abertura, que é o tempo em segundos que a porta ficará aberta, entre outras configurações:

The screenshot shows a configuration window titled 'Editar' with the following fields and values:

- Nome Disp.: Bio Inox Plus SS 311
- Num. Porta: 1
- Nome Porta: Bio Inox Plus SS 311 MF-1
- Zona de Tempo Padrão: 24-Hour Accessible
- Período de Porta Aberta: ---
- Modo Verificação: Qualquer
- Senha Coação: Configuração
- Senha Emergência: Configuração
- Configuração Wiegand: [Configurações Wiegand](#)
- Tipo sensor: Sem
- Atraso do Sensor: 15 (0 a 254 Segundos)
- Bloquear ao Fechar:
- Marcar Ponto:
- Tempo Abertura: 1.0 (Segundo(1-10))
- Int. entre Identificação: 0 (0 a 10 Segundos)
- Max. Recorrências de Negação: 0
- Alarme de Porta Aberta: 1 (Segundo(1-99))
- Permitir SRB:

At the bottom, there are two checkboxes: 'Copiar Configurações para todas as Portas desta Controladora' (unchecked) and 'Copiar Configurações para todas as Portas de todas as Controladoras' (unchecked). 'OK' and 'Cancelar' buttons are at the bottom right.

Opções de configuração de porta

3. A descrição das funções setadas é apresentada na tabela a seguir:

Função	Descrição
Nome disp.	Nome do dispositivo adicionado anteriormente
Num. porta	Número da porta controlada pelo dispositivo
Nome porta	Nome da porta controlada pelo dispositivo (editável)
Zona de tempo padrão	Zona de tempo na qual o dispositivo está vinculado
Período de porta aberta	Período pré-determinado em que o dispositivo abre a porta independente da zona de tempo a que pertença
Modo de verificação	Método de autenticação que o dispositivo estará disponível para leitura durante a operação do sistema de controle de acesso
Senha de coação	Senha definida para ser utilizada em momentos de necessidade, a mesma abre a porta e dispara um alarme
Senha de emergência	Senha definida para ser utilizada no momento de emergência, exemplo incêndio, terremoto, ou outras emergências a serem definidas pelo operador do sistema
Configuração wiegand	Configuração do padrão de comunicação wiegand para o funcionamento do leitor escravo que se comunique neste padrão
Tipo sensor	Sensor de fechadura (Nenhum, Normalmente Aberto ou Normalmente Fechado)
Atraso do sensor	Tempo em segundos configurado de espera entre a abertura da porta e o acionamento do sensor de porta
Bloquear ao fechar	Altera o status da porta de aberta para fechada
Marcar ponto	Registra o horário e o dia do evento
Tempo de abertura	Tempo em que a porta permanece destrancada
Int. entre identificação	Intervalo entre as leituras
Veze de erros por alarme	Quantidade de tentativas de acesso negadas para disparo de alarme
Alarme de porta aberta	Alarme disparado ao deixar a porta aberta
Permitir SRB	Habilita controle externo da porta (não disponível nesta versão)

Descrição de configurações de porta

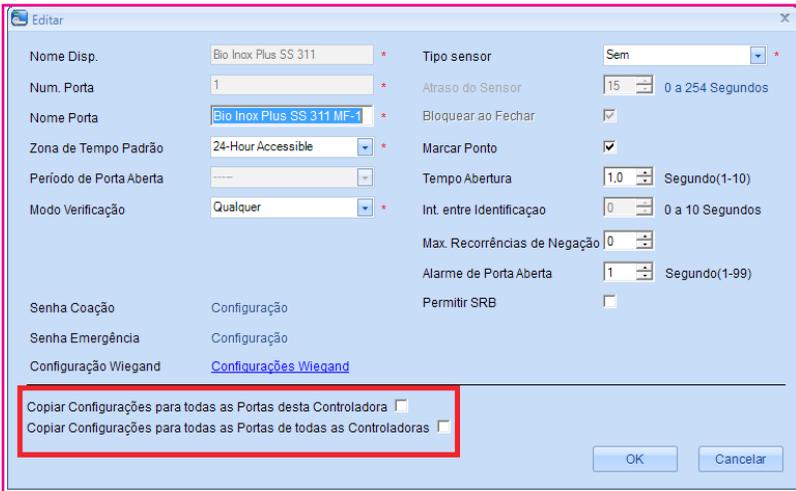
### Importante:

- » A ativação da função Senha de Coação para controladoras da linha CT 500 Intelbras, necessitam de um leitor escravo conectado à controladora para performar o seu acionamento. Após o cadastro da senha de coação e o sincronismo das informações com os dispositivos, é necessário digitar a seguinte sequência no teclado do leitor escravo:

**CAMPAINHA + SENHA DE COAÇÃO + #**

- » A função senha de coação só está disponível para dispositivo da linha CT 500 Intelbras.

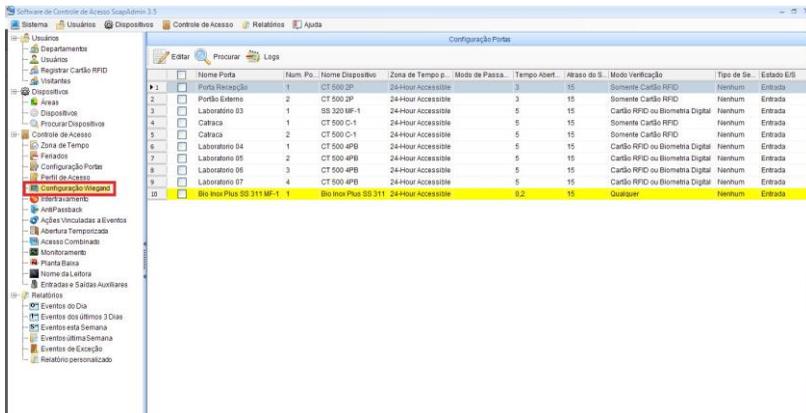
4. É possível também marcar algumas opções finais que visam replicar as configurações aos demais integrantes do sistema de controle de acesso.



Replicando configurações aos demais dispositivos do sistema

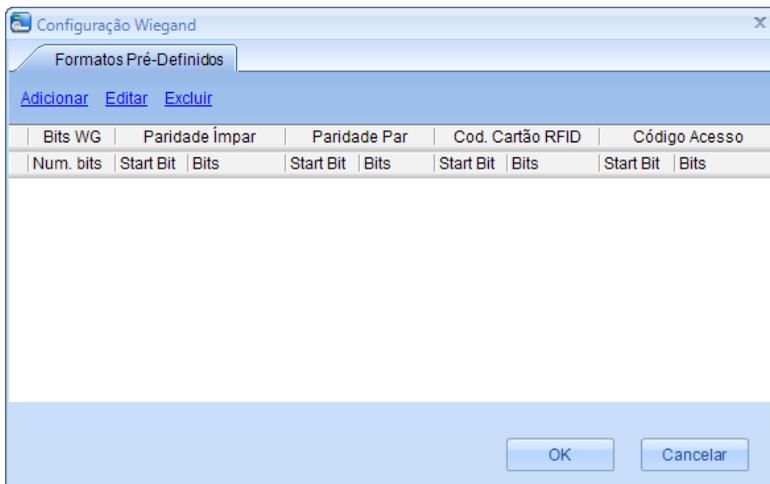
**Importante:** algumas das funções descritas na tabela acima podem não estar disponíveis conforme o dispositivo adicionado. Por isso, é fundamental a leitura do manual de usuário do seu dispositivo para garantir que ele possui a função que se deseja configurar.

**Obs.:** a função Configurações Wiegand também está disponível na guia lateral do software SoapAdmin 3.5 logo abaixo da opção Perfil de acesso dentro das funções de Controle de acesso.



Configurações wiegand

Nesta nova tela, é possível entrar com todos os parâmetros em bits que se referem à taxa de comunicação Wiegand e, em seguida, confirmá-los clicando em OK. Contudo, esses parâmetros só devem ser alterados com a utilização no manual de usuário dos respectivos leitores que serão utilizados.

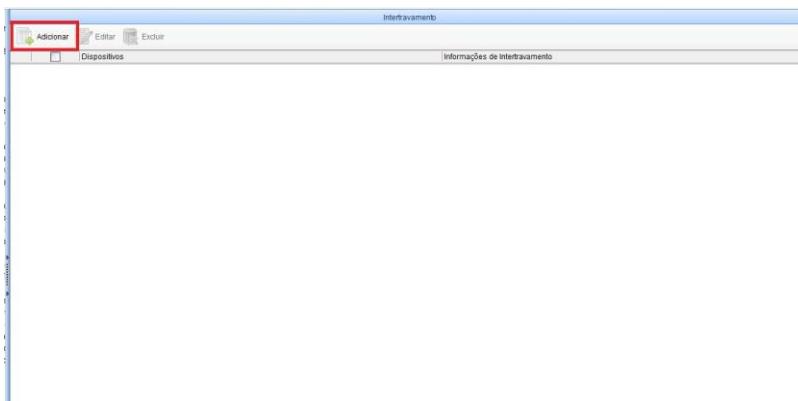


Configurando o padrão Wiegand

## 6.5. Intertravamento

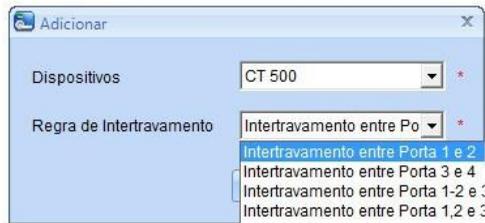
Esta função possibilita criar uma situação de interdependência entre duas ou mais portas de uma controladora (CT 500). Estando aberta uma das portas configuradas na função, as demais permanecerão fechadas até que a porta aberta feche também, possibilitando ao usuário então proceder a porta subsequente do sistema. Para configurar o sistema, execute os passos descritos a seguir:

1. Na tela de visualização do intertravamento, clique sobre o botão Adicionar;



Adicionando intertravamento

- Na nova tela, selecione a controladora que estará configurada para o intertravamento no campo Dispositivos e selecione uma das opções para a Regra de Intertravamento;



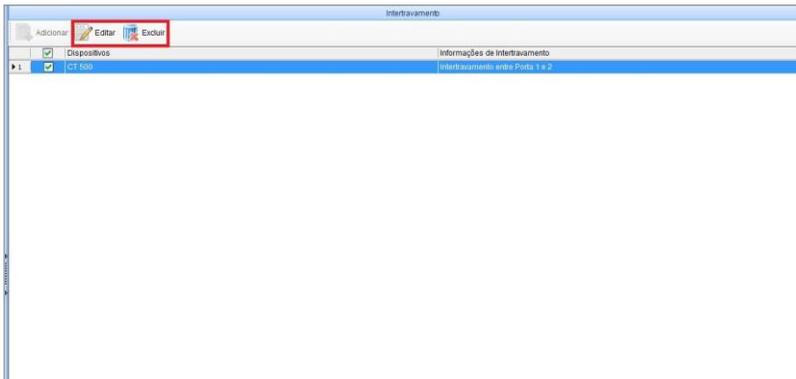
Configurando intertravamento

- Após selecionar a Regra de intertravamento, clique sobre o botão Ok e sincronize as informações com o dispositivo;
- As opções disponíveis para setar a Regra de intertravamento são:

Opção de regra	Descrição
Intertravamento entre porta 1 e 2	Porta 2 fechada enquanto porta 1 aberta e vice-versa.
Intertravamento entre porta 3 e 4	Porta 4 fechada enquanto porta 3 aberta e vice-versa.
Intertravamento entre porta 1-2 e 3-4	Porta 2 fechada enquanto porta 1 aberta e vice-versa. Porta 4 fechada enquanto porta 3 aberta e vice-versa.
Intertravamento entre porta 1, 2 e 3	Porta 2 e 3 fechada enquanto porta 1 aberta e vice-versa.
Intertravamento entre porta 1, 2, 3 e 4	Porta 2, 3 e 4 fechada enquanto porta 1 aberta e vice-versa.

Descrição de configurações de intertravamento

- É possível também editar ou excluir o Intertravamento adicionado anteriormente. Para isso, clique sobre o botão Editar ou Excluir na tela de visualização do Intertravamento, após selecionar o perfil criado. Feitas as modificações, clique em Ok e sincronize as informações com o dispositivo.



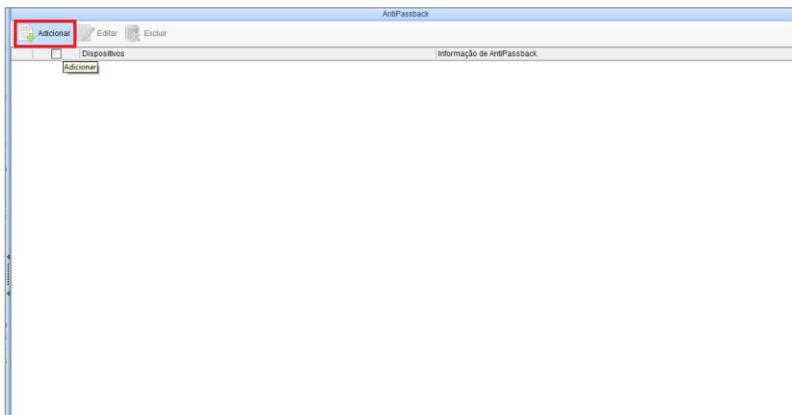
Editando ou excluindo regra de intertravamento

- Importante:** » Só é possível adicionar uma regra de intertravamento por dispositivo pertencente ao sistema de controle de acesso.
- » Esta função está disponível apenas para controladoras da linha CT 500 e restrita ao número de no mínimo duas e no máximo 4 portas.

## 6.6. Anti-passback

Esta função visa controlar a entrada e a saída do usuário de modo que, uma vez que o usuário entrou em uma área específica, ele não poderá entrar novamente sem que tenha saído primeiramente. Esta função é bem versátil e pode ser configurada entre portas de um mesmo ambiente ou entre ambientes independentes. Para configurar esta função, execute os passos descritos a seguir:

1. Na tela de visualização do Anti-passback, clique sobre o botão Adicionar;



Adicionando Anti-passback

2. Na nova tela escolha o tipo de dispositivo para o qual será configurada a regra de anti-passback. Na sequência defina a regra que será aplicada bem como o estado inicial do dispositivo, este último, aplicável apenas para dispositivos que não sejam da linha CT 500. No exemplo a seguir, as duas imagens demonstram a utilização de uma controladora CT 500 e de um dispositivo SDTSDK;

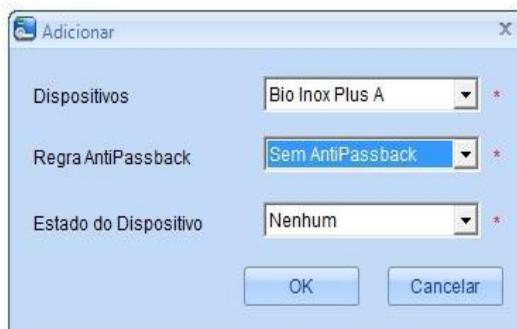


Configurando regra para CT 500

Regra Anti-passback	Descrição
Porta 1 e 2	Quando faço uma operação na porta 1, tenho que fazer a próxima operação na porta 2, não importando o sentido. Quando faço uma operação na porta 2, tenho que fazer a próxima operação na porta 1, não importando o sentido.
Porta 3 e 4	Quando faço uma operação na porta 3, tenho que fazer a próxima operação na porta 4, não importando o sentido. Quando faço uma operação na porta 4, tenho que fazer a próxima operação na porta 3, não importando o sentido.
Porta 1 e 2, porta 3 e 4	Quando faço uma operação na porta 1, tenho que fazer a próxima operação na porta 2, não importando o sentido. Quando faço uma operação na porta 2, tenho que fazer a próxima operação na porta 1, não importando o sentido. Quando faço uma operação na porta 3, tenho que fazer a próxima operação na porta 4, não importando o sentido. Quando faço uma operação na porta 4, tenho que fazer a próxima operação na porta 3, não importando o sentido.
(Entre porta 1 e 2) e (entre porta 3 e 4)	Quando faço uma operação na porta 1 ou 2, tenho que fazer a próxima operação na porta 3 ou 4, não importando o sentido. Quando faço uma operação na porta 3 ou 4, tenho que fazer a próxima operação na porta 1 ou 2, não importando o sentido.
Entre porta 1 e 2 ou 3	Quando faço uma operação na porta 1, tenho que fazer a próxima operação na porta 2 ou 3, não importando o sentido. Quando faço uma operação na porta 2 ou 3, tenho que fazer a próxima operação na porta 1, não importando o sentido.
Entre porta 1 e 2 ou 3 ou 4	Quando faço uma operação na porta 1, tenho que fazer a próxima operação na porta 2 ou 3 ou 4, não importando o sentido. Quando faço uma operação na porta 2 ou 3 ou 4, tenho que fazer a próxima operação na porta 1, não importando o sentido.

Regra Anti-passback	Descrição
Entre leitores da porta 1	Regra válida apenas entre os leitores de entrada e saída da porta 1.
Entre leitores da porta 2	Regra válida apenas entre os leitores de entrada e saída da porta 2.
Entre leitores da porta 3	Regra válida apenas entre os leitores de entrada e saída da porta 3.
Entre leitores da porta 4	Regra válida apenas entre os leitores de entrada e saída da porta 4.

Descrição das regras anti-passback para controladoras CT 500



Configurando regra para dispositivo SDTSDK

Regra Anti-passback	Descrição
Sem anti-passback	Anti-passback desativado
Anti-passback de saída	Regra válida para eventos de saída
Anti-passback de entrada	Regra válida para eventos de entrada
Anti-passback de entrada/saída	Regra válida para eventos de entrada e saída

Descrição das regras anti-passback para dispositivo STDSDK

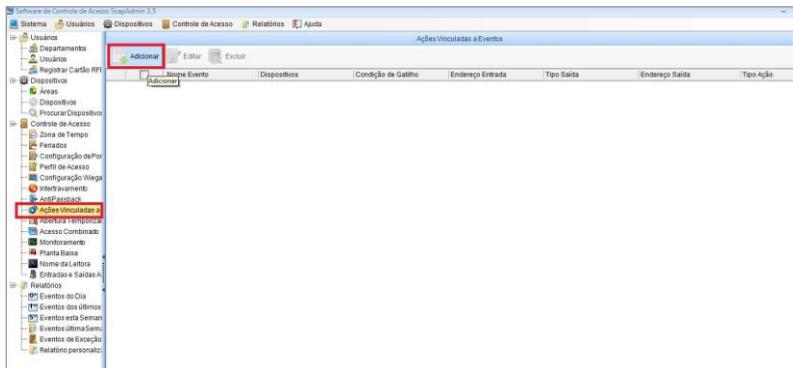
- Também é necessário setar o estado do dispositivo SDTSDK, que poderá ser Nenhum, Entrada ou Saída. Após as configurações, clique no botão Ok e sincronize as informações com os dispositivos do sistema.

**Importante:** caso o estado do dispositivo seja setado para Nenhum a regra de anti-passback definida será ignorada pelo dispositivo.

## 6.7. Ações vinculadas a eventos

Esta função permite configurar ações vinculadas a determinados tipos de eventos. Esses eventos serão gatilhos para, por exemplo, abrir uma porta, fechar uma porta, abrir ou fechar uma saída auxiliar do dispositivo que por sua vez irá acionar um sistema externo tal qual um sistema de alarme. Para configurar esta função, execute os passos descritos a seguir:

1. Selecione o botão Adicionar na tela de visualização de Ações vinculadas a eventos;



Configurando ações vinculadas a eventos

2. Na nova tela, insira o nome da ação criada, selecione o dispositivo que receberá a configuração, o gatilho que acionará o Evento de exceção e, por fim, as configurações para o Tipo de saída, Endereço de saída e o Tipo de ação;



Configurando ações vinculadas a eventos

3. A seguir estão listados os tipos de Gatilhos disponíveis, bem como os Endereços de entrada, Tipos de saída, Endereço de saída e Tipo de ação.

Gatilhos	Gatilhos
Abertura acesso combinado (biometria digital)	Abertura senha coação
Abertura acesso combinado (cartão RFID)	Abertura senha emergência
Abertura biometria digital	Abertura temporizada (cartão RFID + biometria digital)
Abertura biometria digital de coação	Abertura temporizada (biometria digital)
Abertura cartão RFID + biometria digital	Acesso combinado (biometria digital)
Abertura durante modo de passagem	Acesso combinado (cartão RFID + biometria digital)
Abertura normal	Acesso combinado (cartão RFID)
Abertura remota	Acesso negado
Abertura remota normal	Anti-passback
Biometria digital expirada	Biometria digital não registrada
Cartão RFID expirado	Cartão RFID não registrado
Entrada auxiliar aberta	Entrada auxiliar fechada
Falha ao fechar porta durante modo de passagem	Fechamento remoto
Fim modo passagem	Fora da zona de tempo (cartão RFID)
ID durante modo de passagem (biometria digital)	ID durante modo de passagem (cartão RFID)
Intertravamento	Intervalo de marcação muito curto
Intervalo de marcação muito curto (biometria digital)	Porta aberta
Porta aberta corretamente	Porta arrombada
Porta fechada corretamente	Porta fora horário (biometria digital)
Porta fora horário (botoeira)	Senha inválida
Verificação abertura temporizada	Zona de tempo inválido
<b>Endereço de entrada</b>	
Qualquer	Disp. A, B, C (CT 500)
<b>Tipo de saída</b>	
Porta	Saída auxiliar
<b>Endereço de saída</b>	
Porta- (1)	Porta- (2)
<b>Tipo de ação</b>	
Fecha	Abre
Deixa aberto	

Descrição das opções de configurações para os eventos

- Importante:** » Ao selecionar a opção Abre também será necessário definir o tempo em segundos do Intervalo. Esse tempo é configurável de 1 a 254 segundos.
- » Os tipos de saídas bem como o número de portas e os endereços de saída podem mudar de acordo com o tipo do dispositivo adicionado ao sistema de controle de acesso.

## 6.8. Abertura temporizada

A função Abertura temporizada permite ao operador do sistema de controle de acesso criar uma situação em que a porta controlada estará aberta independentemente da zona de tempo cadastrada para esta porta. Para isso, além de adicionar a porta em que será aplicada essa configuração, é necessário incluir ao perfil os usuários que servirão de gatilho para o início dessa função. Por exemplo: uma recepção de uma empresa deverá permanecer com sua porta de entrada aberta durante o expediente comercial. Contudo, o gatilho para o início dessa condição é o acesso via cartão RFID do usuário que trabalha na recepção, daí para frente a porta permanecerá aberta até que a função seja desabilitada no monitoramento em tempo real, voltado à porta a ser controlada pela zona de tempo vinculada a ela anteriormente.

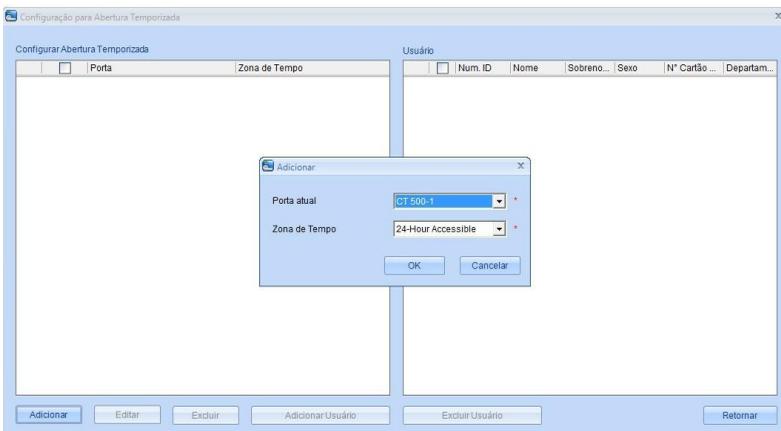
Para configurar essa condição, é necessário seguir o procedimento:

1. Clique no botão Configuração na tela de visualização da Abertura temporizada;



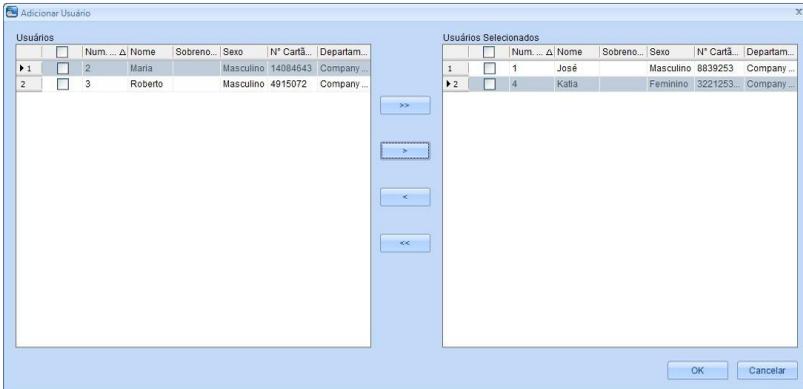
Configurando abertura temporizada

2. Na nova tela, clique no botão Adicionar e uma nova tela surgirá, por meio da qual será possível adicionar a porta em que será configurada a condição de Abertura temporizada, bem como a zona de tempo vinculada a ela. Após as definições, clique em OK e sincronize as informações com o dispositivo;



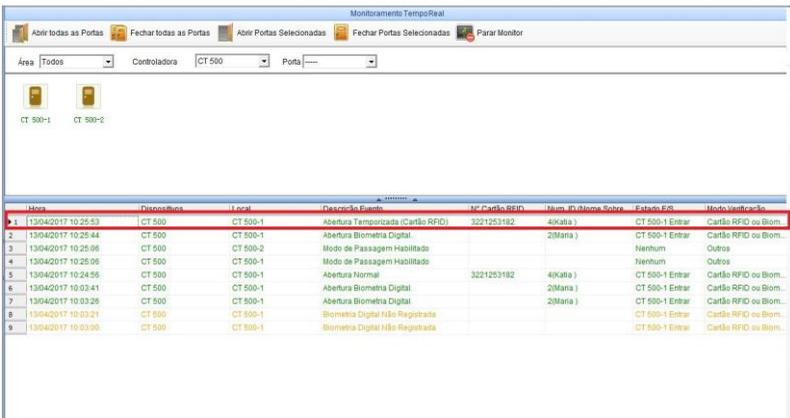
Adicionando porta à temperatura temporizada

3. Na sequência, é necessário adicionar os usuários que pertencem a essa condição e que servirão de gatilho para o início da condição de Abertura temporizada. Para isso, selecione a porta adicionada no item anterior e clique no botão Adicionar usuários. Na nova tela que surgirá, selecione os usuários do banco de dados cujos eventos de entrada servirão de gatilhos para o início da condição, clicando sobre as setas de navegação centrais, de modo que passarão do lado esquerdo para o lado direito da tela. Ao final clique em Ok e sincronize as informações com o dispositivo;



Adicionando usuários à abertura temporizada

4. Na função Monitoramento é possível verificar os registros que serão gerados quando um dos usuários-gatilho acessar a porta configurada. Note que, caso algum outro usuário que não esteja configurado como gatilho para condição de Abertura temporizada tente o acesso, terá o acesso liberado, contudo a porta se comportará regida pela zona de tempo padrão, voltando a fechar após ter decorrido o Tempo de abertura de porta configurado. Após um dos usuários-gatilho efetuar o acesso à porta, esta permanecerá aberta até que a condição Modo de passagem esteja desabilitada.



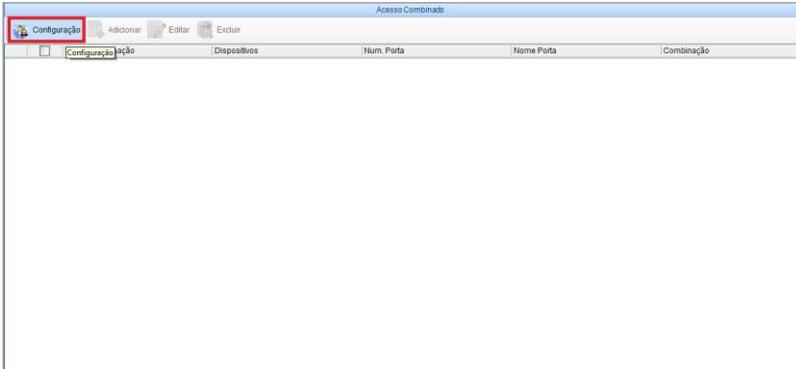
Eventos de abertura temporizada

**Importante:** esta função está disponível apenas para a linha de controladora CT 500. Para desabilitar esta função, basta selecionar a opção Desabilitar modo de passagem entrada, disponível em Fechar portas seleccionadas ou Fechar todas as portas. Uma vez desabilitada, a porta funcionará com base na zona de tempo padrão, configurada previamente.

## 6.9. Acesso combinado

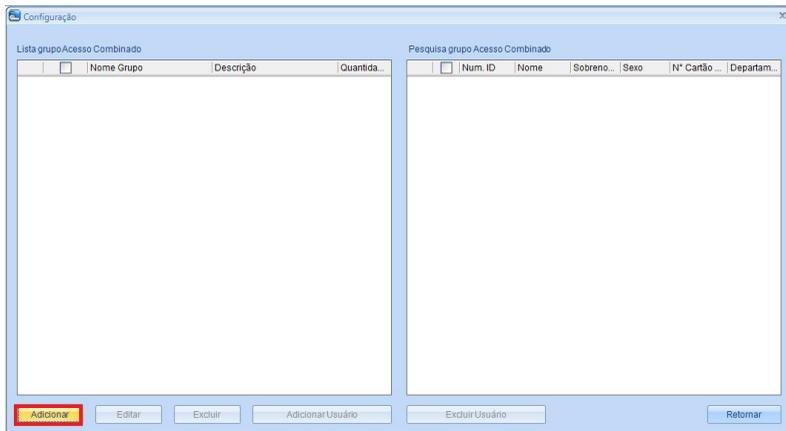
Essa função possibilita cadastrar uma condição que, para a porta abrir, será necessária a autenticação de 1 ou mais usuários de pelo menos dois grupos diferentes. Essa autenticação dependerá do tipo de chave cadastrada no perfil do usuário e da configuração do método de autenticação na regra do acesso combinado.

1. Para configurar esse parâmetro, selecione o botão Configuração na tela de visualização do acesso combinado;



Configurando acesso combinado por grupos

2. Na nova tela, crie os grupos que irão compor a combinação posterior, bem como vincule o dispositivo que receberá a configuração e o modo de verificação que os usuários que estiverem vinculados a esses grupos deverão ter para acessar o ambiente controlado;



Adicionando grupos para combinação

3. Na nova tela insira o nome e a descrição do grupo, o método de autenticação para a entrada, o número do grupo que está sendo criado e o nível de acesso do grupo, ou seja, a zona de tempo a qual o grupo pertence;

The screenshot shows a dialog box titled "Adicionar" with a close button (X) in the top right corner. It contains the following fields and options:

- Nome Grupo:** A text input field containing "P&D" with an asterisk (\*) to its right.
- Descrição:** A text input field containing "Desenvolvimento".
- Parâmetros do Dispositivo:** A section containing:
  - Grupo No.:** A dropdown menu with "2" selected.
  - Modo de verificação:** A dropdown menu with "Cartão RFID e Senha" selected.
  - Nível de Acesso:** A dropdown menu with "24-Hour Accessible" selected.
  - Ativo em Feriados**
- Buttons:** "OK" and "Cancelar" buttons at the bottom.

Adicionando primeiro grupo

- Importante:** » A escolha do método de autenticação deve ser coerente com as formas de autenticação disponíveis no dispositivo utilizado no sistema de controle de acesso. Verifique o manual do dispositivo antes de configurar.
- » A lista completa dos métodos de autenticação pode ser consultada no tópico 6.4. Configuração de portas.

The screenshot shows a dialog box titled "Adicionar" with a close button (X) in the top right corner. It contains the following fields and options:

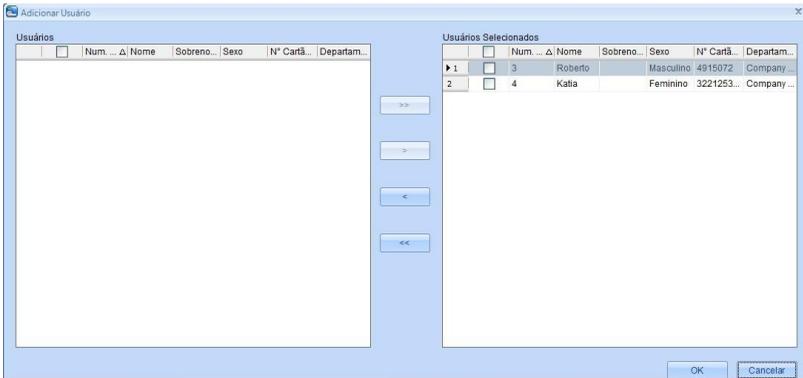
- Nome Grupo:** A text input field containing "Produção" with an asterisk (\*) to its right.
- Descrição:** A text input field containing "Linha".
- Parâmetros do Dispositivo:** A section containing:
  - Grupo No.:** A dropdown menu with "3" selected.
  - Modo de verificação:** A dropdown menu with "Somente Senha" selected.
  - Nível de Acesso:** A dropdown menu with "24-Hour Accessible" selected.
  - Ativo em Feriados**
- Buttons:** "OK" and "Cancelar" buttons at the bottom.

Adicionando segundo grupo

**Importante:** » A escolha do método de autenticação deve ser coerente com as formas de autenticação disponíveis no dispositivo utilizado no sistema de controle de acesso. Verifique o manual do dispositivo antes de configurar.

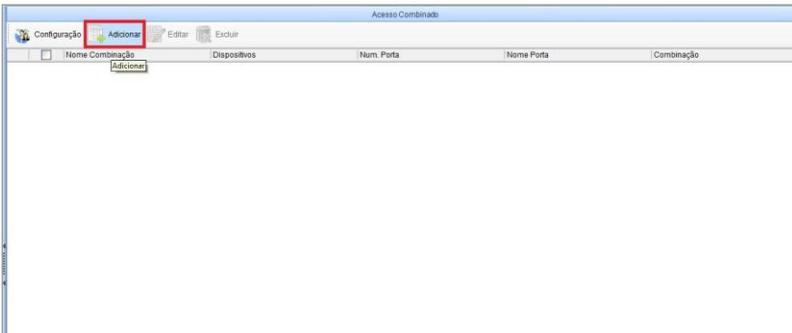
» A lista completa dos métodos de autenticação pode ser consultada no tópico 6.4. Configuração de portas.

4. Após a criação dos grupos, é necessário incluir os respectivos usuários aos seus respectivos grupos. Para isso, selecione um dos grupos criados e clique no botão Adicionar usuários. Na nova tela, selecione os usuários que desejar e atribua-os ao grupo utilizando as setas de navegação central. Por fim, clique em Ok para confirmar a inclusão e repita a operação para os demais grupos existentes;



Atribuindo usuários ao grupo

5. Uma vez criados os grupos e vinculados os seus respectivos usuários, é o momento de criar a combinação de acesso por grupo. Para isso, clique sobre o botão Adicionar na tela de visualização do acesso combinado;



Criando o acesso combinado entre grupos

6. Na nova tela, selecione o dispositivo que receberá a configuração, o nome dessa combinação, bem como o seu número identificador, os grupos e a quantidade de usuários de cada grupo que serão necessários para que a combinação de acesso ocorra. Feitas as configurações, clique no botão Ok e sincronize as informações com os dispositivos.

Opção de Porta: Duo SS 210-1 \*

Nome Combinação: Supervisionado \*

Parâmetros do Dispositivo

Combinação No.: 2

Num. Usuários em cada Grupo

Grupo	Nome	Usuários
Grupo1	P&D	1
Grupo2	Produção	1
Grupo3	----	0
Grupo4	----	0
Grupo5	----	0

OK Cancelar

Combinação de acesso entre grupos

## 6.10. Monitoramento

Esta função possibilita monitorar todos os dispositivos que compõem o sistema de controle de acesso, apresentando em tempo real todos os eventos gerados em qualquer uma das portas controladas pelos dispositivos do sistema, sejam estes eventos de acesso liberado, negado, coação, entre outros. Note na figura a seguir a exemplificação da tela de monitoramento, nela é possível filtrar os dispositivos que se deseja ver, tendo como opções Todos os dispositivos ou Dispositivos individuais, selecionando-os através das caixas de opções marcadas com o número 1 na imagem.

1. Uma vez selecionado, é necessário clicar no botão Inicia monitor marcado com o número 2 na imagem a seguir;

Monitoramento Tempo Real

Abrir todas as Portas Fechar todas as Portas Abrir Portas Selecionadas Fechar Portas Selecionadas Iniciar Monitor 2

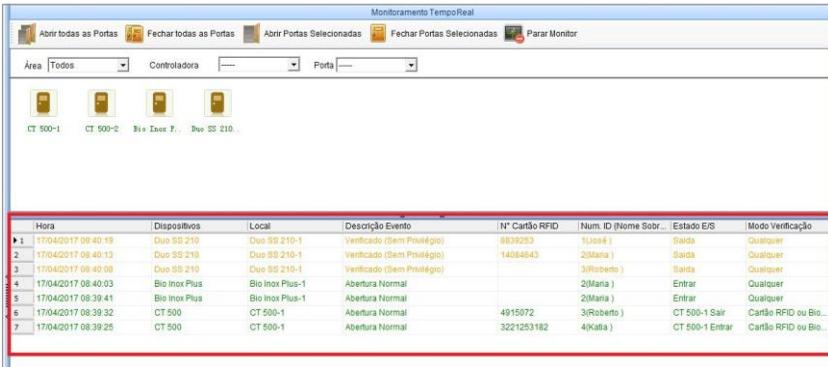
Área: Todos Controladora: ----- Porta: ----- 1

CT 500-1 CT 500-2 Bi o Incox P... Duo SS 210...

Hora	Dispositivos	Local	Descrição Evento	N° Cartão RFID	Num. ID (No)
------	--------------	-------	------------------	----------------	--------------

Iniciando monitoramento em tempo real

- Na imagem a seguir está representada a tela de monitoramento em tempo real, onde estão representados todos os dispositivos do sistema de controle de acesso e seus eventos estão descritos no enquadramento do quadro vermelho;



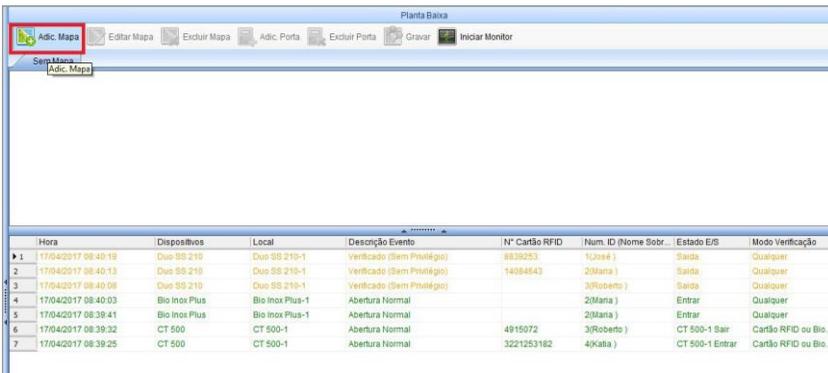
Eventos do sistema de controle de acesso

- Para parar o monitoramento, basta clicar sobre o botão Parar monitor e os eventos não serão mais exibidos.

## 6.11. Planta baixa

Semelhante ao monitoramento, a função Planta baixa permite que o usuário carregue uma planta de um ambiente ou organização onde as portas controladas pelo sistema estarão representadas graficamente. Para isso, siga o procedimento descrito a seguir:

- Na tela de visualização da função Planta baixa, clique sobre o botão Adic. mapa;



Tela inicial função planta baixa

- Na nova tela, insira o nome do mapa que está carregando e clique em Pesquisar para carregar o arquivo de imagem, na sequência, clique no botão Ok para exibir o mapa carregado;



Carregando mapa para sistema

3. Caso deseje, clique sobre os botões Editar mapa ou Excluir mapa para editar ou excluir o mapa carregado;
4. Clique no botão Adic. porta para posicionar as portas disponíveis no sistema de controle de acesso;

Hora	Dispositivos	Local	Descrição Evento	N° Cartão RFID	Num. ID (Nome Sobr...	Estado E/S	Modo Verificação
17/04/2017 08:40:19	Duo SS 210	Duo SS 210-1	Verificado (Sem Privilegio)	6829253	1(Luiz)	Saida	Qualquer
17/04/2017 08:40:13	Duo SS 210	Duo SS 210-1	Verificado (Sem Privilegio)	14084843	2(Maria)	Saida	Qualquer
17/04/2017 08:40:08	Duo SS 210	Duo SS 210-1	Verificado (Sem Privilegio)		3(Roberto)	Saida	Qualquer
17/04/2017 08:40:03	Bio Inox Plus	Bio Inox Plus-1	Abertura Normal		2(Maria)	Entrar	Qualquer
17/04/2017 08:39:41	Bio Inox Plus	Bio Inox Plus-1	Abertura Normal		2(Maria)	Entrar	Qualquer
17/04/2017 08:39:32	CT 500	CT 500-1	Abertura Normal	4915072	3(Roberto)	CT 500-1 Sair	Cartão RFID ou Bio...
17/04/2017 08:39:25	CT 500	CT 500-1	Abertura Normal	3221253182	4(Katia)	CT 500-1 Entrar	Cartão RFID ou Bio...

Mapa de planta baixa carregado

5. Na nova tela, selecione o dispositivo que deseja adicionar para que as portas disponíveis sejam exibidas no mapa. Clicando sobre o dispositivo no mapa, arraste-o e posicione-o sobre a área que representa fisicamente o local que está sendo controlado pelo dispositivo. Repita esse processo para quantos dispositivos for necessário. Por fim, clique no botão Iniciar monitor para que as portas online, sejam exibidas no mapa carregado;

Hora	Dispositivos	Local	Descrição Evento	N° Cartão RFID	Num. ID (Nome Sobr...	Estado E/S	Modo Verificação
17/04/2017 08:40:19	Duo SS 210	Duo SS 210-1	Verificado (Sem Privilegio)	6829253	1(Luiz)	Saida	Qualquer
17/04/2017 08:40:13	Duo SS 210	Duo SS 210-1	Verificado (Sem Privilegio)	14084843	2(Maria)	Saida	Qualquer
17/04/2017 08:40:08	Duo SS 210	Duo SS 210-1	Verificado (Sem Privilegio)		3(Roberto)	Saida	Qualquer
17/04/2017 08:40:03	Bio Inox Plus	Bio Inox Plus-1	Abertura Normal		2(Maria)	Entrar	Qualquer
17/04/2017 08:39:41	Bio Inox Plus	Bio Inox Plus-1	Abertura Normal		2(Maria)	Entrar	Qualquer
17/04/2017 08:39:32	CT 500	CT 500-1	Abertura Normal	4915072	3(Roberto)	CT 500-1 Sair	Cartão RFID ou Bio...
17/04/2017 08:39:25	CT 500	CT 500-1	Abertura Normal	3221253182	4(Katia)	CT 500-1 Entrar	Cartão RFID ou Bio...

Portas posicionadas no mapa

6. Clique sobre o botão Gravar para salvar as posições das portas no mapa ou Excluir porta para excluir algumas das portas adicionadas anteriormente. Para parar o monitoramento, clique sobre o botão Parar monitoramento.

## 6.12. Nome da leitora

Esta função permite editar o nome das leitoras adicionadas no sistema de controle de acesso que estão instaladas nas portas controladas pelos dispositivos. Para isso, siga o processo a seguir:

1. Na tela inicial de exibição das leitoras, selecione a leitora que deseja editar e clique no botão Editar;

	Nome de Dispositivo	Nome de Porta	Número da Porta	Número da Leitora	Nome da Leitora	Entrada / Saída
1	CT 500	CT 500-1	1	1	CT 500-1 Entrar	Entrada
2	CT 500	CT 500-1	1	2	CT 500-1 Sair	Saída
3	CT 500	CT 500-2	2	3	CT 500-2 Entrar	Entrada
4	CT 500	CT 500-2	2	4	CT 500-2 Sair	Saída

Tela inicial de edição de leitoras

**Importante:** é possível editar apenas uma leitora por vez.

2. Na nova tela, altere o nome da leitora e clique no botão Ok para confirmar. Sincronize as informações com os dispositivos;

Nome de Máquina: CT 500  
Nome de Porta: CT 500-1  
Número da Leitora: 1  
Nome da Leitora: Recepção - Entrada  
Estado Entrada e Saída: Entrada

OK Cancelar

Editando nome da leitora

3. Repita esse processo para alterar a nomenclatura de todas as leitoras que desejar. Clique sobre o botão Registro para verificar todas as modificações realizadas por outros operadores e pelo seu perfil no sistema de controle de acesso.

	Usuário	Horário	Tipo de objeto	Ação	Mensagem
1	admin	17/04/2017 09:30:45	Reader	Adicionar	Atualizar Leitora:Recepção - Entrada
2	admin	17/04/2017 09:29:13	Reader	Adicionar	Atualizar Leitora:Recepção - Entrada
3	admin	11/04/2017 08:40:54	Reader	Adicionar	Adicionar Leitoras em lote
4	admin	05/04/2017 11:02:35	Reader	Adicionar	Adicionar Leitoras em lote
5	admin	28/12/2015 17:10:58	Reader	Adicionar	Adiciona leitoras em lote
6	admin	28/12/2015 17:01:41	Reader	Adicionar	Adiciona leitoras em lote
7	admin	28/12/2015 16:57:56	Reader	Adicionar	Adiciona leitoras em lote
8	admin	28/12/2015 16:57:30	Reader	Adicionar	Adiciona leitoras em lote

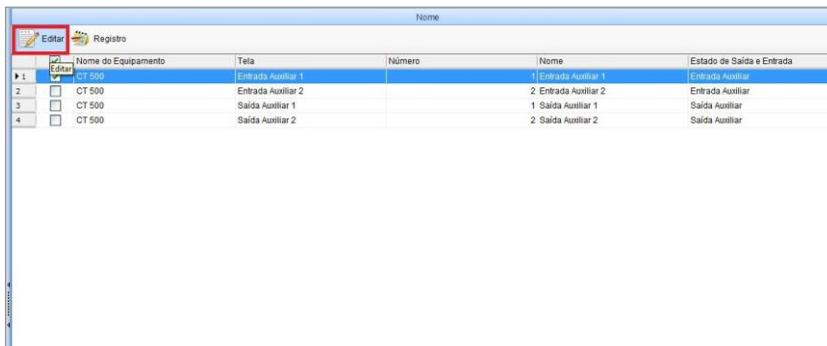
Registros de logs

**Importante:** função disponível apenas para dispositivos CT 500.

### 6.13. Entradas e saídas auxiliares

Da mesma forma que na função Nome da leitora, esta função permite que se altere a nomenclatura das entradas e saídas auxiliares do dispositivo. Para isso, siga o procedimento:

1. Na tela inicial de exibição das entradas e saídas auxiliares, selecione a entrada ou saída auxiliar que deseja editar e clique no botão Editar;

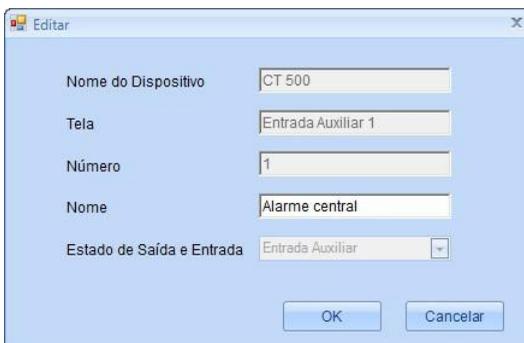


	Nome do Equipamento	Tela	Número	Nome	Estado de Saída e Entrada
1	CT 500	Entrada Auxiliar 1		1   Entrada Auxiliar 1	Entrada Auxiliar
2	CT 500	Entrada Auxiliar 2		2   Entrada Auxiliar 2	Entrada Auxiliar
3	CT 500	Saída Auxiliar 1		1   Saída Auxiliar 1	Saída Auxiliar
4	CT 500	Saída Auxiliar 2		2   Saída Auxiliar 2	Saída Auxiliar

Tela inicial de entradas e saídas auxiliares

**Importante:** é possível editar apenas uma entrada ou saída auxiliar por vez.

2. Na nova tela, altere o nome da entrada ou saída auxiliar e clique no botão Ok para confirmar. Sincronize as informações com os dispositivos;



Nome do Dispositivo: CT 500

Tela: Entrada Auxiliar 1

Número: 1

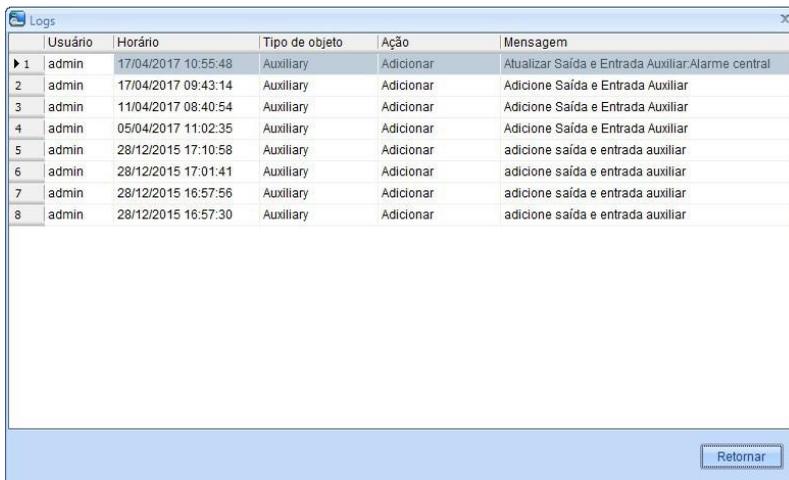
Nome: Alarme central

Estado de Saída e Entrada: Entrada Auxiliar

OK Cancelar

Editando nome de entradas e saídas auxiliares

3. Repita este processo para todas as leitoras que desejar alterar a nomenclatura. Caso deseje, clique sobre o botão Registro e serão exibidas todas as modificações realizadas por outros operadores e pelo seu perfil no sistema de controle de acesso.



	Usuário	Horário	Tipo de objeto	Ação	Mensagem
1	admin	17/04/2017 10:55:48	Auxiliary	Adicionar	Atualizar Saída e Entrada Auxiliar:Alarme central
2	admin	17/04/2017 09:43:14	Auxiliary	Adicionar	Adicione Saída e Entrada Auxiliar
3	admin	11/04/2017 08:40:54	Auxiliary	Adicionar	Adicione Saída e Entrada Auxiliar
4	admin	05/04/2017 11:02:35	Auxiliary	Adicionar	Adicione Saída e Entrada Auxiliar
5	admin	28/12/2015 17:10:58	Auxiliary	Adicionar	adicione saída e entrada auxiliar
6	admin	28/12/2015 17:01:41	Auxiliary	Adicionar	adicione saída e entrada auxiliar
7	admin	28/12/2015 16:57:56	Auxiliary	Adicionar	adicione saída e entrada auxiliar
8	admin	28/12/2015 16:57:30	Auxiliary	Adicionar	adicione saída e entrada auxiliar

[Retornar](#)

Registro de logs de entradas e saídas auxiliares

**Importante:** função disponível apenas para dispositivos CT 500.

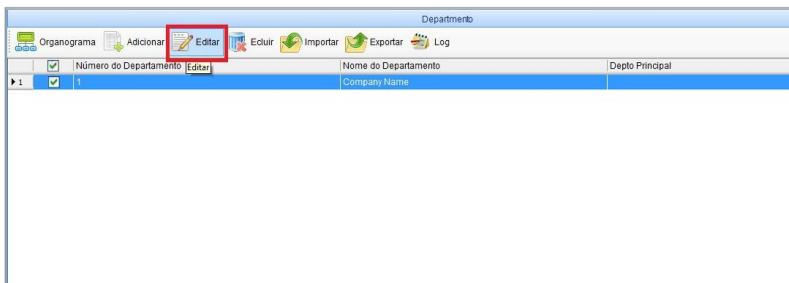
## 7. Usuários

Nesta seção são cadastrados e configurados os usuários que irão compor o banco de dados do sistema de controle de acesso, bem como os departamentos aos quais pertencem. A seguir, estão listados os tópicos que tratarão dos seguintes assuntos, respectivamente: Cadastro de departamentos, Cadastro de usuários e Cadastros dos métodos de autenticação (cartão RFID, Senha, Biometria digital, etc.), conforme a disponibilidade do dispositivo controlador de acesso adicionado ao sistema.

### 7.1. Departamentos

Esta função possibilita o cadastro dos departamentos presentes na organização ou empresa. Esses departamentos serão vinculados aos usuários posteriormente. Note que já existe um departamento cadastrado de fábrica no software de nome Company name, que é um departamento raiz e não poderá ser excluído, pode apenas ser editado. Para fazer a edição desse departamento e criar novos, siga o procedimento:

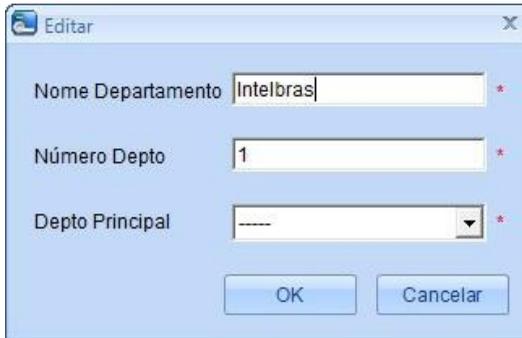
1. Na tela inicial dos departamentos, selecione o departamento raiz e clique em Editar;



Departamento		
Organograma	Adicionar	Editar
<input checked="" type="checkbox"/>	Número do Departamento	<a href="#">[editar]</a>
<input checked="" type="checkbox"/>	Nome do Departamento	Nome do Departamento
<input checked="" type="checkbox"/>	Company Name	Depdo Principal

Tela inicial departamentos

2. Na nova tela, altere o nome do departamento e deixe o campo Depto principal em branco (----). Neste campo será feito o vínculo dos demais departamentos criados posteriormente. Clique em Ok para confirmar as modificações;



Editar

Nome Departamento Intelbras \*

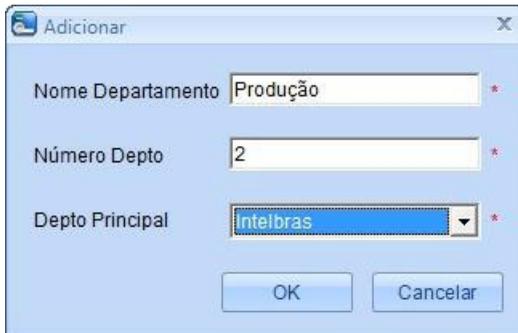
Número Depto 1 \*

Depto Principal ---- \*

OK Cancelar

Editando departamento raiz

3. Para criar novos departamentos, clique no botão Adicionar da tela inicial dos departamentos. Na nova tela, preencha o nome do novo departamento, altere seu número identificador para 2 (número preenchido sequencialmente) e, por fim, no campo Depto principal, vincule-o ao departamento raiz, ou seja Intelbras no exemplo;



Adicionar

Nome Departamento Produção \*

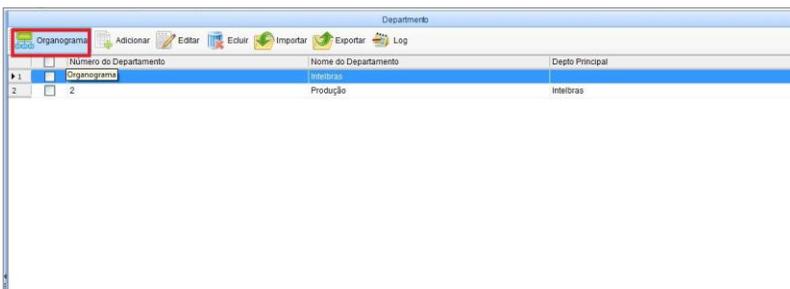
Número Depto 2 \*

Depto Principal Intelbras \*

OK Cancelar

Adicionando novos departamentos

4. Repita o processo acima para criar novos departamentos sempre que necessário, e vincule-os conforme a necessidade de sua organização ou empresa;
5. Caso queira excluir algum dos departamentos criados, selecione-o na tela inicial e clique no botão Excluir;
6. É possível clicar nos botões Exportar ou Importar para salvar os departamentos criados em Excel ou .txt ou mesmo trazer uma planilha de departamentos previamente criados, em um destes dos formatos para dentro do sistema de controle de acesso;
7. Por fim, após criar e vincular todos os departamentos da organização ou empresa, é possível visualizar o organograma do mesmo clicando no botão Organograma na tela inicial;



Departamento			
	Número do Departamento	Nome do Departamento	Depto Principal
1	1	Intelbras	
2	2	Produção	Intelbras

Selecionando organograma

- Na nova tela, estarão representados por ordem, todos os departamentos criados anteriormente e devidamente vinculados. Nesta tela também é possível Adicionar, Editar, Excluir e Retornar para a tela inicial.



Visualizando organograma

## 7.2. Sétimo passo usuários

Para cadastrar usuários e vinculá-los aos departamentos criados anteriormente, siga os passos descritos abaixo:

- Na tela inicial de usuários, clique em Adicionar para inserir um novo cadastro de usuário.

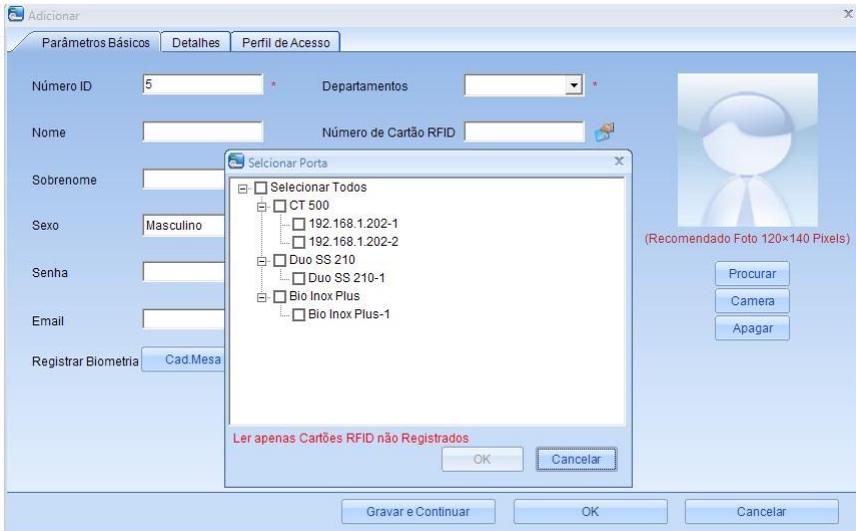
Usuários											
	Número ID	Nome	Sobrenome	Número do Car...	Número do Dep...	Nome do Depa...	Sexo	Número Biometri...	Número de Blo...	Num. Velas	Número de Faces
1	1	José		8839253	1	Intelbras	Masculino	2	0	0	0
2	2	Maria		14084543	1	Intelbras	Masculino	1	0	0	0
3	3	Roberto		4915072	1	Intelbras	Masculino	0	0	0	0
4	4	Katia		3221253182	1	Intelbras	Feminino	2	0	0	0

Tela inicial Usuários

- Na nova janela, será necessário preencher as informações de 3 abas do cadastro. São elas: Parâmetros Básicos, Detalhes e Perfil de Acesso.
- Na aba de Parâmetros Básicos, entre com as informações de Nome, Sobrenome, Sexo, é possível cadastrar também uma senha numérica no campo Senha (4 a 6 dígitos), E-mail, Departamentos que o usuário pertence e demais chaves de comunicação como (Cartão RFID e Biometria Digital).

Aba Parâmetros Básicos

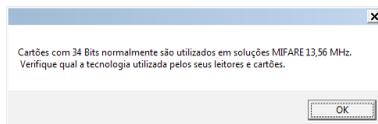
4. Para o cadastro do campo Número de Cartão RFID, clique sobre o ícone  para abrir a lista de dispositivos adicionais habilitados para a leitura do Cartão RFID. Caso opte por fazer o cadastro do cartão RFID utilizando o Cadastrador de Mesa, basta clicar sobre o campo em branco com o mouse e aproximar o cartão da área de leitura do cartão RFID do Cadastrador de Mesa.



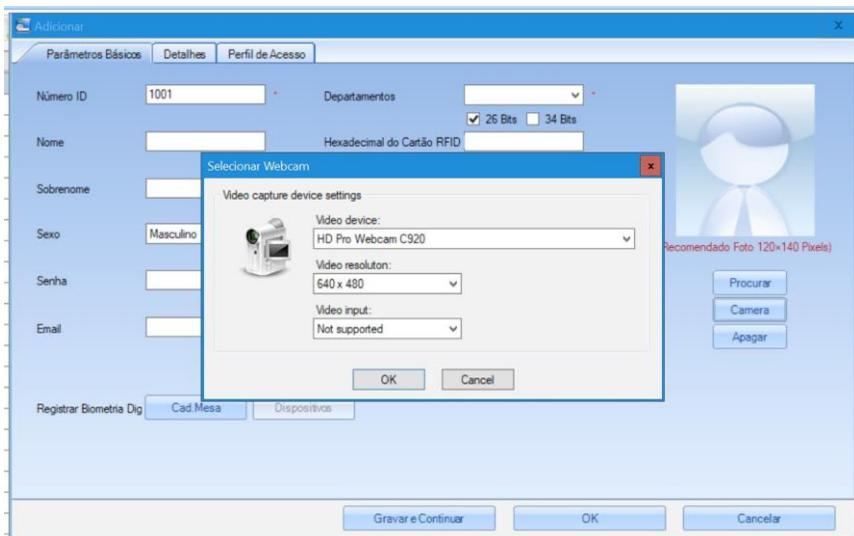
Cadastro de Cartão RFID

### Importante:

- » Após selecionar os dispositivos para fazer a leitura do Cartão RFID, selecione o padrão do cartão utilizado (26 bits para 125KHz) e (34 Bits para 13,56MHz Mifare).3
- » Logo após o campo Número de Cartão RFID é possível cadastrar o valor do cartão RFID em hexadecimal Hexadecimal do Cartão RFID, esta função é importante para o cadastro das tags veiculares UHF.
- » Caso seja utilizado o cadastrador de mesa, verifique o checkbox com o padrão da chave (26 bits) ou (34 bits). Esse padrão é essencial para o bom funcionamento da tag cadastrado. Par o sistema que funciona na frequência 125KHz o padrão de fábrica é 26 bits. Já para os sistemas que funcionam na frequência 13,56MHz (Mifare), o padrão correto é 34 bits. Ao alterar este padrão, verifique as configurações do seu leitor escravo conectado aos controladores de acesso.
- » A seguinte mensagem de alerta é exibida pelo software ao alterar o padrão de fábrica 26 bits para 34 bits.



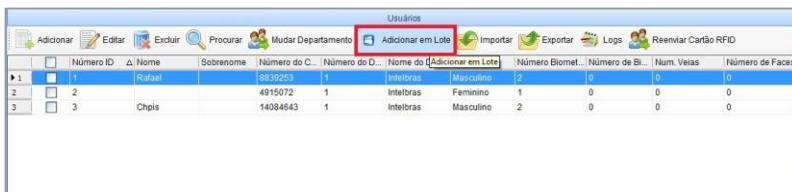
- » É possível atribuir a foto do usuário através da webcam, para isso, clique sobre a opção Câmera para fazer a captura da imagem do usuário.
- » Caso haja mais de um dispositivo de câmera instalado em seu computador, uma nova janela se abrirá para que seja feita a escolha de qual das câmeras instaladas será utilizada para efetuar a captura da imagem. Veja a representação na figura abaixo:



### 7.3. Cadastro de usuários em lote

O software SoapAdmin 3.5 possui uma versatilidade para eventualidades em que seja necessário o cadastro de uma grande quantidade de usuários de uma só vez, a função Adicionar em lote. Para isso, siga o procedimento descrito abaixo:

1. Na tela inicial dos Usuários clique sobre o botão Adicionar em lote;



Função de cadastro de usuários em lote

2. Na nova tela, é necessário digitar as informações para o cadastro em lote. São elas:
  - » **Algarismos-padrão:** neste campo são inseridos antes ou depois dos parênteses com asterisco algum tipo de número que servirá de prefixo (que vem antes) ou sufixo (que vem depois) do cadastro do usuário. Exemplo 221 ou 122, sendo que o numeral (22) é padrão e está representado como prefixo ou sufixo do número do cadastro sequência 1.
  - » **Num. máximo de dígitos (\*):** é a quantidade máxima que será cadastrada de usuários. Exemplo: se o campo for preenchido com o número 2, serão cadastrados usuários de 1 a 99. Caso seja preenchido com o número 3, serão cadastrados usuários de 1 a 999, e assim sucessivamente.
  - » **De, até:** determina o número inicial e o número final do lote a ser cadastrado. Exemplo: de 1 a 20, o primeiro cadastro será o número 1 e o último será o número 20.
  - » Também é possível copiar os campos de um cadastro já existente para os novos que serão cadastrados. Esses campos estão representados por caixas de marcação e devem ser marcados conforme a necessidade do cadastro a ser realizado. São eles: Departamento, Sexo, Escolaridade, Tipo de contrato, Tipo, Telefone e Acesso combinado.
  - » Ao final clique em Ok e aguarde o término do cadastro.

Adicionar em Lote

Do Usuário: Rafael (1) Copiar Dados

Número ID

Algarismos Padrão: 22(\*)

Núm. Máximo de Dígitos(\*): 2

De: 1 Até: 20

Selecione os campos para copiar

Departamento

Sexo

Escolaridade

Tipo contrato

Tipo

Telefone

Acesso Combinado

Progresso

Máximo 10000 Usuários

OK Cancelar

Configurações para o cadastro em lote

- Para voltar à tela de usuários, clique em Cancelar;
- Note que agora estão aparecendo os 20 perfis de usuários criados acompanhados do prefixo (22). Também estará presente o primeiro usuário criado manualmente e que serviu de fonte para cópia dos dados para os demais.

Usuários											
	Número ID	Nome	Sobrenome	Número do Car.	Número do Dep.	Nome do Depa.	Sexo	Número Biometr.	Número de Blo.	Num. Veias	Número de Faces
1	1	Rafael		8839253	1	InteIbraa	Masculino	2	0	0	0
2	2201	2201			1	InteIbraa	Masculino	0	0	0	0
3	2202	2202			1	InteIbraa	Masculino	0	0	0	0
4	2203	2203			1	InteIbraa	Masculino	0	0	0	0
5	2204	2204			1	InteIbraa	Masculino	0	0	0	0
6	2205	2205			1	InteIbraa	Masculino	0	0	0	0
7	2206	2206			1	InteIbraa	Masculino	0	0	0	0
8	2207	2207			1	InteIbraa	Masculino	0	0	0	0
9	2208	2208			1	InteIbraa	Masculino	0	0	0	0
10	2209	2209			1	InteIbraa	Masculino	0	0	0	0
11	2210	2210			1	InteIbraa	Masculino	0	0	0	0
12	2211	2211			1	InteIbraa	Masculino	0	0	0	0
13	2212	2212			1	InteIbraa	Masculino	0	0	0	0
14	2213	2213			1	InteIbraa	Masculino	0	0	0	0
15	2214	2214			1	InteIbraa	Masculino	0	0	0	0
16	2215	2215			1	InteIbraa	Masculino	0	0	0	0
17	2216	2216			1	InteIbraa	Masculino	0	0	0	0
18	2217	2217			1	InteIbraa	Masculino	0	0	0	0
19	2218	2218			1	InteIbraa	Masculino	0	0	0	0
20	2219	2219			1	InteIbraa	Masculino	0	0	0	0
21	2220	2220			1	InteIbraa	Masculino	0	0	0	0

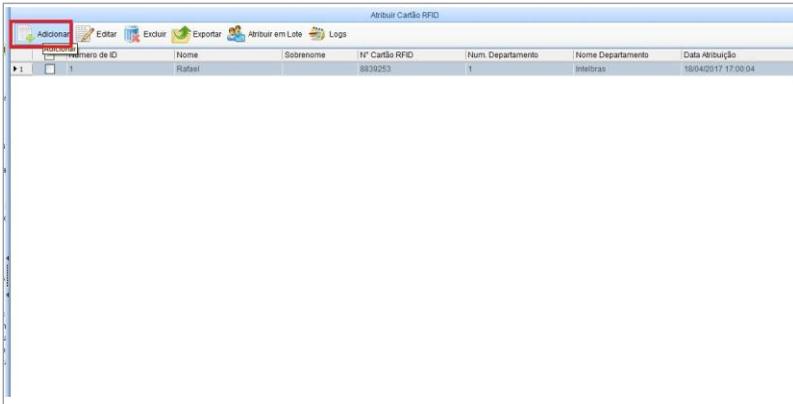
Lista de usuários cadastrados em lote

- Importante:** » É necessário ter ao menos um usuário cadastrado manualmente para servir de base para os demais, que serão cadastrados em lote.
- » O número máximo de usuários cadastrados nesta função é de 10.000 por vez.
  - » Após o cadastro em lote, é necessário editar cada usuário individualmente para completar seu cadastro, atribuindo-lhe o nome e outras informações necessárias, bem como vinculá-lo a um perfil de acesso.

## Registro de cartão RFID

Essa função possibilita atribuir os cartões RFID aos usuários cadastrados manualmente ou em lote, de duas formas: Adicionar a chave do cartão RFID a cada usuário sem efetuar a leitura do mesmo ou Atribuir o cartão RFID em lote para um número determinado de usuários. As diferenças de cada uma dessas modalidades estão listadas a seguir:

1. Para adicionar a chave do cartão RFID, sem passá-lo no leitor, é necessário ter conhecimento da chave contida no cartão que se deseja adicionar. Uma vez conhecido esse número, clique no botão Adicionar na tela inicial da função Registrar cartão RFID;



Tela inicial de registro de cartão RFID

2. Na nova tela, selecione o usuário e digite o número da chave do cartão RFID e clique em Ok;



A screenshot of a dialog box titled "Adicionar". It contains two input fields: "Usuário" with a dropdown menu showing "1-Rafael" and "N° Cartão RFID" with a text input field containing "8839253". Both fields have a red asterisk to their right. At the bottom are "OK" and "Cancelar" buttons.

Tela de adição da chave do cartão RFID

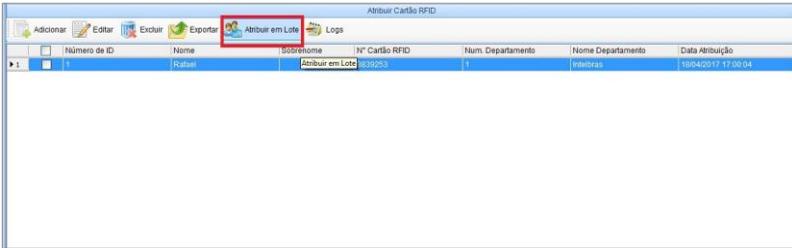
3. É possível editar também uma chave vinculada ao usuário anteriormente, para isso, selecione o usuário na lista de usuários cadastrados e clique no botão Editar. Após as alterações, clique em Ok para confirmar e sincronize as informações com os dispositivos;



A screenshot of a dialog box titled "Editar". It contains two input fields: "Usuário" with a dropdown menu showing "1-Rafael" and "N° Cartão RFID" with a text input field containing "8839253". Both fields have a red asterisk to their right. At the bottom are "OK" and "Cancelar" buttons.

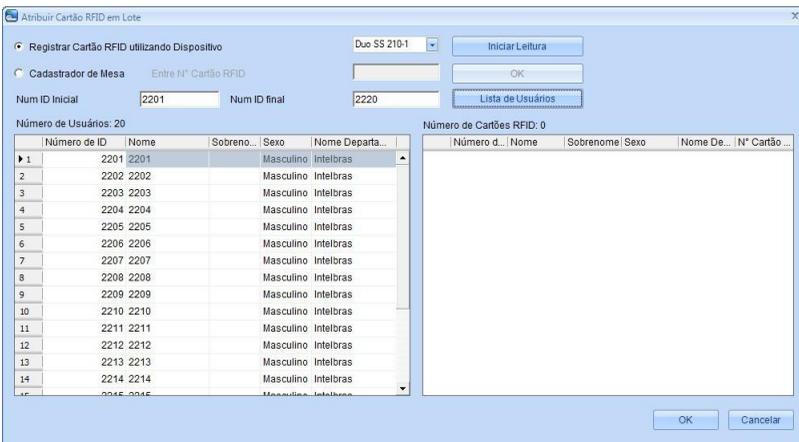
Editando cartão RFID do usuário

4. Outra função importante é a função Atribuir em lote, que permite atribuir várias chaves aos usuários cadastrados anteriormente de uma vez só. Para isso, clique no botão Atribuir em lote na tela inicial da função Registrar cartão RFID;



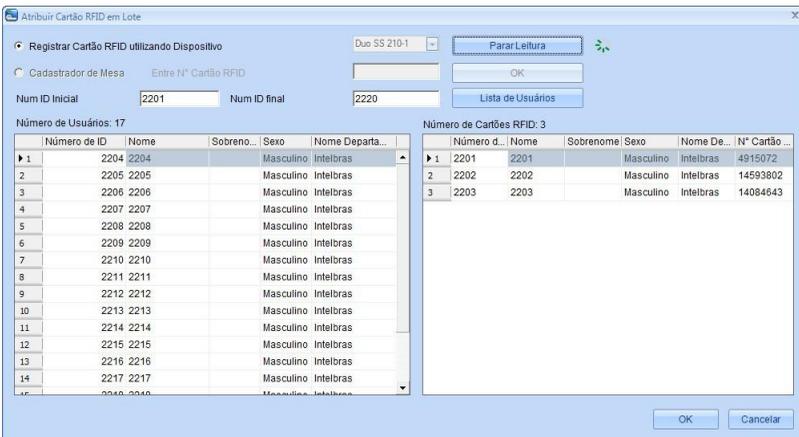
Selecionando função de cadastro em lote

5. Na nova tela, será necessário definir o método de leitura dos cartões RFID sendo as opções Dispositivo ou Cadastrador de mesa. Caso escolha Dispositivo, será necessário selecionar o dispositivo para leitura. Na sequência, é necessário atribuir o número do ID (usuário) inicial e o número de ID final e clicar no botão Lista de usuários;



Listando usuários para leitura

6. Após listados todos os usuários selecionados, clique no botão Iniciar leitura. À medida que os cartões forem lidos, o sistema irá atribuir o primeiro cartão lido ao primeiro usuário da lista e assim sucessivamente;



Atribuindo cartões em lote

7. Durante a leitura é possível pausar o processo, basta clicar no botão Parar leitura que o processo é pausado. Para voltar ao processo, clique no botão Iniciar leitura novamente;
8. Ao final das leituras, todos os usuários listados estarão no outro lado da coluna e é necessário clicar em Ok para validar as informações, sincronizando as informações posteriormente com os demais dispositivos do sistema de controle de acesso.

### Importar e exportar usuários

1. Também é possível exportar para Excel, txt, o banco de dados de usuários ou importar nestes mesmos formatos planilhas ou informações cadastradas fora do sistema. Para exportar, clique no botão Exportar, selecione a extensão Excel ou txt e salve o arquivo. Para importar, clique no botão Importar, selecione a extensão Excel ou txt e clique no botão Prox., na sequência, selecione os campos que deseja trazer do relatório para o sistema e clique em Prox. Até o término do processo.

	Número ID	Nome	Sobrenome	Número do Car...	Número do Dep...	Nome do Depa...	Sexo	Número Biometri...	Número de Bio...	Num. Veias	Número de Faces
1	1	José		8839253	1	Intelbras	Masculino	2	0	0	0
2	2	Maria		14084643	1	Intelbras	Masculino	1	0	0	0
3	3	Roberto		4915072	1	Intelbras	Masculino	0	0	0	0
4	4	Katia			1	Intelbras	Feminino	2	0	0	0

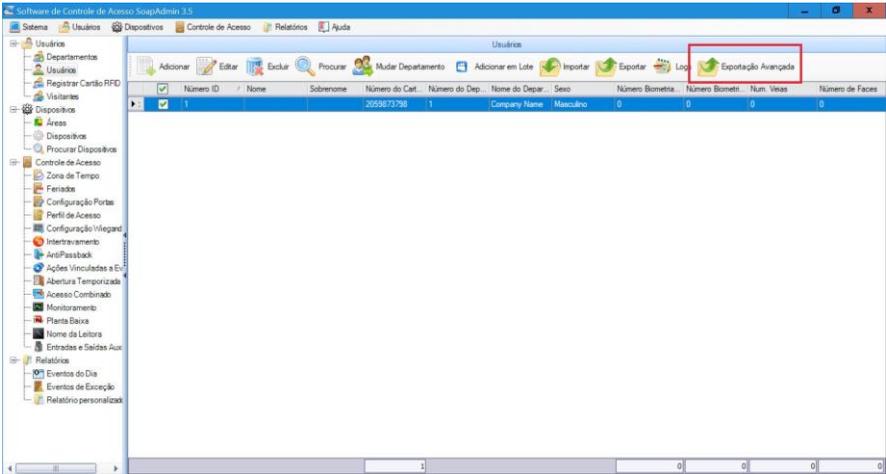
Importar ou exportar informações

Selecionando arquivo para importar

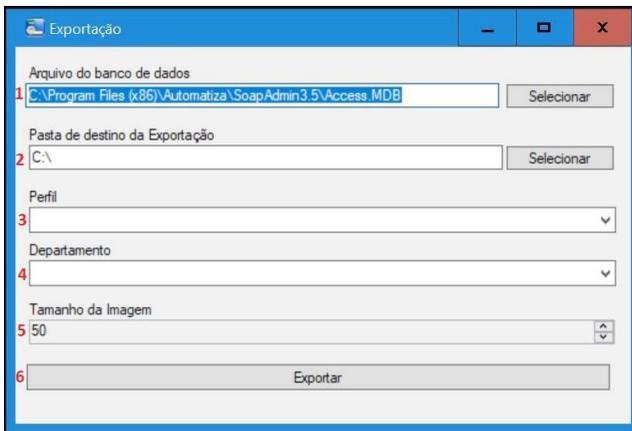
Selecionando informações do arquivo para importar

**Importante:** a função de Importar, necessita que os campos presentes na Column Name estejam presentes na planilha a ser importada, ou seja, uma vez exportado para Excel, é possível fazer alterações do arquivo e importá-lo novamente para o sistema.

2. Também é possível exportar de forma avançada para arquivo texto (Compatível com Excel), o banco de dados de usuários. Para exportar de forma avançada, clique no botão Exportação Avançada.



Exportação Avançada



Selecionando informações do arquivo para importar

Será apresentada a tela de exportação da imagem 111. Nela podemos:

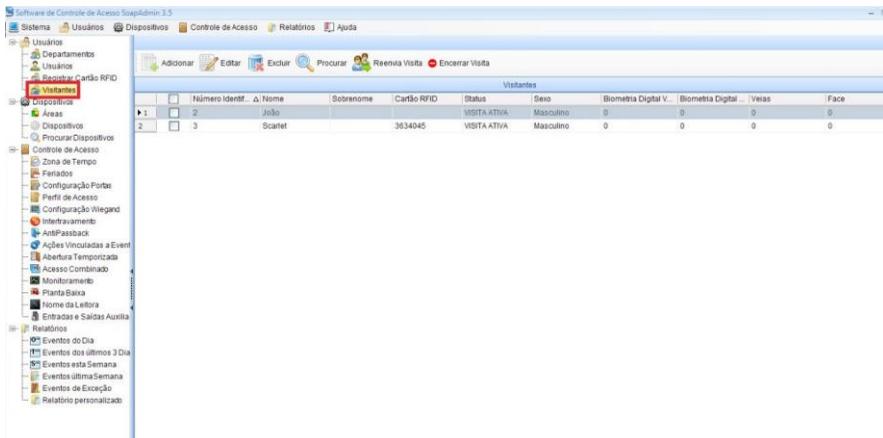
- » (1) Selecionar de qual banco de dados iremos exportar a informações;
- » (2) Selecionar a pasta onde será salvo o arquivo com os usuários exportados;
- » (3) Definir um filtro sobre a lista de usuários a ser exportada baseado no perfil dos mesmos, ou seja, somente usuários com o perfil selecionado serão exportados, caso não selecionado nenhum perfil, serão exportados os usuários independentemente do perfil em que estão inseridos;
- » (4) Definir um filtro sobre a lista de usuários a ser exportada baseado no departamento dos mesmos, ou seja, somente usuários com o departamento selecionado serão exportados, caso não selecionado nenhum departamento, serão exportados os usuários independentemente do departamento em que estão inseridos;
- » (5) Definir qual o tamanho da imagem em relação ao tamanho atual da mesma no banco de dados em porcentagem, exemplo: caso definido 60% a imagem exportada terá 60 por cento do tamanho da imagem salva no banco de dados.
- » (6) Realizar o processo de exportação.

Os campos exportados são:

- » **UID:** número identificador do usuário;
- » **Nome\_Usuario:** nome do usuário;
- » **Cartao:** código do cartão do usuário;
- » **Senha:** senhas de acesso dos usuários;
- » **Departamento:** departamento ao qual o usuário pertence;
- » **Grupo\_de\_pontos\_de\_acesso:** perfil de acesso do usuário;
- » **Biometria:** código texto referente a biometria do usuário;
- » **Foto:** foto convertida para texto.

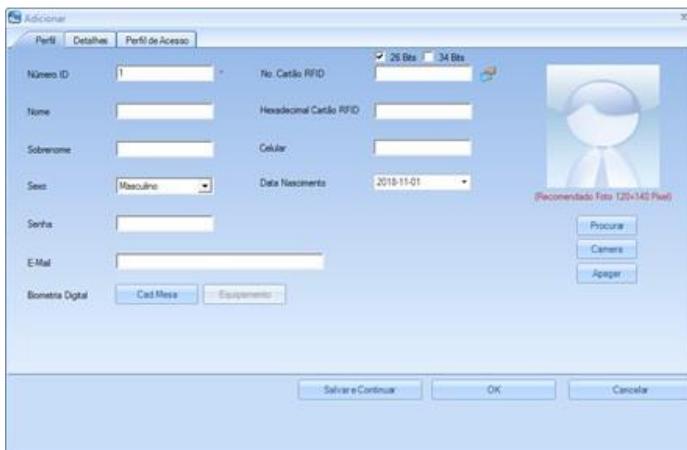
## Cadastro de Visitantes

Na tela inicial do software, dentro do módulo Usuários, é possível acessar a tela de cadastro e visualização de visitantes. Esta função permite criar usuários que estarão ativos em determinados pontos do sistema de controle de acesso por um período de validade pré-determinado pelo operador do software.



Módulo Visitantes

1. Na nova janela, clique no botão Adicionar para criar um novo perfil de visitantes e navegue pelas abas Perfis, Detalhes e Perfil de Acesso, semelhantes às de um usuário comum.



Aba Perfil Cadastro de Visitantes

**Importante:** caso utilize o cadastrador de mesa para efetuar a captura do cartão RFID do visitante, verificar o padrão de bits configurado no sistema. Para um sistema 125 KHz o padrão de fábrica é 26 bits, já setado. Já para um sistema na frequência 13,56 MHz o padrão correto é 34 bits. Neste caso pode ser necessária a configuração física dos leitores instalados nos controladores de acesso.

## 8. Relatórios

A função Relatórios torna possível filtrar e demonstrar os eventos gerados durante a operação do sistema de controle de acesso. Esta função permite ao operador do software consultar e gerar relatórios customizados na sequência:

- » **Eventos do dia:** traz predefinidos os eventos gerados no dia corrente. Para consultá-los clique na função Eventos do dia e preencha as informações pertinentes para a exibição. Ao final, clique em Procurar, para que os eventos sejam demonstrados na tela.

Período	Nº Cartão RFID	Nome Dispositivo	Estado E/S	Nome	Modo Verificação
2017-04-20		Duo SS 210			Qualquer

Hora	Num. ID	Nome	Sobrenome	Nº Cartão	Dispositivos	Local	Modo Verific.	Estado E/S	Evento	Descrição
2017-04-20 08:12:28	1	Rafael		8839253	Duo SS 210	Duo SS 210-1	Qualquer	Entrar	Verificado (Sem P.	

Eventos do dia

- » **Eventos dos últimos 3 dias:** traz predefinidos os eventos gerados nos últimos 3 dias a contar do dia corrente. Para consultá-los, clique na função Eventos dos últimos 3 dias, faça os filtros necessários e clique em Procurar para listar todos os eventos na tela.

Hora	Num. ID	Nome	Sobrenome	Nº Cartão	Dispositivos	Local	Modo Verific.	Estado E/S	Evento	Descrição
2017-04-20 09:12:28	1	Rafael		8839253	Duo SS 210	Duo SS 210-1	Qualquer	Entrar	Verificado (Sem P.	
2017-04-18 17:38:23	3	Chpils		14084643	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:36:53	3	Chpils		14084643	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:33:22	3	chpils		14084643	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:33:07	3	chpils		14084643	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:30:16	3	chpils		14084643	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:30:12	3	chpils		14084643	Duo SS 210	Duo SS 210-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:27:56	1	Rafael		8839253	Duo SS 210	Duo SS 210-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:27:52	1	Rafael		8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:23:30	3	chpils		148811530	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:23:22	3	chpils		148811530	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:23:07	3	chpils		148811530	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:16:52	1	Rafael		8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:16:46	1	Rafael		8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:13:49	1	Rafael		8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:07:02	1	Rafael		8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
2017-04-18 17:06:56	1	Rafael		8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	

Eventos dos últimos 3 dias

- » **Eventos esta semana:** traz predefinidos os eventos gerados na semana corrente a contar do dia de cadastro. Por exemplo, ao consultar esse relatório na quinta-feira, teremos um horizonte de eventos que começa na segunda-feira e vai até a quinta-feira da semana corrente. Para consultá-lo, clique na função **Eventos esta semana**, faça os filtros necessários e clique em **Procurar** para listar todos os eventos na tela.

Eventos da Semana										
Exportar Excluir todos Eventos Procurar Período: 2017-04-17 00:00 -- 2017-04-23 23:59 Num. ID: <input type="text"/> N° Cartão RFID: <input type="text"/> Nome Dispositivo: <input type="text"/> Nome: <input type="text"/> Estado E/S: <input type="text"/> Descrição Evento: <input type="text"/> Modo Verificação: Qualquer <input type="text"/> <input type="button" value="Procurar"/> <input type="button" value="Cancelar"/>										
Hora	Num. ID	Nome	Sobrenome	N° Cartão	Dispositivos	Local	Modo Verific.	Estado E/S	Evento	Descrição
1	2017-04-20 09:12:28	1	Rafael	8839253	Duo SS 210	Duo SS 210-1	Qualquer	Entrar	Verificado (Sem P.	
2	2017-04-18 17:38:23	3	Chips	14084643	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
3	2017-04-18 17:38:53	3	Chips	14084643	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
4	2017-04-18 17:33:22	3	chips	14084643	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
5	2017-04-18 17:33:07	3	chips	14084643	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
6	2017-04-18 17:30:16	3	chips	14084643	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
7	2017-04-18 17:30:12	3	chips	14084643	Duo SS 210	Duo SS 210-1	Qualquer	Entrar	Abertura Normal	
8	2017-04-18 17:27:56	1	Rafael	8839253	Duo SS 210	Duo SS 210-1	Qualquer	Entrar	Abertura Normal	
9	2017-04-17 17:27:52	1	Rafael	8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
10	2017-04-18 17:23:30	3	chips	148811530	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
11	2017-04-18 17:23:22	3	chips	148811530	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
12	2017-04-18 17:23:07	3	chips	148811530	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
13	2017-04-18 17:16:52	1	Rafael	8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
14	2017-04-18 17:16:46	1	Rafael	8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
15	2017-04-18 17:13:49	1	Rafael	8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
16	2017-04-18 17:07:02	1	Rafael	8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
17	2017-04-18 17:06:56	1	Rafael	8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
18	2017-04-17 08:40:19	1	José	8839253	Duo SS 210	Duo SS 210-1	Qualquer	Saida	Verificado (Sem P.	
19	2017-04-17 08:40:13	2	Maria	14084643	Duo SS 210	Duo SS 210-1	Qualquer	Saida	Verificado (Sem P.	
20	2017-04-17 08:40:06	3	Rosierito	4910972	Duo SS 210	Duo SS 210-1	Qualquer	Saida	Verificado (Sem P.	
21	2017-04-17 08:40:03	2	Maria	14084643	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	
22	2017-04-17 08:39:41	2	Maria	14084643	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Entrar	Abertura Normal	

Eventos esta semana

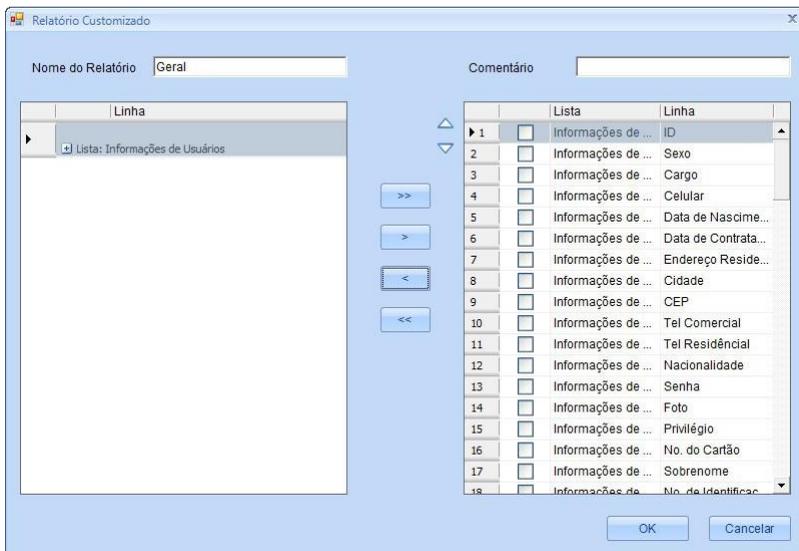
- » **Eventos última semana:** traz predefinidos os eventos gerados na semana anterior tomando como referência a semana corrente. Para consultá-lo, clique na função **Eventos da última semana**, faça os filtros necessários e clique em **Procurar** para listar todos os eventos na tela.

Eventos última Semana										
Exportar Excluir todos Eventos Procurar Período: 2017-04-10 00:00 -- 2017-04-16 23:59 Num. ID: <input type="text"/> N° Cartão RFID: <input type="text"/> Nome Dispositivo: <input type="text"/> Nome: <input type="text"/> Estado E/S: <input type="text"/> Descrição Evento: <input type="text"/> Modo Verificação: Qualquer <input type="text"/> <input type="button" value="Procurar"/> <input type="button" value="Cancelar"/>										
Hora	Num. ID	Nome	Sobrenome	N° Cartão	Dispositivos	Local	Modo Verific.	Estado E/S	Evento	Descrição
1	2017-04-13 17:02:23	1	José	8839253	Duo SS 210	Duo SS 210-1	Qualquer	Pausa-Sai	Abertura Normal	
2	2017-04-13 17:02:21	4	Katia	3221255162	Duo SS 210	Duo SS 210-1	Qualquer	Saida	Verificado (Sem P.	
3	2017-04-13 16:54:13	4	Katia	3221255162	Duo SS 210	Duo SS 210-1	Qualquer	Entrar	Abertura Normal	
4	2017-04-13 16:54:07	1	José	8839253	Duo SS 210	Duo SS 210-1	Qualquer	Saida	Verificado (Sem P.	
5	2017-04-13 14:26:05	1	José	8839253	Duo SS 210	Duo SS 210-1	Qualquer	Entrar	Abertura Normal	
6	2017-04-13 14:22:07	1	José	8839253	Duo SS 210	Duo SS 210-1	Qualquer	Saida	Verificado (Sem P.	
7	2017-04-13 14:22:54	1	José	8839253	Duo SS 210	Duo SS 210-1	Qualquer	Saida	Verificado (Sem P.	
8	2017-04-11 14:43:04	1	Zezinho Tr.	8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Saida	Verificado (Sem P.	
9	2017-04-11 14:43:04	1	Zezinho Tr.		Bio Inox Plus	Bio Inox Plus-1	Qualquer	Saida	Verificado (Sem P.	
10	2017-04-11 14:43:00	1	Zezinho Tr.		Bio Inox Plus	Bio Inox Plus-1	Qualquer	Saida	Verificado (Sem P.	
11	2017-04-11 14:43:00	1	Zezinho Tr.	8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Saida	Verificado (Sem P.	
12	2017-04-11 14:42:54	1	Zezinho Tr.		Bio Inox Plus	Bio Inox Plus-1	Qualquer	Saida	Verificado (Sem P.	
13	2017-04-11 14:42:54	1	Zezinho Tr.	8839253	Bio Inox Plus	Bio Inox Plus-1	Qualquer	Saida	Verificado (Sem P.	
14	2017-04-11 14:37:20	1	Zezinho Tr.		Bio Inox Plus	Bio Inox Plus-1	Qualquer	Saida	Verificado (Sem P.	
15	2017-04-11 14:37:17	1	Zezinho Tr.		Bio Inox Plus	Bio Inox Plus-1	Qualquer	Saida	Verificado (Sem P.	
16	2017-04-11 14:36:00	1	Zezinho Tr.		Bio Inox Plus	Bio Inox Plus-1	Qualquer	Saida	Verificado (Sem P.	
17	2017-04-11 14:35:92	2	Tiazinha d.		Bio Inox Plus	Bio Inox Plus-1	Qualquer	Saida	Verificado (Sem P.	

Eventos última semana

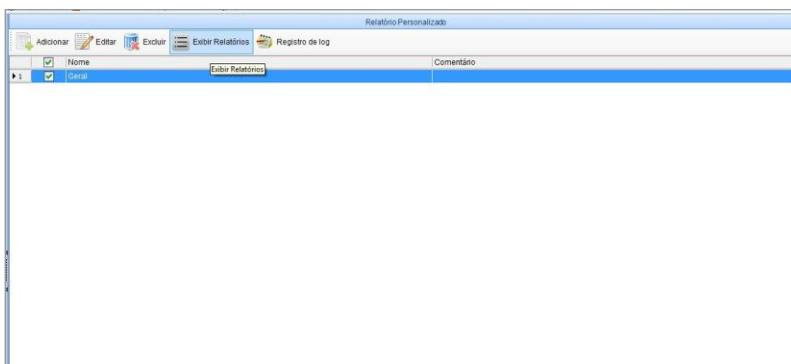


- » Na nova tela, selecione as informações que deverão estar contidas no seu relatório disponíveis na coluna da direita e, utilizando as setas de navegação centrais, passe-as para a coluna da esquerda. Digite um nome para o relatório criado e algum comentário que achar relevante. Por fim, clique no botão Ok para gerar o relatório personalizado.



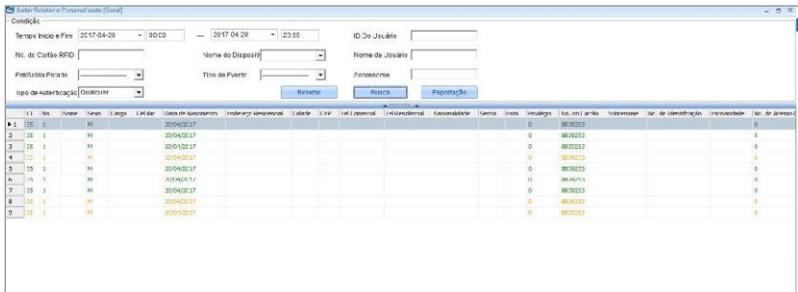
Adicionando informações ao relatório personalizado

1. Caso queira editar o relatório criado, selecione-o na lista de visualização da tela inicial e clique no botão Editar, faça as modificações e, em seguida, clique no botão Ok para confirmá-las;
2. Caso deseje excluir o relatório criado, selecione-o na lista de visualização da tela inicial e clique no botão Excluir, confirmando a operação posteriormente;
3. Para exibir o relatório criado, selecione-o na lista de visualização da tela inicial e clique no botão Exibir relatórios;



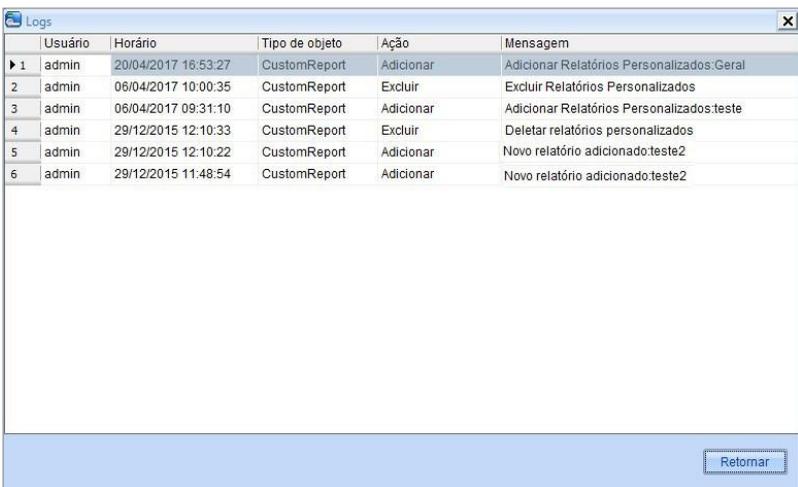
Exibir relatório personalizado

4. Na nova tela, faça as alterações necessárias e clique em Procurar para que os eventos sejam exibidos na tela;



Consultando eventos relatório personalizado

5. O botão Registro de logs exibe uma lista de alterações feitas pelo o operador do software SoapAdmin 3.5. Para voltar clique no botão Retornar.



Logs relatório personalizado

## 9. Sistema

Nesta seção, estão disponíveis as principais funções de configurações do software SoapAdmin 3.5., tais quais: Permissão de operador, Operador, Trocar senha de operador, Inicialização do sistema, Gerenciamento do banco de dados, Configurações do sistema, Navegação, Selecione idioma, Módulos opcionais e Sair. Estas funções estão disponíveis no botão Sistema localizado na barra de tarefas superior.



Funções da seção Sistema

### 9.1. Permissão de operador

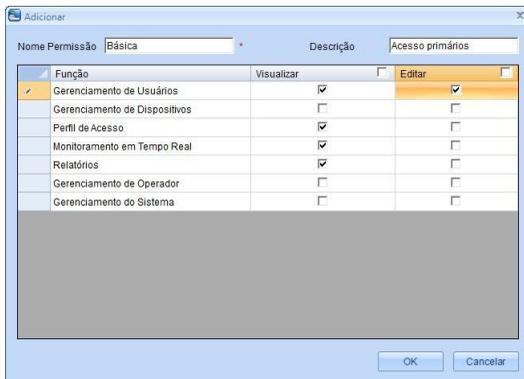
Nesta função é permitido criar níveis de permissão de acesso ao software SoapAdmin 3.5, diferentes do perfil do administrador, para um operador novo cadastrado.

1. Para acessá-la, clique no botão Permissão de operador e na sequência no botão Adicionar, para incluir uma permissão nova;



Adicionando nova permissão de operador

2. Na nova tela, digite o nome da nova permissão, sua descrição e selecione no quadro de Função as permissões que o perfil terá, bem como o nível definido para cada uma delas (visualização ou edição). Ao final clique no botão Ok para criar a nova permissão;



Setando nível de permissão para o operador

3. Caso queira editar ou excluir a nova permissão, clique nos botões Editar ou Excluir disponíveis na tela de visualização das permissões, após selecioná-las na lista.



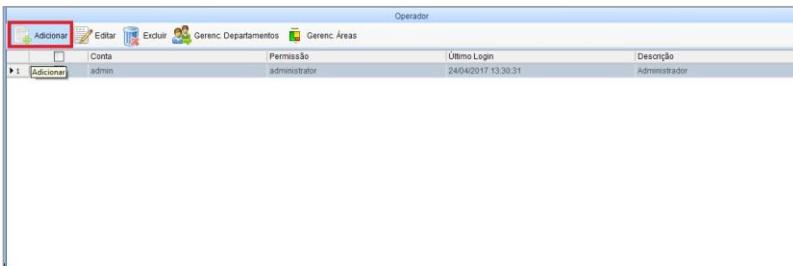
Editando ou excluindo permissão

**Importante:** a permissão de fábrica com o nome de administrador não pode ser excluída e nem editada, por ser uma permissão raiz do software.

## 9.2. Operador

Nesta função é possível criar novos cadastros de operadores que irão logar no software SoapAdmin 3.5.

1. Para criar um novo perfil, clique no botão Adicionar na tela inicial da função Operador;



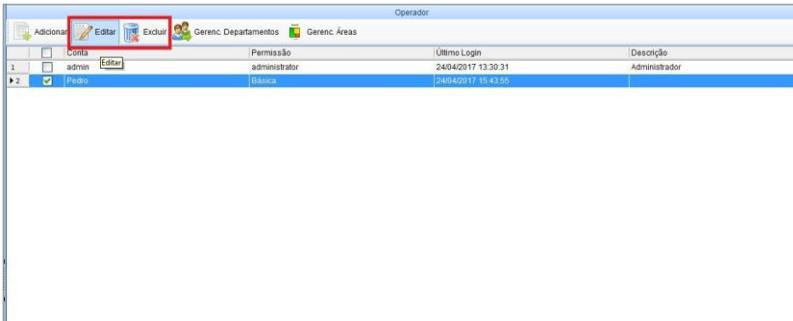
Adicionando novo operador

2. Na nova tela, entre com as informações necessárias do novo operador e vincule-o ao nível de permissão que ele deverá ter. No campo Status, marque Normal para ativá-lo ou Desabilitado para torná-lo inativo e confirme em Ok;

Nome	Pedro	*
Senha	*****	*
Conf. Senha	*****	*
Permissão	Básica	*
Descrição		
Status	<input checked="" type="radio"/> Normal <input type="radio"/> Desabilitado	
OK		Cancelar

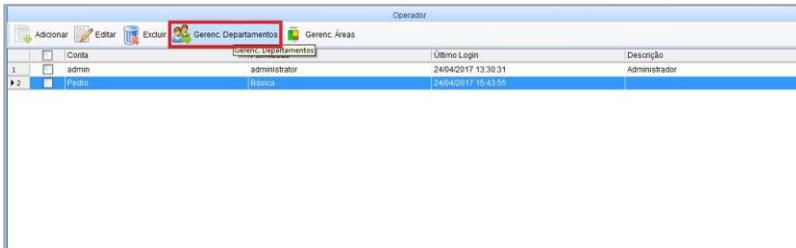
Criando novo operador

3. É possível editar ou excluir o operador criado, para isso, clique sobre os botões Editar ou Excluir após selecionar o perfil do operador na tela de visualização dos operadores existentes;



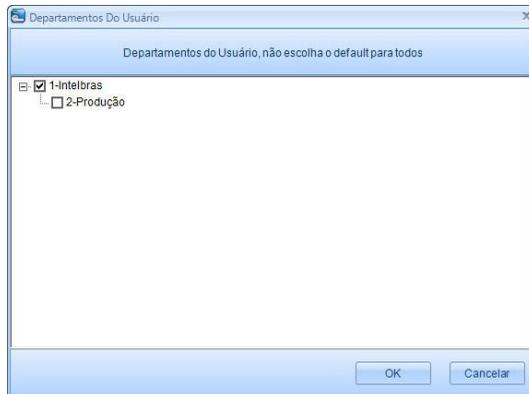
Editando ou excluindo operador

4. Na função Operador, também é possível vincular o operador criado a um dos departamentos que estão vinculados ao banco de dados dos usuários do sistema de controle de acesso. Para isso, clique no botão Gerenc. departamentos;



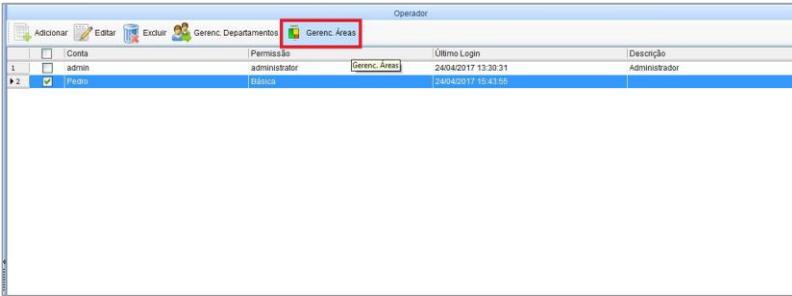
Verificando departamentos

5. Na nova tela selecione um dos departamentos existentes e clique em Ok para validar o vínculo;



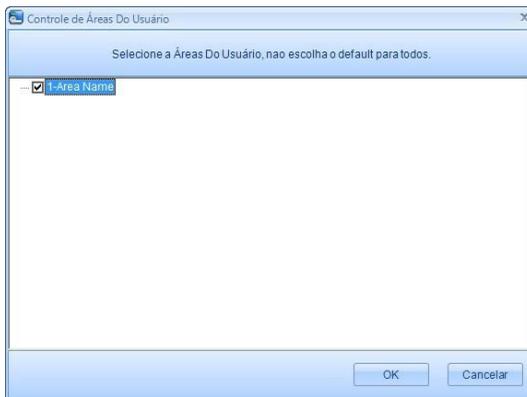
Vinculando departamentos

6. Da mesma forma, é possível vincular o perfil do operador criado para um perfil de área existente. Para isso, clique no botão Gerenc. áreas na tela inicial da função Operador;



Vinculando áreas

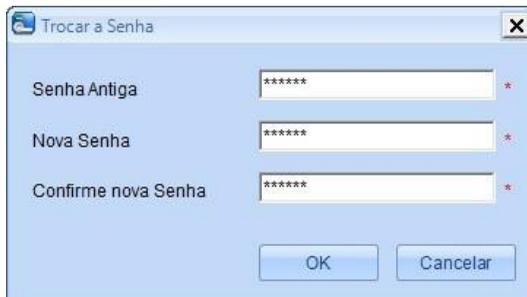
7. Na nova tela, selecione a área desejada e clique em Ok para confirmar o vínculo.



Selecionando área para vínculo de operador

### 9.3. Trocar senha de operador

Esta função possibilita alterar a senha de um perfil de operador criado anteriormente. Para isso, clique na guia Sistemas e no botão Trocar senha de operador. Na nova tela preencha a senha antiga e digite a nova senha, confirmando-a novamente no campo abaixo. Após isso, clique em Ok para validar a alteração.



Alterando a senha do operador

## 9.4. Gerenciamento do banco de dados

Esta função disponibiliza consultas e ajustes nos bancos de dados disponíveis no software SoapAdmin 3.5. Por padrão, o banco de dados do software é o banco Access, outras versões de banco não estão disponíveis para o software.

### Conexão com o banco de dados

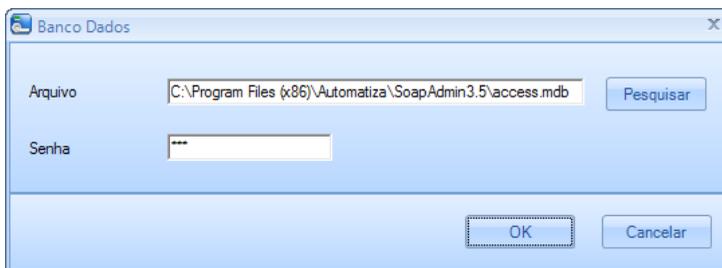
Nesta função, será possível setar qual o banco de dados será utilizado pelo software SoapAdmin 3.5 (Access) padrão. Após setar banco de dados clique em Prox para pular para a nova tela.



Conexão com o banco de dados

**Importante:** o campo Outras versões não estão disponíveis não deve ser marcado, pois não está habilitado no software.

Na nova tela, atribua uma senha e confirme o caminho em que o banco de dados será salvo, por fim, clique em Ok para confirmar e reinicialize o software.



Configurando a conexão com o banco de dados

### Backup do banco de dados

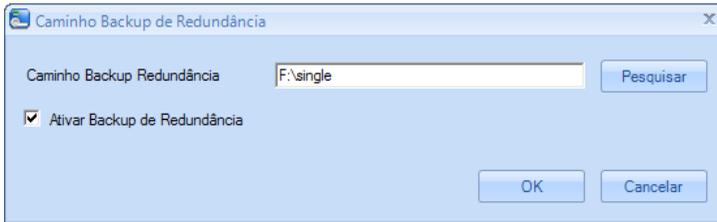
Esta função permite ao usuário definir o local onde será salvo o backup do banco de dados. Clique no botão Backup do banco de dados e em Salvar para confirmar.

### Restaurar banco de dados

Esta função permite ao operador restaurar o backup do banco de dados no local definido pelo item anterior. Clique no botão Restaurar banco de dados, selecione o arquivo no local definido acima, e clique em Abrir para puxar o backup mais recente.

### Caminho para backup de redundância

Esta função possibilita definir outro caminho para o backup do banco de dados, além da pasta padrão de fábrica. É necessário estipulá-la também no momento da instalação do sistema. Também é necessário marcar a opção Ativar backup de redundância. Clique em Ok para confirmar as configurações.

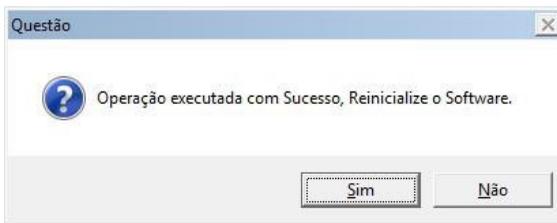


Ativando backup do banco de dados

**Importante:** o campo Ativar backup de redundância deve ser marcado para ativar o backup do banco de dados.

### Reparação banco de dados de acesso

Esta função possibilita resolver possíveis inconsistências apresentadas no banco de dados, de modo a garantir o funcionamento correto do sistema de controle de acesso. Para ativar a função, clique sobre o botão Reparação do banco de dados e, em seguida, em Sim para reiniciar o software.



Reparação do Banco de Dados

### Configuração máquina cliente

Processo utilizando o banco de dados padrão (Access)

1. Após instalar o software na máquina cliente, faça o login como Administrador e selecione a opção Gerenciamento do Banco de Dados e posteriormente Conexão ao Banco de Dados.



Conexão banco de dados na máquina cliente

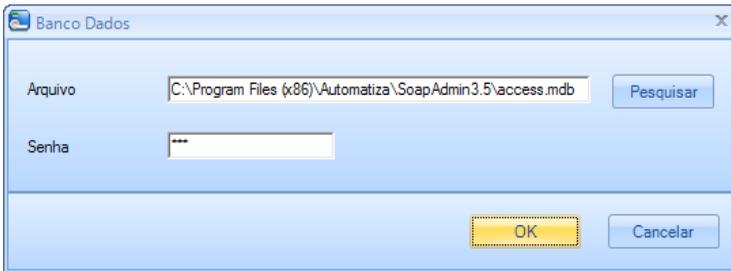
2. Na nova tela, clique em Próximo;



Definindo Tipo de Banco de Dados (Access)

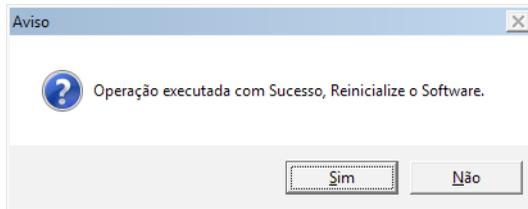
3. Na nova janela, insira o endereço onde está localizado o banco de dados da máquina servidor. O endereço padrão de instalação é: C:\Program Files (x86)\Automatiza\SoapAdmin3.5;

4. Mantenha os valores preenchidos no campo Senha e no final, clique no botão OK.



Endereçando o banco de dados do servidor

5. Verifique a informação de sucesso e reinicie o software.

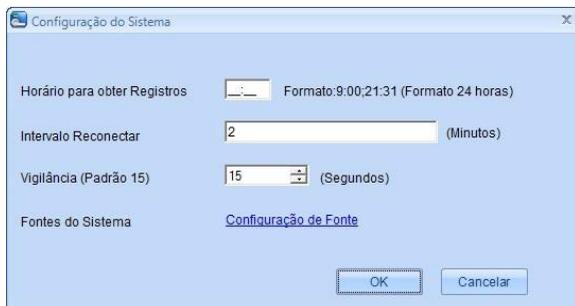


Confirmação de alteração de banco de dados

**Importante:** recomendamos que sejam configuradas até 03 máquinas na configuração Cliente e mais uma como Servidor. Esta configuração está homologada de fábrica e atende a grande parte dos casos de aplicação de mercado

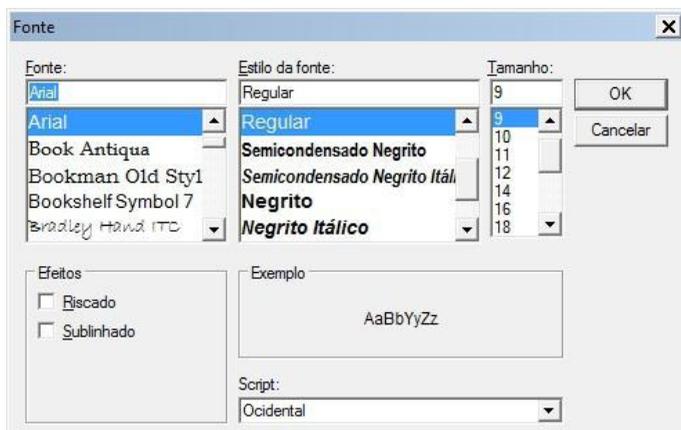
## 9.5. Configurações do sistema

Nesta função, é possível configurar o horário para conexão de registros de controle de acesso, bem como os intervalos para conexão dos sincronismos com os dispositivos do sistema, além das demais informações, como fontes do sistema. Ao fazer as configurações necessárias, clique em Ok para confirmar.



Configurações do sistema

É possível também alterar as fontes (tipo de letras) utilizadas no sistema. Clique em Configuração de fonte, selecione a fonte e o tamanho desejados e, por fim, clique em Ok para salvar as alterações.



Alteração da fonte do sistema

## 9.6. Navegação

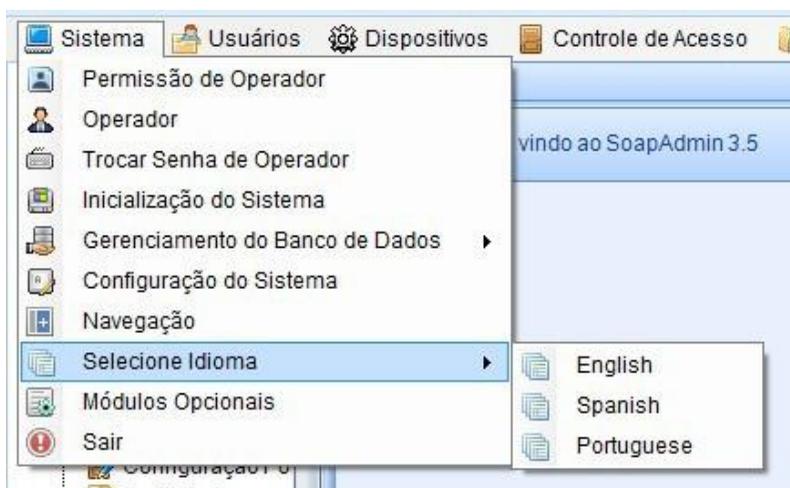
Este botão retorna à tela inicial de navegação do software. Clique no botão Navegação e a tela a seguir será exibida.



Tela de navegação

## 9.7. Seleção de idioma

Este botão permite alterar o idioma do software SoapAdmin 3.5 para as seguintes opções: English (inglês), Spanish (español) ou Portuguese (português). Após selecionar o idioma, será necessário reiniciar o software.



Seleção de idioma

## 9.8. Módulos opcionais

Este botão possibilita cadastrar uma chave de identificação e uma chave de registro que serão registradas e aparecerão nos relatórios de eventos de exceção através das configurações feitas na função Ações vinculadas a eventos. Após a configuração, clique no botão Registrar para confirmar as configurações.



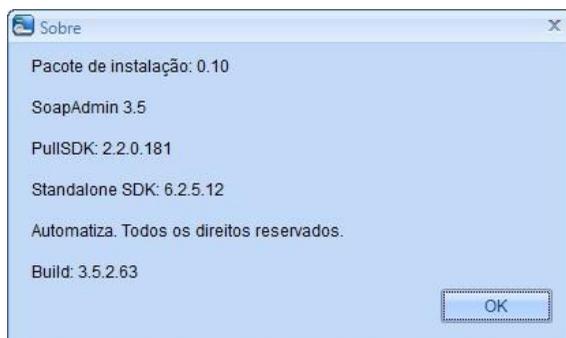
Registrando chaves para eventos de exceção

- Importante:** » Algumas considerações devem ser seguidas visando manter o sistema de controle de acesso funcional:
- » Utilize um nobreak com autonomia que permita o correto desligamento da máquina servidora em caso de queda de energia.
  - » Antes de sair do sistema, interrompa o monitoramento em tempo real, caso as telas de monitoramento ou planta baixa tenham sido utilizadas.
  - » Feche o software SoapAdmin 3.5 antes de desligar o computador.
  - » Não encerre o processo do aplicativo do SoapAdmin 3.5, utilizando o gerenciador de tarefas do Windows®.
  - » Configure o software SoapAdmin 3.5 para fazer backup do banco de dados, preferencialmente em uma pasta compartilhada armazenada em um outro computador.

## 10. Ajuda

---

Neste botão estão disponíveis para acesso via HTML este manual do usuário na íntegra e também as informações do pacote de instalação da versão instalada do software SoapAdmin 3.5. Para consultar o manual, clique no botão Ajuda. Para consultar as informações de versão do software, clique no botão Sobre.



Botão Sobre

# Política de privacidade

---

Esta é a Política de privacidade (“Política”) que é firmada entre você, de agora em diante denominado Usuário, e a Intelbras S/A - INDÚSTRIA de Telecomunicação Eletrônica Brasileira, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº 82.901.000/0001-27, estabelecida na rodovia BR 101, km 210, Área Industrial, São José/SC, representando, neste ato, todas as suas filiais, de agora em diante denominada INTELBRAS. Esta Política foi projetada para regular a coleta, o armazenamento, o uso e o compartilhamento de informações compartilhadas com a INTELBRAS. Ao aceitar esta Política, o Usuário reconhece que analisou e concordou com as condições descritas, a Intelbras não acessa, transfere, capta, nem realiza qualquer outro tipotratamento de dados pessoais a partir deste produto. de acordo com os termos desta Política, bem como manifesta ciência de que a Política pode ser modificada, a qualquer tempo, com todas as atualizações publicadas nesta página. Sendo usuário menor de idade ou incapaz em quaisquer aspectos, precisará da permissão de seus pais ou responsáveis, que também deverão concordar com a Política e suas condições.

Qualquer dúvida em relação à Política de Privacidade pode ser esclarecida nos contatos: E-mail: [privacidade@intelbras.com.br](mailto:privacidade@intelbras.com.br)

## 1. Coleta de informações

Ao utilizar o software disponibilizado pela INTELBRAS, fica o Usuário ciente de que a INTELBRAS não acessa, transfere, capta, nem realiza qualquer outro tipo tratamento de dados pessoais a partir deste produto, tais como nome, telefone, e-mail, endereço, conforme descrito nesta Política. As informações podem ser classificadas em dois tipos: pessoais e não pessoais.

Informações pessoais são dados que estão relacionados ao Usuário, e que permitem a sua identificação, incluindo, mas não se limitando ao nome, data de nascimento, endereço de contato, número de contato, endereço de e-mail e arquivos de conteúdo em vídeo que podem conter informações de identidade visual pessoal.

Informações não pessoais são dados que não estabelecem qualquer relação com um indivíduo específico, como ocupação, idioma, código de área, números de série do produto, URLs, comportamento do usuário, arquivos de conteúdo em vídeo que não contenham informações de identidade visual pessoais, etc.

## 2. Armazenamento de informações pessoais

Conforme estipulado na Política, a INTELBRAS Intelbras não acessa, transfere, capta, nem realiza qualquer outro tipo de tratamento de dados pessoais a partir deste produto, e também realizará uma revisão periódica da eficácia dos atuais métodos de armazenamento e tratamento, incluindo precauções de segurança física, para evitar o acesso não autorizado.

A INTELBRAS possui as melhores práticas, incluindo tecnologias e estratégias razoáveis para a proteção dos dados, mas a INTELBRAS não pode garantir que suas informações pessoais estejam sob segurança absoluta, tendo em vista a tecnologia de segurança da informação existente. O Usuário reconhece que a INTELBRAS não se responsabiliza por quaisquer perdas no caso de suas informações pessoais serem reveladas, furtadas ou roubadas por motivo de força maior ou problemas de segurança que não tenham sido causados pela INTELBRAS.

## 3. Uso de informações pessoais

A fim de proporcionar uma melhor experiência ao usuário, a INTELBRAS poderá usar suas informações pessoais para os seguintes propósitos:

- » Viabilizar o uso do software com todas as suas soluções e funcionalidades, armazenando o histórico necessário para o seu funcionamento e melhor experiência do Usuário.
- » Aumentar a segurança do aplicativo e de outros serviços prestados pela INTELBRAS, tais como autenticação de usuários, proteção de segurança, detecção de fraudes, arquivamento e backups.
- » A menos que o Usuário opte por cancelar a inscrição, a INTELBRAS poderá contatá-lo enviando comunicações eletrônicas para informar sobre novos produtos e serviços. A INTELBRAS também poderá utilizar informações pessoais para fins internos, tais como auditorias, análise de dados e pesquisas.

## 4. Compartilhamento de informações pessoais

A INTELBRAS não divulgará suas informações pessoais, a menos que (i) tenha seu consentimento prévio por escrito; (ii) esteja de acordo com as leis e regulamentos aplicáveis ou exigidos pelas autoridades; (iii) seja obrigada por decisão judicial; (iv) esteja de acordo com os termos da Política; (v) seja essencial para a proteção dos interesses legítimos da INTELBRAS.

A INTELBRAS poderá permitir que seus funcionários acessem os dados em ocasiões específicas com base na necessidade de conhecimento, e assegurará que cumpram

com as obrigações no mesmo nível estabelecido pela Política.

Além disso, a INTELBRAS pode disponibilizar certas informações não pessoais a parceiros estratégicos confiáveis que ocasionalmente trabalham com a INTELBRAS para proporcionar uma melhor experiência ao Usuário e aumentar a qualidade dos serviços do software. Sob essas circunstâncias, a aceitação da Política significa que o Usuário concorda e autoriza a INTELBRAS a fornecer suas informações a tais terceiros.

## 5. Atualizações na Política de Privacidade

Esta Política passa por constantes atualizações, assim, a INTELBRAS recomenda rever periodicamente esta página para acompanhar e estar ciente das modificações. Caso sejam feitas alterações relevantes nos termos desta Política, a INTELBRAS publicará nova Política, notificando o Usuário.

Se você suspeitar de que suas informações pessoais estejam sendo coletadas ou utilizadas de maneira ilegal, ou que qualquer regra desta Política esteja sendo infringida de qualquer maneira, entre em contato com a INTELBRAS, imediatamente, através do site [www.intelbras.com.br](http://www.intelbras.com.br) ou e-mail [privacidade@intelbras.com.br](mailto:privacidade@intelbras.com.br).

# Termos de uso de software

---

## 1. Aceitação do contrato

Este é um contrato firmado entre você, de agora em diante denominado de USUÁRIO, e a Intelbras S/A - Indústria de Telecomunicação Eletrônica Brasileira, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o n.º 82.901.000/0001-27, estabelecida na rodovia BR 101, km 210, Área Industrial, São José/SC, e de agora em diante denominada simplesmente de Intelbras. Estes Termos de uso de serviço regem o uso do serviço disponibilizado gratuitamente pela Intelbras e/ou seus parceiros, denominado INTELBRAS INCONTROL WEB, desenvolvido para computadores em LAN. Se você não concordar com estes termos não use esse serviço. Leia-as atentamente, pois, se você começou a usar esse serviço, ficará configurado que aceitou todos os termos e concorda em cumpri-los. Se você, usuário, for menor de idade ou declarado incapaz em quaisquer aspectos, precisará da permissão de seus pais ou responsáveis, que também deverão concordar com estes mesmos termos e condições.

## 2. Licença limitada

Você recebeu uma licença limitada, não transferível, não exclusiva, livre de royalties e revogável, para baixar, instalar, executar e utilizar esse serviço em seu dispositivo. Você reconhece e concorda que a Intelbras concede ao usuário uma licença exclusiva para uso e, dessa forma, não lhe transfere os direitos sobre o produto. O serviço de-verá ser utilizado por você, usuário. A venda, transferência, modificação, engenharia reversa ou distribuição, bem como a cópia de textos, imagens ou quaisquer itens contidos no software são expressamente proibidas. Você reconhece que a Intelbras é proprietária de todos os direitos, títulos e interesses referentes ao INTELBRAS IN- CONTROL WEB e ao software relacionado. INTELBRAS INCONTROL WEB é a marca comercial ou registrada da Intelbras. Você não pode alterar, destruir, ocultar ou remover de outra forma qualquer as informações sobre direito autoral, os rótulos ou avisos de propriedade dos softwares da Intelbras.

## 3. Do Cadastro

Para a acesso ao software é necessário que o USUÁRIO realize um cadastro prévio onde forneça voluntariamente informações sobre si, tais como: USUÁRIO, senha, endereço de e-mail (Dados). O USUÁRIO declara que os Dados fornecidos são fiéis e verdadeiros e compromete-se a manter seus dados sempre atualizados.

INTELBRAS não é responsável pelas informações prestadas, a Intelbras não acessa, transfere, capta, nem realiza qualquer outro tipo tratamento de dados pessoais a partir deste produto.

O titular e administrador da conta será aquele definido no momento do cadastro, a partir dos Dados oferecidos pelo USUÁRIO. A conta é pessoal e poderá ser acessada unicamente mediante a utilização do USUÁRIO e senha criados pelo próprio USUÁRIO no momento do cadastro, sendo este o único e exclusivo responsável por manter o sigilo de seu USUÁRIO e senha, a fim de garantir a segurança de sua conta e impedir o acesso não autorizado por terceiros. O USUÁRIO é o único responsável por todas as atividades associadas a sua conta.

O USUÁRIO deverá seguir os padrões de segurança de registro de senha e realizar a troca imediata da senha padrão.

#### 4. Direitos autorais

O USUÁRIO não adquire, pelo presente instrumento ou pela utilização do SOFTWARE, nenhum direito de propriedade intelectual ou outros direitos exclusivos, incluindo patentes, desenhos, marcas, direitos autorais ou quaisquer direitos sobre informações confidenciais ou segredos de negócio, bem como sobre o conteúdo disponibilizado no software, incluindo, mas não se limitando a textos, gráficos, imagens, logotipos, ícones, fotografias, conteúdo editorial, notificações, softwares e qualquer outro material, sobre a INTELBRAS ou relacionados a ele ou a qualquer parte dele. O USUÁRIO também não adquire nenhum direito sobre o SOFTWARE ou relacionado a ele ou a qualquer componente dele, além dos direitos expressamente licenciados ao USUÁRIO neste Termo ou em qualquer outro contrato mutuamente acordado por escrito entre as partes.

Ao utilizar o SOFTWARE, o USUÁRIO concorda em cumprir com as seguintes diretrizes:

- I. Não é permitido postar ou transmitir informação, dado, texto, software, gráficos, sons, fotografias, vídeos, mensagens ou outro conteúdo que seja ilegal, ofensivo, impreciso, difamatório, obsceno, fraudulento, prejudicial, ameaçador ou abusivo.
- II. Não interferir no uso de outros usuários do SOFTWARE.
- III. Não postar ou fazer upload de qualquer vírus, worms, arquivo corrompido ou outro software capaz de perturbar, incapacitar ou prejudicar o funcionamento do SOFTWARE.
- IV. Cumprir com este Termo e quaisquer leis ou regulamentos aplicáveis;
- V. Não se passar por qualquer pessoa ou entidade, declarar falsamente ou deturpar sua afiliação com uma pessoa ou entidade.
- VI. Não enviar ou transmitir conteúdo que o USUÁRIO não tem o direito de pu-

blicar ou transmitir sob qualquer lei ou sob relações contratuais ou fiduciárias (tais como informação privilegiada, informações confidenciais, etc).

VII. Não usar o SOFTWARE para solicitar, obter ou armazenar dados pessoais ou senhas de outros usuários.

## 5. Alterações, modificações e rescisão

A Intelbras reserva-se o direito de, a qualquer tempo, modificar estes termos, seja incluindo, removendo ou alterando quaisquer de suas cláusulas. Tais modificações terão efeito imediato após a publicação. Ao continuar com o uso do serviço você terá aceitado e concordado em cumprir os termos modificados. Assim como, a Intel-bras pode, de tempos em tempos, modificar ou descontinuar (temporária ou permanentemente) a distribuição ou a atualização desse serviço. O USUÁRIO não poderá responsabilizar a Intelbras nem seus diretores, executivos, funcionários, afiliados, agentes, contratados ou licenciadores por quaisquer modificações, suspensões ou descontinuidade do serviço.

Para fins contratuais, o USUÁRIO concorda em receber comunicações da INTELBRAS de forma eletrônica (termos e condições, acordos, notificações, divulgações e outras comunicações da INTELBRAS), seja por e-mail ou comunicação interna no próprio SOFTWARE e que, desta forma estabelecida, as comunicações da INTELBRAS satisfazem e cumprem com os requisitos legais, como se fosse em via impressa.

## 6. Indenização

Em nenhum caso a INTELBRAS será responsável por danos pessoais ou qualquer prejuízo incidental, especial, indireto ou consequente, incluindo, sem limitação, prejuízos por perda de lucro, corrupção ou perda de dados, falha de transmissão ou recepção de dados, não continuidade do negócio ou qualquer outro prejuízo ou perda comercial, decorrentes ou relacionados ao uso do SOFTWARE ou a sua incapacidade em usar o SOFTWARE, por qualquer motivo.

## 7. Consentimento para coleta e proteção do uso de dados

O USUÁRIO concorda que a INTELBRAS pode coletar os dados pessoais de cadastro e perfil, e usar dados técnicos de seu dispositivo, tais como especificações, configurações, versões de sistema operacional, tipo de conexão à internet e afins.

Os dados pessoais coletados do USUÁRIO serão exclusivamente utilizados para fins de execução do presente contrato, com o objetivo principal de ativação das funcionalidades do SOFTWARE, sendo que o uso destes dados é intrínseco ao próprio funcionamento do SOFTWARE, e para uso e benefícios do titular. Ainda, alguns recursos do

SOFTWARE poderão solicitar dados adicionais do USUÁRIO, tais como, nome, telefone, endereço, funcionários, instaladores, serviços prestados, região de atendimento, treinamentos realizados, clientes atendidos, e todos outros dados vinculados à sua atividade comercial. O aceite do USUÁRIO ao presente Contrato desde já autoriza a INTELBRAS a indicar o USUÁRIO como parceiro da INTELBRAS e publicar os dados públicos de contato nos sites, softwares e demais mídias sociais da INTELBRAS, de acordo com a previsão do Manual do Programa de Canais e demais políticas definidas pela INTELBRAS e compartilhadas previamente com o USUÁRIO.

No desenvolvimento de quaisquer atividades relacionadas com a execução do presente Contrato, as Partes observam o regime legal de proteção de dados pessoais, empenhando-se em proceder a todo o tratamento de dados pessoais que venha a mostrar-se necessário ao desenvolvimento do Contrato no estrito e rigoroso cumprimento da Lei.

Os dados pessoais aqui elencados consideram-se os dados das próprias Partes ou mesmo os dados pessoais de seus colaboradores, contratados ou subcontratados.

A fim de garantir a proteção dos dados, o USUÁRIO obriga-se a:

- a. Tratar e usar os dados pessoais da INTELBRAS ou de seus PARCEIROS nos termos legalmente permitidos, em especial recolhendo, registrando, organizando, conservando, consultando ou transmitindo os mesmos, apenas e somente nos casos em que seu titular tenha dado o consentimento expresso e inequívoco, ou nos casos legalmente previstos;
- b. Tratar os dados de modo compatível com as finalidades para os quais tenha sido recolhidos;
- c. Conservar os dados apenas durante o período necessário à prossecução das finalidades da recolha ou do tratamento posterior, garantindo a sua confidencialidade;
- d. Implementar as medidas técnicas e organizativas necessárias para proteger os dados contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizada, bem como contra qualquer outra forma de tratamento ilícito dos mesmos;
- e. Informar imediatamente a INTELBRAS, devendo prestar toda a colaboração necessária a qualquer investigação que venha a ser realizada, caso exista alguma quebra de segurança, ou suspeita da mesma, independentemente de

colocar ou não em causa a segurança e integridade dos dados pessoais;

f. Garantir o exercício, pelos titulares, dos respectivos direitos de informação, acesso e oposição;

g. Assegurar que os seus colaboradores, contratados ou subcontratados que venham a ter acesso a dados pessoais no contexto deste Contrato cumpram as disposições legais aplicáveis em matéria de proteção de dados pessoais, e as disposições contratuais aqui elencadas, não cedendo, vendendo, compartilhando ou divulgados tais dados a terceiros, nem deles fazendo uso para quaisquer fins que não os estritamente consentidos pelos respectivos titulares.

O USUÁRIO será responsabilizado perante a INTELBRAS ou terceiros em caso de qualquer violação, compartilhamento, exclusão, cessão, venda, alteração automática dos dados sem prévio e expreso consentimento do seu titular.

## **8. Marcas Registradas e Direitos de Propriedade Intelectual da Intelbras**

O USUÁRIO reconhece que as Marcas Registradas e os Direitos de Propriedade Intelectual da INTELBRAS representam um dos ativos estratégicos da INTELBRAS sendo de exclusiva propriedade da mesma.

Durante a vigência deste Termo, será concedido ao USUÁRIO o direito de uso não exclusivo das Marcas Registradas e outros Direitos de Propriedade Intelectual da INTELBRAS, sendo que o USUÁRIO deverá utilizá-los estritamente de acordo como (i) “Manual da Marca Intelbras”; e (ii) quaisquer outras instruções recebidas da INTELBRAS. O LICENCIADO também garante que suas atividades de propaganda e promocionais cumpram com o (i) Manual da Marca Intelbras; (ii) Programa de Canais Intelbras; e (iii) e a legislação aplicável.

O USUÁRIO não poderá registrar quaisquer Direitos de Propriedade Intelectual da INTELBRAS, tais como qualquer palavra, símbolo, marca identificativa ou nome semelhante às Marcas Registradas da INTELBRAS ou nome de domínio durante a vigência deste contrato ou mesmo após o seu encerramento.

Todo e qualquer direito do USUÁRIO de utilizar as Marcas Registradas e outros Direitos de Propriedade Intelectual da INTELBRAS cessará automaticamente quando do encerramento do presente termo.

O USUÁRIO deverá prontamente notificar a INTELBRAS, por escrito, de qualquer suspeita de uso não autorizado ou infração aos Direitos de Propriedade Intelectu-

al da INTELBRAS e que venha a ter conhecimento. Se solicitado pela INTELBRAS, o USUÁRIO deverá auxiliar a INTELBRAS em quaisquer investigações, negociações ou procedimentos judiciais em virtude de qualquer alegação de uso indevido ou de violação aos Direitos de Propriedade Intelectual da INTELBRAS.

O USUÁRIO compromete-se a não fazer qualquer tipo de anúncio, propaganda, material publicitário dos Produtos Intelbras, contemplando preços e condições de pagamento vinculando produtos INTELBRAS com produtos de concorrentes, devendo tais propagandas serem feitas de forma separada, sem vinculação de qualquer produto concorrente. A INTELBRAS recomenda que o USUÁRIO não faça mala direta constando preços dos produtos.

É vedada a cópia ou qualquer outra forma de reprodução das informações, manuais, literatura técnica e outros documentos fornecidos pela INTELBRAS, exceto para o cumprimento de obrigações estabelecidas nos termos deste instrumento, e de acordo com a legislação aplicável relativamente a direitos autorais e propriedade intelectual.

As obrigações estabelecidas na presente cláusula obrigam o USUÁRIO durante a vigência do presente instrumento, bem como após seu encerramento ou rescisão manutenção da confidencialidade.

## 9. Isenção de garantias e limitações de responsabilidade

Esse serviço estará em contínuo desenvolvimento e pode conter erros, por isso, o uso é fornecido no estado em que se encontra e sob risco do usuário final. Na extensão máxima permitida pela legislação aplicável, a INTELBRAS e seus fornecedores isentam-se de quaisquer garantias e condições expressas ou implícitas incluindo, sem limitação, garantias de comercialização, adequação a um propósito específico, titularidade e não violação no que diz respeito ao serviço e a qualquer um de seus componentes ou ainda à prestação ou não de serviços de suporte. A INTELBRAS não garante que a operação desse serviço seja contínua e sem defeitos. Com exceção do estabelecido neste documento, não há outras garantias, condições ou promessas vinculadas ao serviço, expressas ou implícitas, e todas essas garantias, condições e promessas podem ser excluídas de acordo com o que é permitido por lei sem prejuízo à Intelbras e a seus colaboradores.

I. A INTELBRAS não garante, declara ou assegura que o uso desse serviço será ininterrupto ou livre de erros e você concorda que a Intelbras poderá remover por períodos indefinidos ou cancelar esse serviço a qualquer momento sem que você seja avisado.

II. A INTELBRAS não garante, declara nem assegura que esse serviço esteja

livre de perda, interrupção, ataque, vírus, interferência, pirataria ou outra ameaça à segurança e isenta-se de qualquer responsabilidade em relação a essas questões. Você é responsável pelo backup dos arquivos armazenados em seu dispositivo.

III. Em hipótese alguma a INTELBRAS, bem como seus diretores, executivos, funcionários, afiliadas, agentes, contratados ou licenciadores responsabilizar-se-ão por perdas ou danos causados pelo uso do serviço.

#### **10. Validade técnica**

Fica estipulado que a INTELBRAS, seus fornecedores ou distribuidores não oferecem um período de validade técnica do SOFTWARE. Não se pode considerar que o programa esteja isento de erros, que seu funcionamento seja ininterrupto ou que suas funções satisfaçam os requisitos dos usuários, razão pela qual fica expressamente estipulado que o licenciado o utiliza por sua conta e risco. Devido à complexidade da relação entre software e hardware, a INTELBRAS não garante que o SOFTWARE INTELBRAS INCONTROL WEB será compatível com todos os sistemas de software e hardware, que irá operar corretamente ou atender às suas expectativas.

#### **11. Foro para dirimir controvérsias**

Estes Termos de uso serão regidos e interpretados de acordo com as leis do Brasil. As partes se submetem à jurisdição exclusiva dos tribunais do Brasil. Para dirimir eventuais dúvidas acerca do presente instrumento, bem como de qualquer evento relacionado à utilização de nossos serviços, fica desde logo eleito o foro da comarca de São José, estado de Santa Catarina, por mais privilegiado que outro foro seja. Se você ainda possui alguma dúvida sobre a forma de utilização de nosso produto, sobre nossos Termos de uso ou sobre nossa Política de privacidade, entre em contato com a Intelbras. Ficaremos felizes com o seu contato.

# Automatiza

Uma marca do Grupo Intelbras

---



*fale com a gente*

**Suporte a clientes:** (48) 2106 0071

**Contato:** [suporte@intelbras.com.br](mailto:suporte@intelbras.com.br)

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.automatiza.com.br](http://www.automatiza.com.br)

04.21

Origem: China