

Control iD

iDAccess

Controlador de Acesso Multifuncional

Apostila de treinamento



Esta apostila é fornecida da forma como está e as informações nela contidas estão sujeitas a mudanças sem aviso prévio. As imagens nesta apostila são unicamente para efeito ilustrativo.

Reprodução, adaptação, ou tradução, parcial ou total, desse manual são proibidas sem permissão expressa por escrito da Control iD.

© 2015 Control iD

Revisão	Data	Alterações
A	13/02/2015	Revisão inicial

Índice

1. Introdução	4
2. Instalação	5
2.1. Instalação da fonte.....	5
2.2. Instalação de acessórios.....	7
2.3. Instalação de leitor de proximidade.....	8
3. Modos de operação	9
4. Configurações iniciais.....	10
4.2. Rede.....	10
4.3. Acessando a interface web	11
4.4. Configuração dos relés	13
4.5. Equipamentos em modo centralizado	17
5. Gerenciamento de acesso.....	19
5.1. Horários.....	19
5.2. Departamentos	21
6. Relatórios	24
6.1. Relatório padrão.....	24
6.2. Relatório customizado	24
7. Sincronização de dados.....	29
7.1. Exportação.....	29
7.2. Importação	30

1. Introdução

Esta apostila de treinamento visa capacitar o usuário quanto à instalação e configuração dos produtos da linha iDAccess. Primeiro, analisaremos como instalar os diferentes tipos de fechaduras, botoeiras e sensores de porta no iDAccess. Em seguida, veremos uma visão geral dos dois modos de funcionamento do iDAccess: stand-alone e integrado, mostrando como é possível configurar o equipamento para operar nos dois modos. Em seguida, será mostrado como realizar as configurações preliminares que habilitarão o usuário final a utilizar a solução: cadastro de usuários e administradores, cadastro de departamentos e configurações de regras de acesso. Além de uma visão geral de como gerar relatórios simples.

Este material visa ser um guia de utilização rápida e não contém informações detalhadas sobre o produto. Estas devem ser obtidas no Manual de Usuário através do site da Control iD.

2. Instalação

2.1. Instalação da fonte

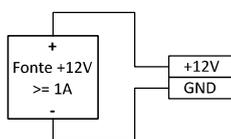
Antes de instalar o iDAccess na parede devemos instalar uma fonte de 12V/1A ou com capacidade superior de corrente (2A, 3A, etc.). A fonte deve ser instalada de preferência no forro, próxima ao equipamento.



**Cada equipamento deve estar ligado à sua própria fonte de alimentação.
A tensão da fonte NÃO deve ser superior a 12V.**

Faça as conexões da fonte de alimentação como se segue:

- 1) Ligue o cabo de alimentação na entrada da fonte.
- 2) Ligue o conector de duas vias do iDAccess na saída da fonte.



2.2. Instalação da fechadura

O iDAccess pode ser conectado aos três tipos mais comuns de fechaduras: eletroímã, strike ou eletromecânica e pino-solenoide. Cada fechadura possui suas próprias características que a tornam melhores ou piores para tipos diferentes de instalações e portas.

Eletroímã

A fechadura de eletroímã, *Magnetic Lock* em inglês, ou ainda fecho eletromagnético consiste em uma bobina (parte fixa) e uma peça metálica (atraque) que é presa à porta (parte móvel). Enquanto houver passagem de corrente pelo eletroímã a parte fixa irá atrair a parte móvel. Quando a distância entre estas duas partes for pequena, ou seja, quando a porta estiver fechada e o atraque sobreposto à parte fixa, a força de atração entre as partes pode superar 1000kg.

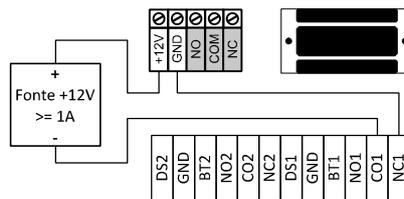
Assim, a fechadura de eletroímã é normalmente ligada ao contato NC do relé de acionamento, pois normalmente esperamos que passe corrente pelo eletroímã e, caso desejemos que a porta seja aberta, o relé deve abrir e interromper o fluxo de corrente.



Fechaduras de eletroímã não funcionam sem energia. Então, para instalações que requerem que a porta não seja aberta, em caso de falta de energia, é necessário o uso de nobreak.

Ligação da fechadura eletroímã

Para ligar a fechadura de eletroímã basta seguir o diagrama abaixo:



Eletromecânica

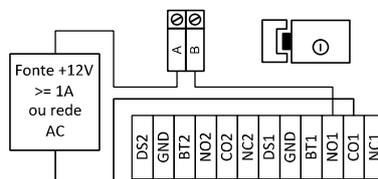
A fechadura eletromecânica ou strike consiste em uma lingueta ligada a um solenoide por meio de um mecanismo simples. Após a abertura da porta, o mecanismo volta ao estado inicial permitindo o fechamento da porta. Assim, a fechadura eletromecânica tem normalmente dois contatos ligados diretamente ao solenoide. Ao passar corrente pela fechadura, a porte será destravada.



Antes de ligar uma fechadura eletromecânica verifique a tensão de operação. É preciso ajustar a fonte para operar com 110V ou 220V dependendo da tensão de operação da fechadura.

Ligação da fechadura eletromecânica

Para ligar a fechadura eletromecânica primeiro ajuste sua fonte à tensão de 110V ou 220V dependendo do tipo de fechadura utilizada. Então, siga o procedimento abaixo:



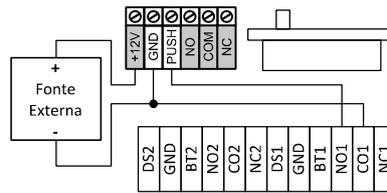
Pino-solenoide

A fechadura do tipo pino-solenoide, também conhecida como solenoide, consiste em uma parte fixa que possui um pino móvel ligado a um solenoide. A fechadura normalmente acompanha uma chapa metálica que deve ser presa à porta (parte móvel). O pino da parte fixa entra na chapa metálica impedindo a abertura da porta.

Em geral, as fechaduras deste tipo necessitam ser alimentadas pela fonte de alimentação do equipamento.

Ligação da fechadura pino-solenóide

Para ligar a fechadura de pino-solenóide basta seguir o diagrama abaixo:

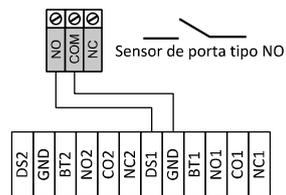


Atente para o fato de que a fechadura é ligada junto à fonte do equipamento.

2.2. Instalação de acessórios

Sensor de porta

Os sensores de porta detectam se a porta está ou não aberta. Normalmente eles são vendidos junto com as fechaduras, mas podem ser encontrados separadamente. A ligação de sensores de porta ligados a fechaduras é bem simples e segue o diagrama a seguir:

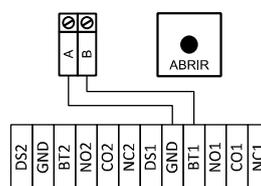


A figura acima mostra a ligação de um sensor de porta do tipo NO. Para um sensor de porta do tipo NC basta, ao invés de ligar o pino NO ao pino DS1, ligarmos o pino NC ao pino DS1.

Botoeira

As botoeiras permitem que a porta seja aberta sem a necessidade de identificação no iDAccess. Normalmente são utilizadas em saídas, para que o usuário não precise se identificar duas vezes.

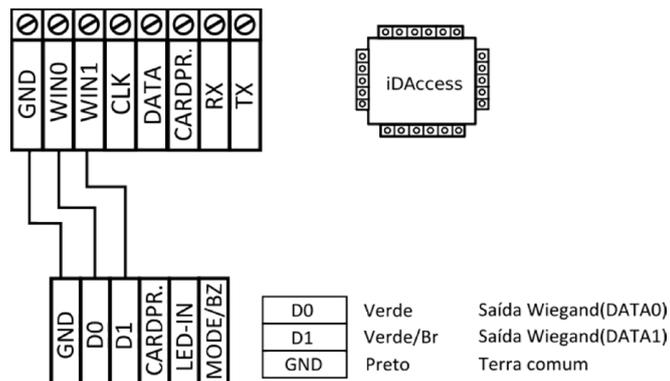
A ligação da botoeira segue o diagrama abaixo:



2.3. Instalação de leitor de proximidade

O protocolo Wiegand utiliza-se de três fios: GND, DATA0 e DATA1. Os dados são transmitidos através dos fios DATA0 e DATA1. Quando não existem dados sendo transmitidos ambos os fios encontram-se em nível lógico 1, fazendo com que a tensão entre um destes fios e GND seja 5V. O DATA0 é utilizado para transmitir o nível lógico 0 e quando esta transmissão ocorrer iremos medir 0V entre DATA0 e GND. Analogamente, o DATA1 é utilizado para transmitirmos o nível lógico 1 e quando isto ocorrer teremos 0V entre DATA1 e GND.

Abaixo temos as ligações necessárias para utilizar este protocolo:



3. Modos de operação

O iDAccess pode ser utilizado de dois modos diferentes: modo stand-alone e modo centralizado. A opção entre um modo de operação e outro só pode ser configurada por meio de um arquivo de licença específico adquirido separadamente. No modo stand-alone todas as operações de cadastro e identificação são realizadas pelo próprio equipamento. Neste modo o equipamento suporta o cadastro de até 2.000 digitais e pode controlar até duas portas simultaneamente. Esta solução é ideal quando o equipamento precisa controlar apenas uma ou duas portas e o número de usuários é relativamente pequeno. Para situações em que há a necessidade de controlar mais de duas portas, ou onde haja muitos usuários a serem cadastrados no sistema, é recomendado utilizar a solução centralizada. Neste modo de operação um ou mais iDAccess são conectados a outro iDAccess, ou a um iDBox, designado previamente como *servidor*. As operações de cadastro e identificação são processadas no servidor e o equipamento se restringe a enviar tentativas de identificação para o servidor e receber sinais para abrir a porta. A conexão entre o equipamento e o servidor é feita, de forma criptografada, via TCP/IP. Basta que o servidor e o iDAccess estejam ligados à mesma rede e que o equipamento esteja relacionado no servidor.

Todas as operações descritas nessa apostila são aplicáveis para os dois modos de operação, com a única diferença que no modo stand-alone as operações são feitas no próprio equipamento e no modo centralizado as operações são feitas no servidor.

4. Configurações iniciais

Tendo o equipamento instalado e funcionando vamos configurar o equipamento para que possamos começar a utilizar todas as funcionalidades que ele oferece: identificação de usuários, regras de acesso, configurador web, etc.

4.1. Rede

A primeira configuração que precisamos fazer é a de rede. O equipamento precisa ter um IP fixo definido para que possamos acessar a interface web. Esta configuração se aplica tanto a equipamentos no modo stand-alone quanto a equipamentos no modo centralizado.

É estritamente necessário mudar os endereços IP de todos os equipamentos, uma vez que todos vêm com IP padrão 192.168.0.129, o que causará conflito de IP na rede.



Antes de definir o IP do equipamento certifique-se de que este endereço não está sendo usado por nenhuma outra máquina.

Para mudar as configurações de rede siga os passos abaixo:

- 1) Acesse o menu principal do equipamento pressionando [MENU] na tela principal.



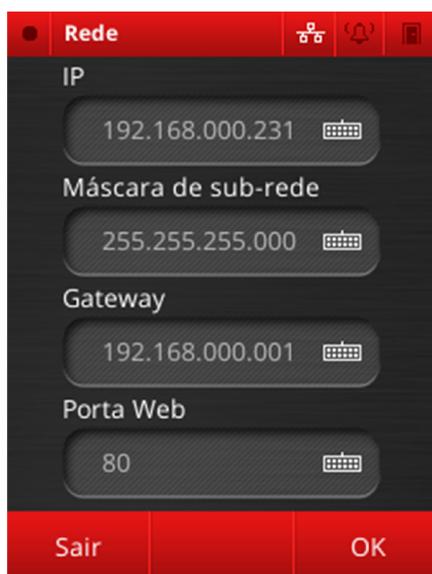
- 2) No menu principal, pressione [CONFIGURAÇÕES].



- 3) No menu de configurações pressione [REDE].



- 4) Na tela de rede configure o IP do equipamento, a máscara de sub-rede, o gateway e a porta TCP utilizada pela interface web.



4.2. Acessando a interface web

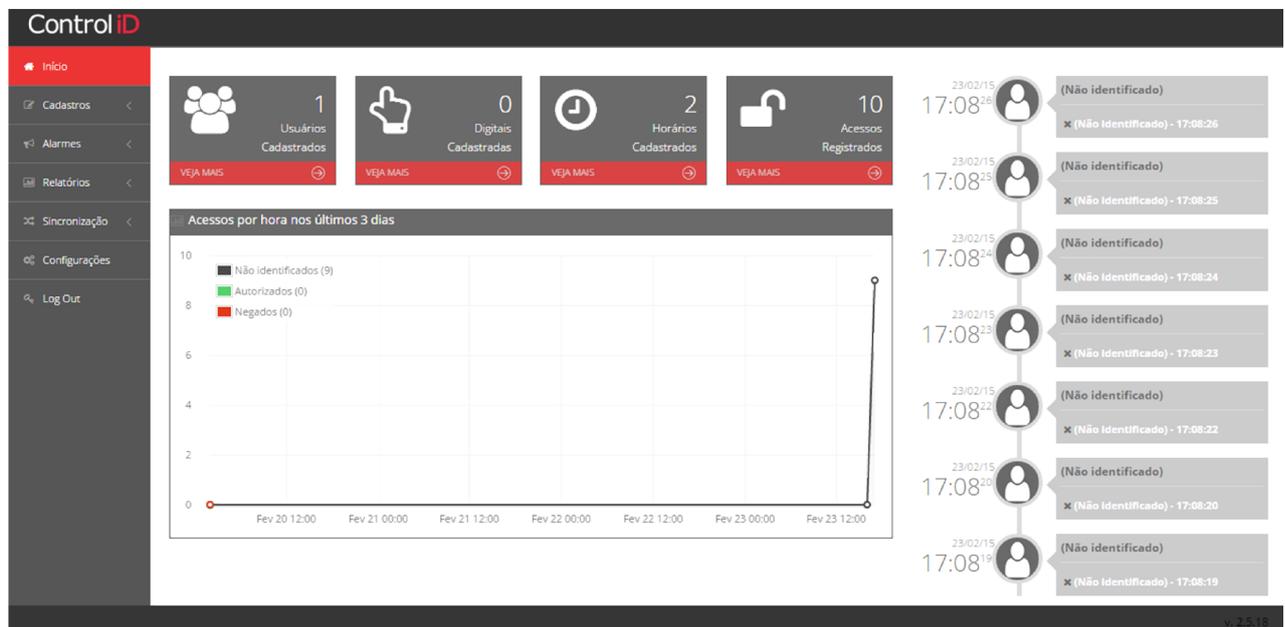
Para facilitar a configuração dos equipamentos o iDAccess conta com uma interface web que possui as configurações acessíveis pela interface gráfica e, ainda, possui funcionalidades exclusivas, somente acessíveis pelo web browser.

Para acessar o configurador web, abra o navegador web (preferencialmente o Google Chrome) e digite o IP definido anteriormente para o equipamento. Você será apresentado à tela de login:



O login e a senha padrões são “admin” e “admin” respectivamente.

Você verá a tela inicial da interface:



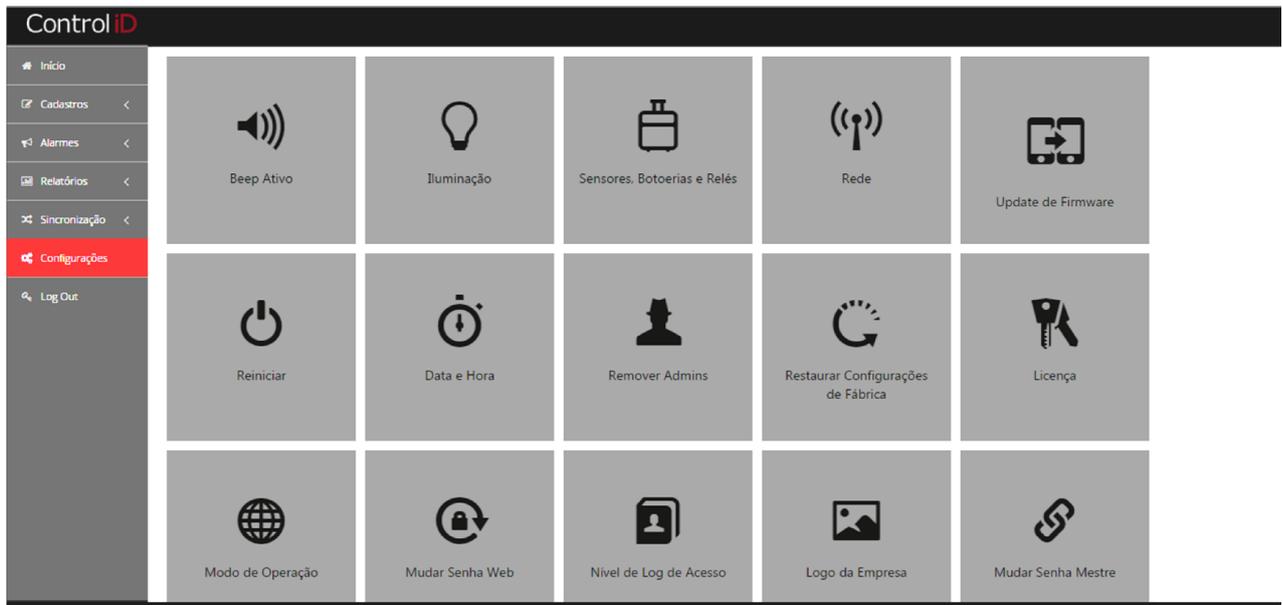
Vamos dar uma ênfase maior em como configurar o equipamento através da interface web. Para consultar detalhes de como operar o equipamento através da interface gráfica consulte o manual do usuário, disponível no site da Control iD.

4.3. Configuração dos relés

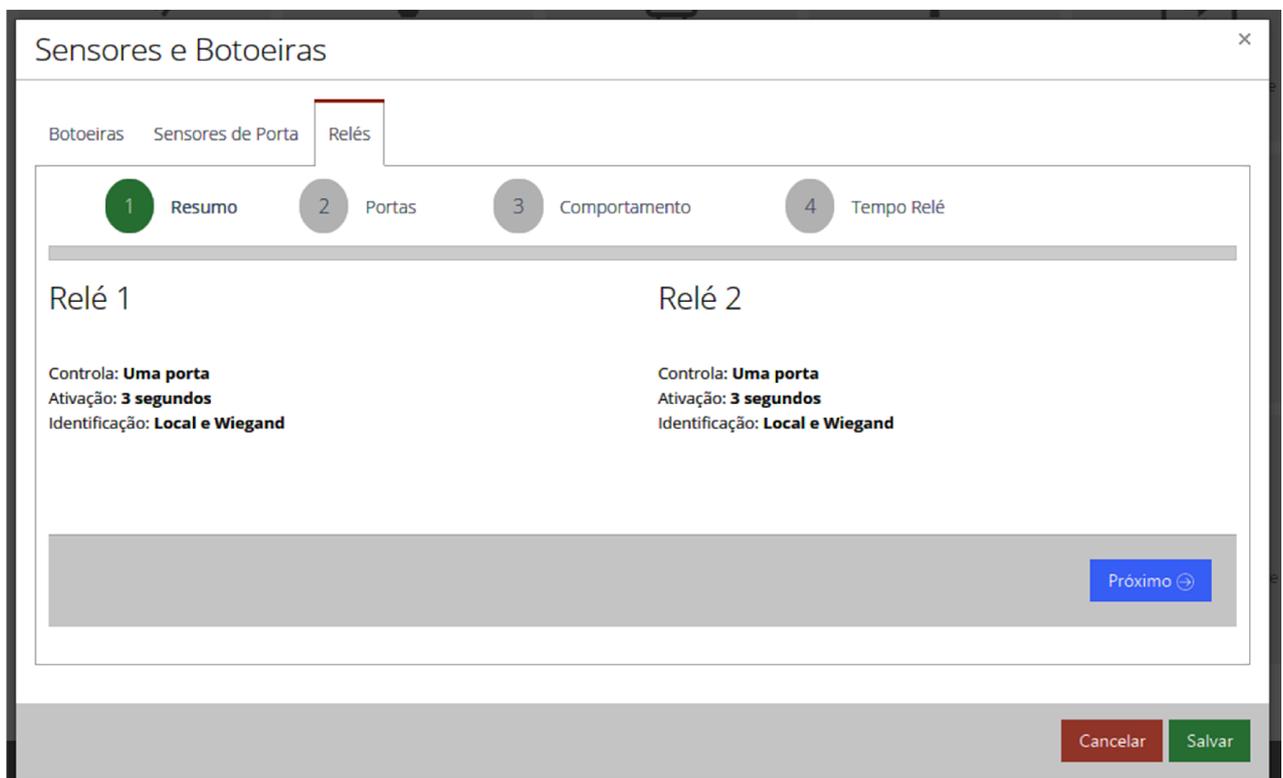
Para que os equipamentos possam controlar adequadamente as portas precisamos configurar como vão operar os dois relés, além de configurarmos botoeiras e sensores de porta, caso estejam conectados ao equipamento.

O iDAccess possui dois relés, que podem ser utilizados para controlar duas portas simultaneamente, duas portas independentes, ou ainda uma porta e uma sirene.

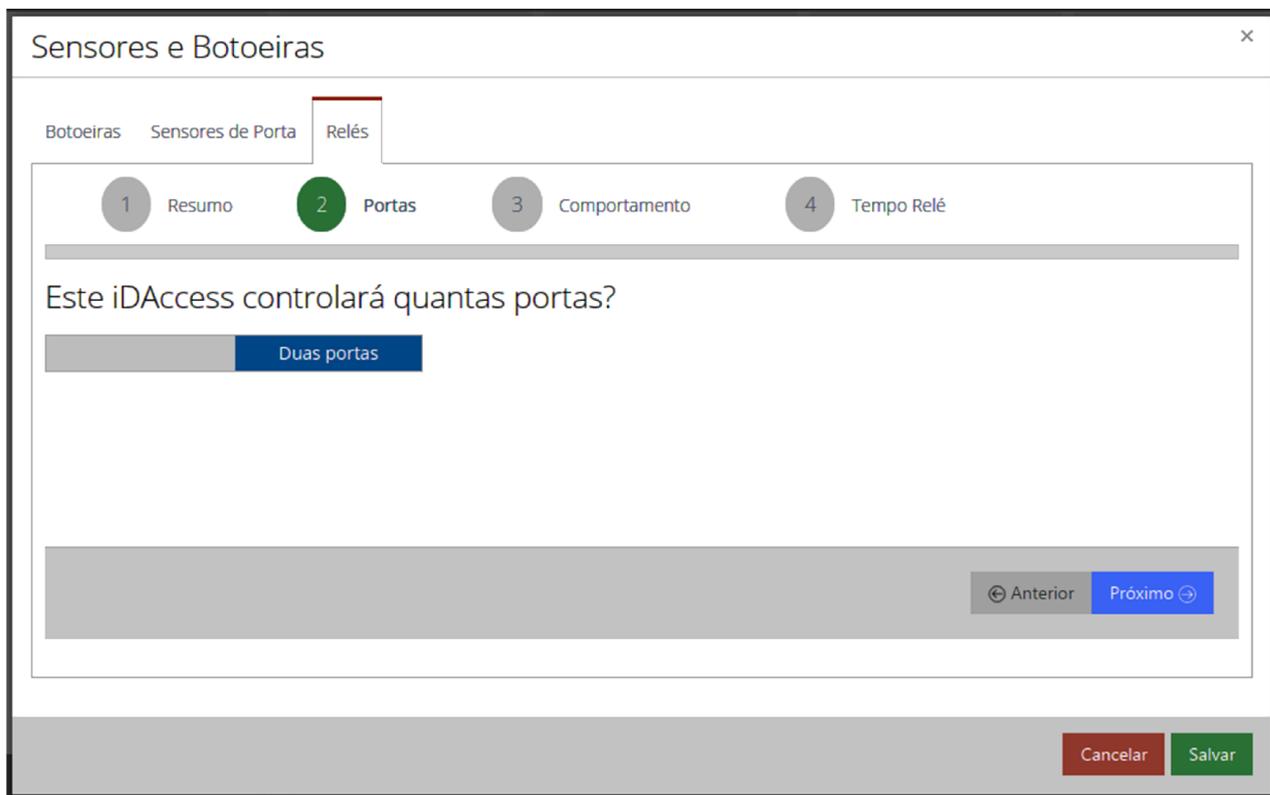
Vamos começar configurando os relés. Acesse a interface web, conforme foi visto no capítulo anterior e, no menu lateral esquerdo, clique em Configurações.



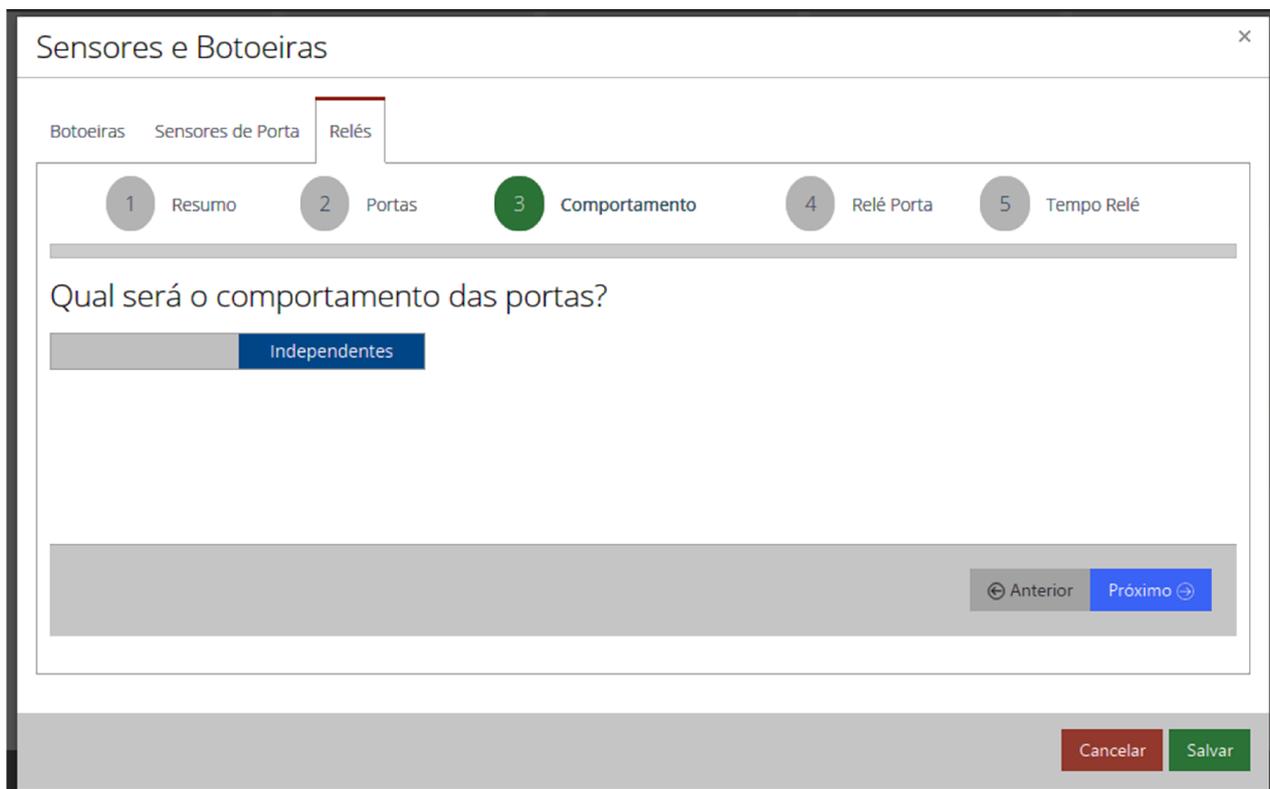
Clique em “Sensores, botoeiras e Relés” e então clique na aba “Relés”.



Pressione “Próximo” para iniciar o processo de configuração do relé.



Primeiramente você deve escolher quantas portas o equipamento vai controlar. Vamos começar configurando-o para controlar duas portas. Selecione “Duas portas” na tela de configuração e clique em “Próximo”.

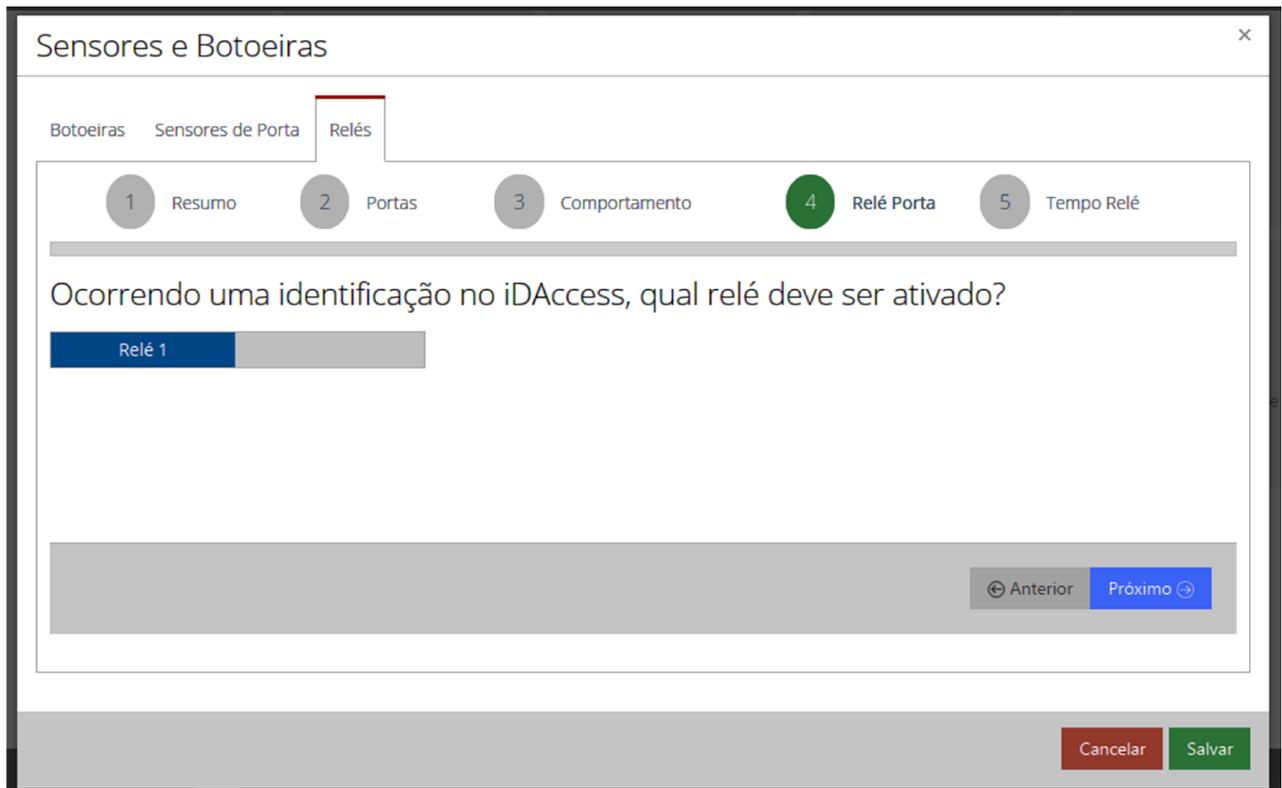


Agora vamos escolher o comportamento das portas controladas pelos relés. Há dois comportamentos possíveis:

- **Clonadas:** os dois relés serão acionados juntos quando uma identificação ocorrer através do equipamento.
- **Independentes:** apenas um dos relés será acionado quando uma identificação ocorrer através do equipamento. O outro relé será acionado quando houver uma identificação proveniente de um leitor externo.

Vamos escolher o modo independente como um exemplo. Selecione “Independentes” na tela de configuração e clique em “Próximo”.

Na próxima etapa devemos escolher qual relé será acionado quando uma identificação ocorrer através do equipamento. Esta etapa não é necessária quando escolhermos os relés com comportamento clonado.



Como exemplo, vamos escolher o relé 1. Selecione “Relé 1” na tela de configuração e clique em “Próximo”.

Botoeiras Sensores de Porta **Relés**

1 Resumo 2 Portas 3 Comportamento 4 Relé Porta **5 Tempo Relé**

Por quanto tempo a porta deve permanecer aberta?

Relé 1

Tempo de de ativação máximo(segundos)

5

Relé 2

Tempo de de ativação máximo(segundos)

5

Anterior

Cancelar Salvar

Por fim vamos configurar o tempo que as portas permanecerão abertas, vamos colocar 5 segundos para cada porta, digite 5 em cada um dos campos de configuração dos relés e clique em “Salvar” para salvar as configurações e fechar a tela.

O processo para configurar um dos relés para ativar uma campanha ou uma sirene é parecido com o exposto acima, a única diferença é que na tela final você deve escolher o que será ligado no segundo relé.

Sensores e Botoeiras

Botoeiras Sensores de Porta **Relés**

1 Resumo 2 Portas 3 Relés 4 Relé Porta **5 _Outro Relé**

O que está ligado no outro relé?

Uma sirene de alarme

Uma campanha

Tempo máximo ativada(segundos)

3

Nada

Anterior

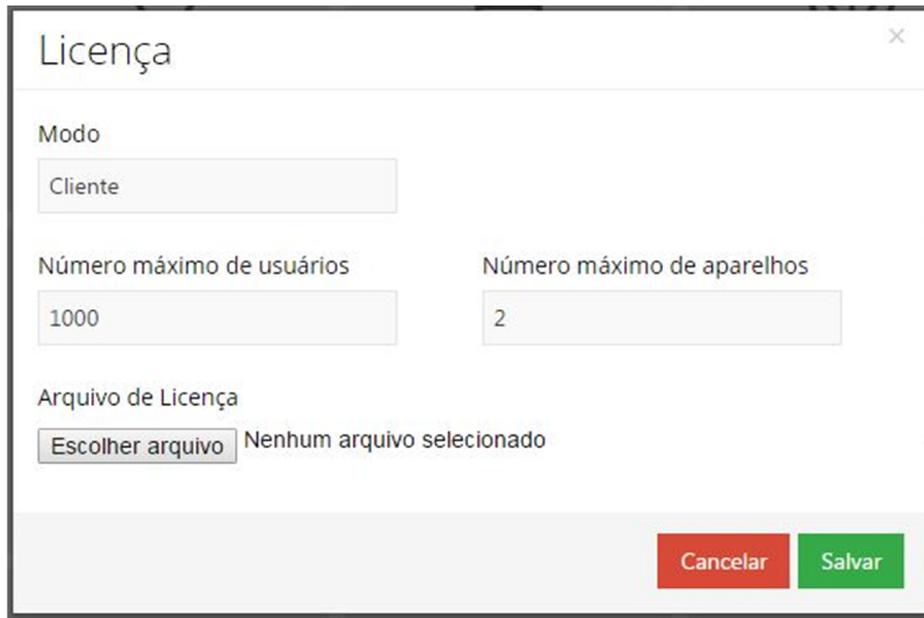
Cancelar Salvar

4.4. Equipamentos em modo centralizado

Se o seu equipamento estiver operando em modo stand-alone então ele já está configurado e pronto para realizar o controle de acesso. Já com equipamentos operando em modo centralizado é necessário realizar configurações adicionais.

A primeira coisa a fazer é definir um equipamento que atuará como servidor. Qualquer iDAccess ou iDBox pode ser utilizado para esse fim, o que diferencia um iDAccess servidor de um iDAccess comum é apenas o modo como o configuramos.

Acesse a interface web deste equipamento designado como servidor e acesse o menu de Configurações, e logo em seguida, clique em “Licença”.



A imagem mostra uma janela de configuração intitulada "Licença". No topo, há um botão "x" para fechar. O formulário contém os seguintes campos:

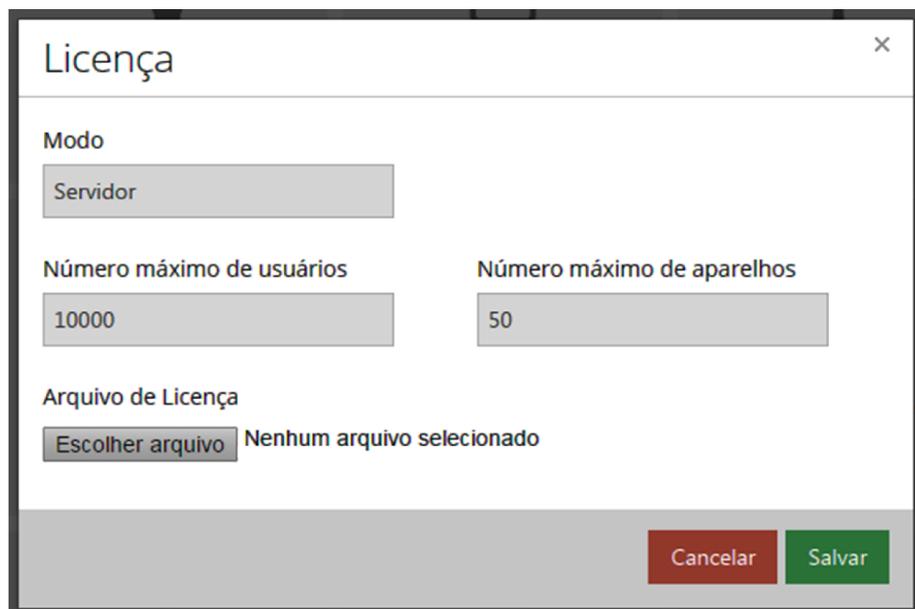
- Modo:** Um menu suspenso com o valor "Cliente" selecionado.
- Número máximo de usuários:** Um campo de texto com o valor "1000".
- Número máximo de aparelhos:** Um campo de texto com o valor "2".
- Arquivo de Licença:** Um botão "Escolher arquivo" seguido do texto "Nenhum arquivo selecionado".

Na base da janela, há dois botões: "Cancelar" (em um botão vermelho) e "Salvar" (em um botão verde).

Selecione o arquivo que contém a licença de servidor. Esse arquivo é fornecido pela Control iD e só pode ser gerado por ela. Contate-nos para adquirir o arquivo de licença.

Clique em “Salvar” e aguarde a mensagem “Licença alterada com sucesso”.

Observe novamente a janela de “Licença”.



A imagem mostra a mesma janela de configuração "Licença", mas com o modo alterado para "Servidor". Os valores dos campos são:

- Modo:** "Servidor".
- Número máximo de usuários:** "10000".
- Número máximo de aparelhos:** "50".
- Arquivo de Licença:** "Escolher arquivo" e "Nenhum arquivo selecionado".

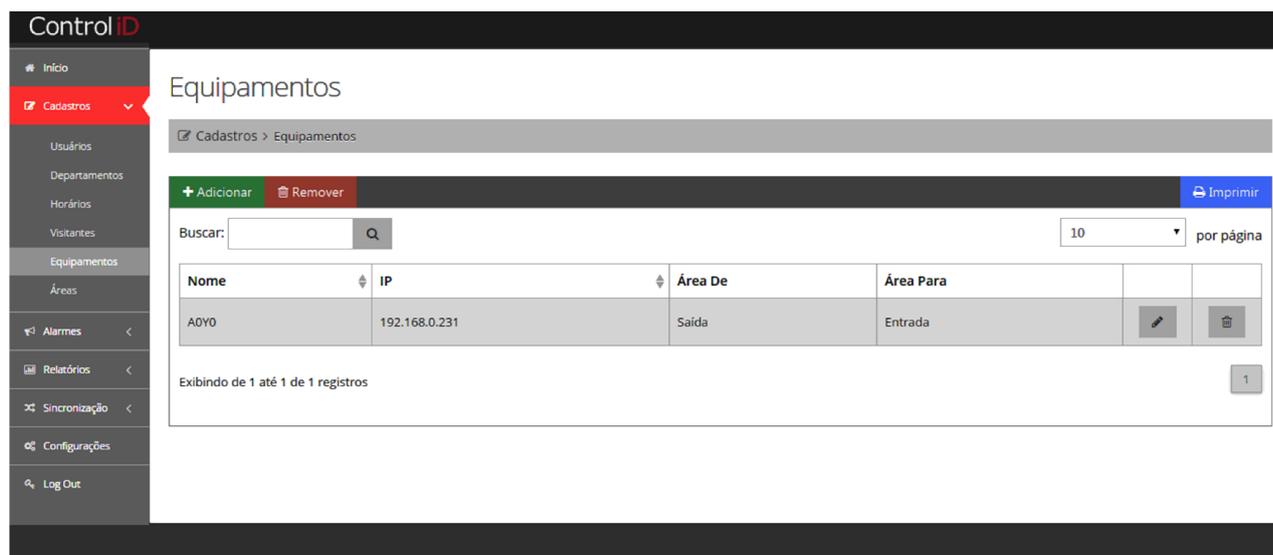
Os botões "Cancelar" e "Salvar" permanecem na base da janela.

Verifique que o “Modo” esteja definido como “Servidor” e que o número máximo de usuários e o número máximo de aparelhos estejam de acordo com o contratado.

Para concluir a configuração do servidor reinicie o equipamento, clicando em “Reiniciar” no menu de configurações. Aguarde 60 segundos até que o configurador web volte a ficar operacional. Repare que agora há mais dois itens no menu de cadastros: equipamentos e áreas. Por enquanto vamos apenas cadastrar equipamentos, veremos mais adiante como cadastrar áreas e como utiliza-las para criar regras de acesso.

A título de exemplo vamos definir o IP de um equipamento, conforme vimos da seção **4.1 - Rede**, como sendo 192.168.0.15.

Abra o menu de cadastro de equipamentos.



The screenshot shows the 'Equipamentos' page in the Control ID system. The sidebar on the left contains a navigation menu. The main area displays a table with the following data:

Nome	IP	Área De	Área Para
A0Y0	192.168.0.231	Saída	Entrada

Você verá que o próprio equipamento servidor já está cadastrado. Clique em “Adicionar” para adicionar um novo equipamento.



The screenshot shows the 'Equipamentos' form with the following fields:

- Nome: Equipamento Exemplo
- IP: 192.168.0.15
- Login: admin
- Senha:
- Área De: Entrada
- Área Para: Saída

Preencha os campos “Área De” e “Área Para” conforme a figura acima e clique em “Salvar”. O equipamento com o IP 192.168.0.15 será localizado e automaticamente configurado para operar como cliente no modo integrado. Você deve fazer isso para todos os equipamentos da rede que forem operar em modo centralizado.

5. Gerenciamento de acesso

O iDAccess permite que você configure acessos individuais e por grupos, possibilitando que você gerencie quem pode entrar em determinada área e em qual horário esta pessoa pode ou não realizar o acesso. O conjunto de mecanismos que permitem esse gerenciamento é denominado “Regra de acesso”.

Cadastrar uma regra de acesso no iDAccess é um processo muito simples e intuitivo. Este processo demanda a realização de dois cadastros, nesta ordem: Horário e Departamento.

5.1. Horários

Para cadastrar um horário acesse o configurador web e clique em “Cadastros” e, em seguida, “Horários”.

Nome	Início	Fim	Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado		
Horário Exemplo	08:00 09:00	18:00 14:00	✗ ✓	✓ ✗	✓ ✗	✓ ✗	✓ ✗	✓ ✗	✗ ✓		
Sempre Liberado	00:00	23:59	✓	✓	✓	✓	✓	✓	✓		

Clique em “Adicionar” para criar um novo horário.

Início	Fim	Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado		
08:00	18:00	✗	✓	✓	✓	✓	✓	✗		
09:00	14:00	✓	✗	✗	✗	✗	✗	✓		

Digite um nome para o horário, como, por exemplo, “Horário Exemplo” e clique em “Adicionar” para adicionar uma faixa horária para este horário.

Faixa de Horário

Início: 08:00

Fim: 18:00

Domingo: [X]

Segunda: [✓]

Terça: [✓]

Quarta: [✓]

Quinta: [✓]

Sexta: [✓]

Sábado: [X]

Cancelar Salvar

Selecione os dias da semana e os horários em que esta faixa será válida. Nosso horário de exemplo será válido de segunda à sexta das 8h às 17h. Isso significa que se alguém vinculado a esse horário não terá acesso autorizado fora desse horário. Clique em “Salvar” para criar a faixa horária.

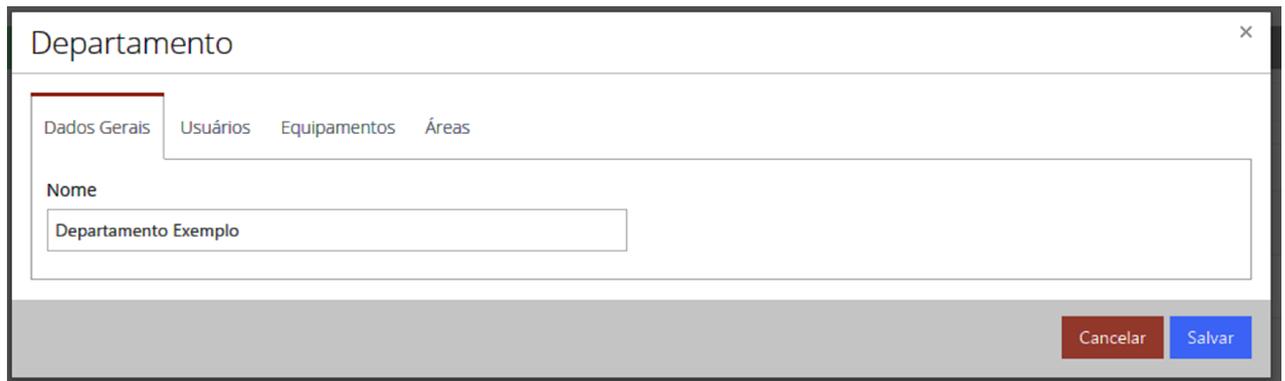
Vamos supor que necessitemos autorizar o acesso deste usuário também aos finais de semana, mas somente das 09h às 14h. Podemos fazer isso adicionando mais uma faixa horária ao nosso horário de exemplo. Para isso clique em “Adicionar” novamente.

Repita o mesmo processo para criar outra faixa horária válida somente aos finais de semana, das 09 às 14h.

Após adicionar todas as faixas de horário desejadas clique em salvar novamente para finalizar o cadastro.

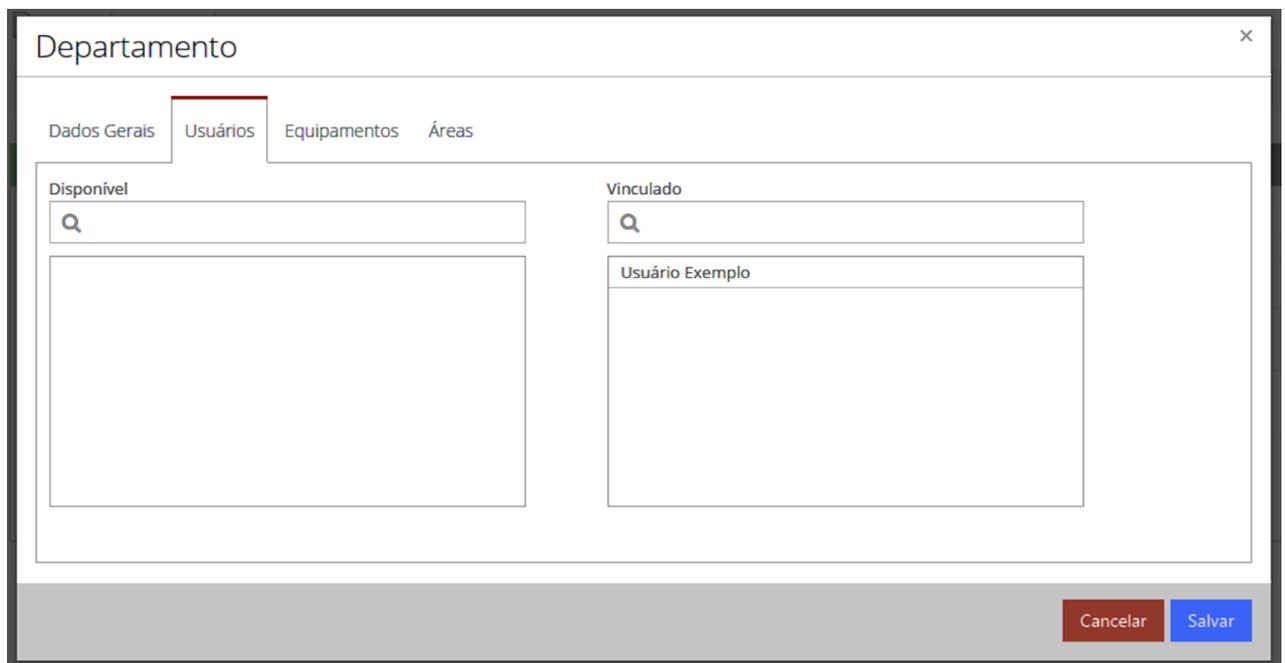
5.2. Departamentos

O próximo passo na criação de uma regra de acesso é vincular os usuários que serão liberados por esta regra a um Departamento. Portanto, criaremos um novo Departamento. Vá em “Cadastros” e, em seguida, “Departamentos”. Clique em “Adicionar”.



A captura de tela mostra a janela de edição de um departamento. No topo, há uma barra de título com o texto "Departamento" e um ícone de fechar. Abaixo, há uma barra de navegação com quatro abas: "Dados Gerais" (destacada com uma borda vermelha), "Usuários", "Equipamentos" e "Áreas". Na aba "Dados Gerais", há um campo de texto rotulado "Nome" com o valor "Departamento Exemplo" inserido. Na base da janela, há dois botões: "Cancelar" (em um botão vermelho) e "Salvar" (em um botão azul).

Na aba “Dados Gerais”, escolha um nome que identificará este Departamento. Clique na aba “Usuários”.



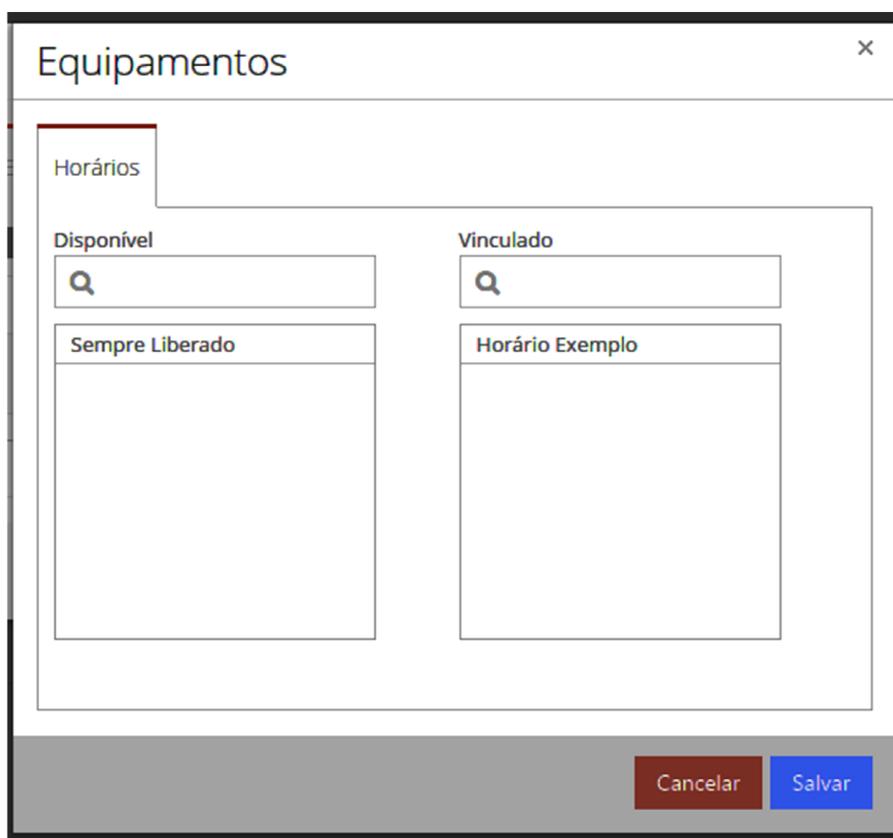
A captura de tela mostra a mesma janela de edição de departamento, mas com a aba "Usuários" selecionada. A interface é dividida em duas colunas. A coluna da esquerda, rotulada "Disponível", contém um campo de busca com um ícone de lupa e uma lista vazia abaixo. A coluna da direita, rotulada "Vinculado", também contém um campo de busca com um ícone de lupa e uma lista com um único item: "Usuário Exemplo". Na base da janela, os botões "Cancelar" e "Salvar" permanecem visíveis.

Vincule os usuários que desejar a este departamento. No nosso caso vamos vincular o “Usuário Exemplo”, para isso clique duas vezes sobre o nome do usuário.

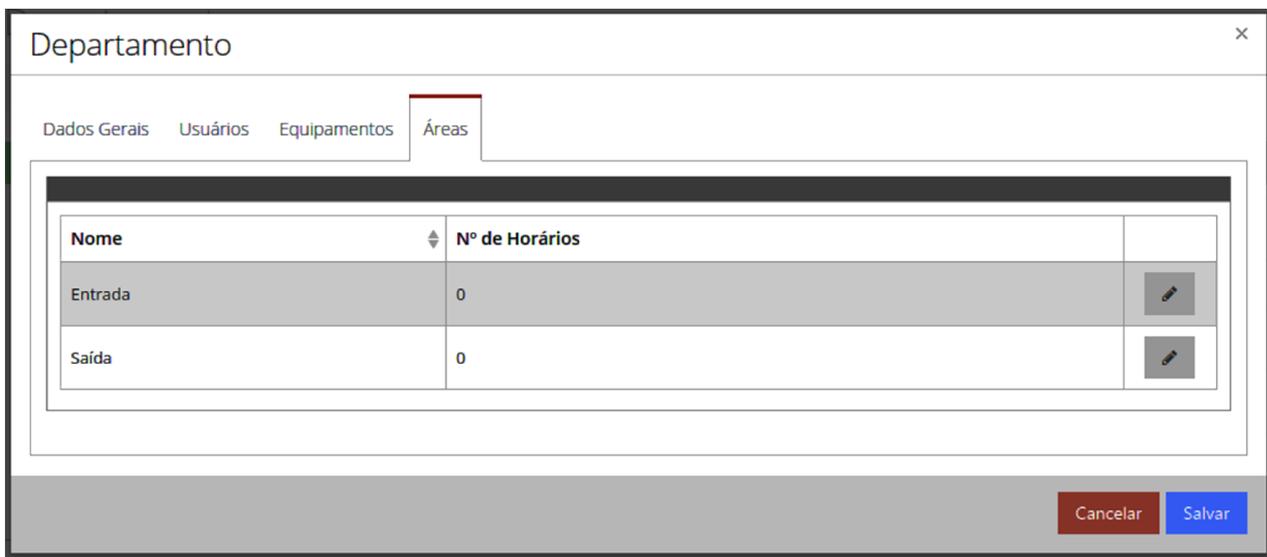
Em seguida clique na aba “Equipamentos”.



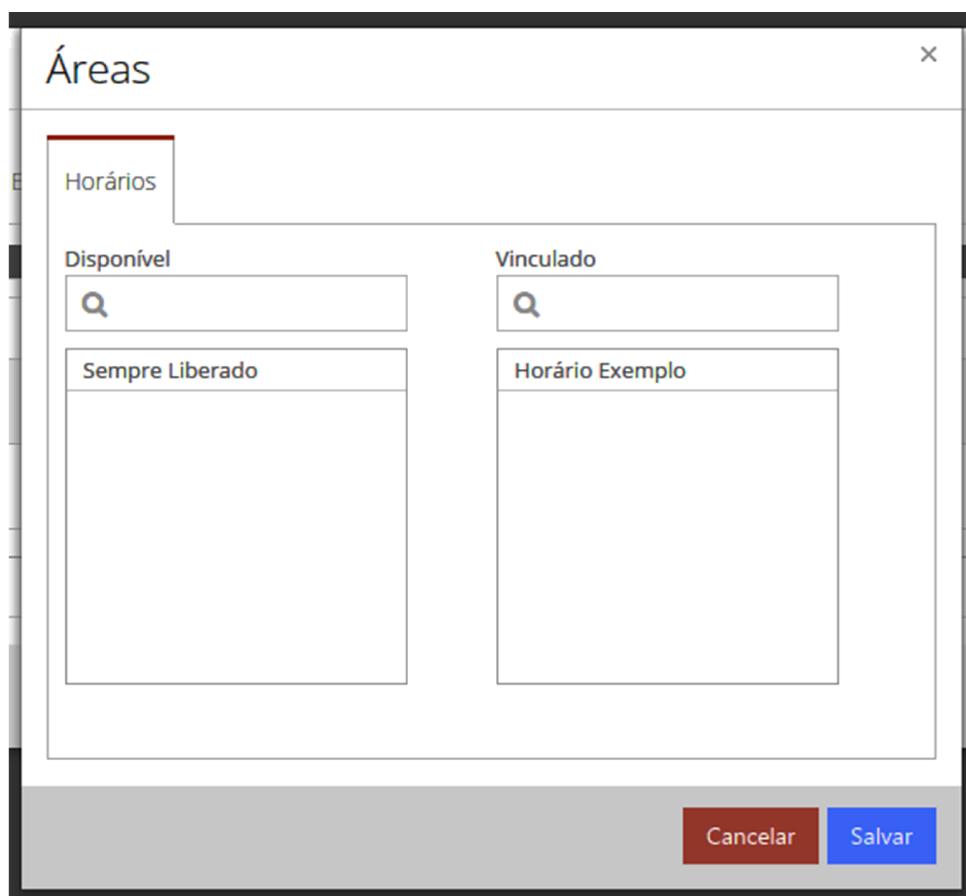
Clique no símbolo de lápis em cada equipamento listado para vincular um ou mais horários ao equipamento.



Pressione “Salvar” para encerrar a vinculação de horários. Quando terminar de editar todos os horários, clique na aba “Áreas”.



Na aba Áreas edite a área que será liberada e vincule o horário criado à mesma.



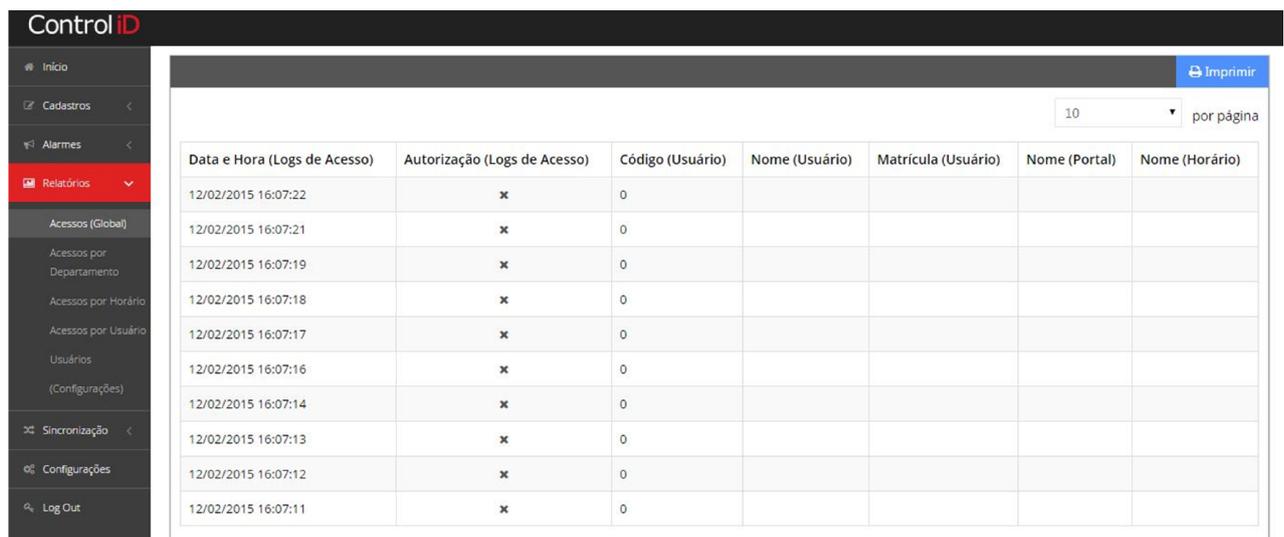
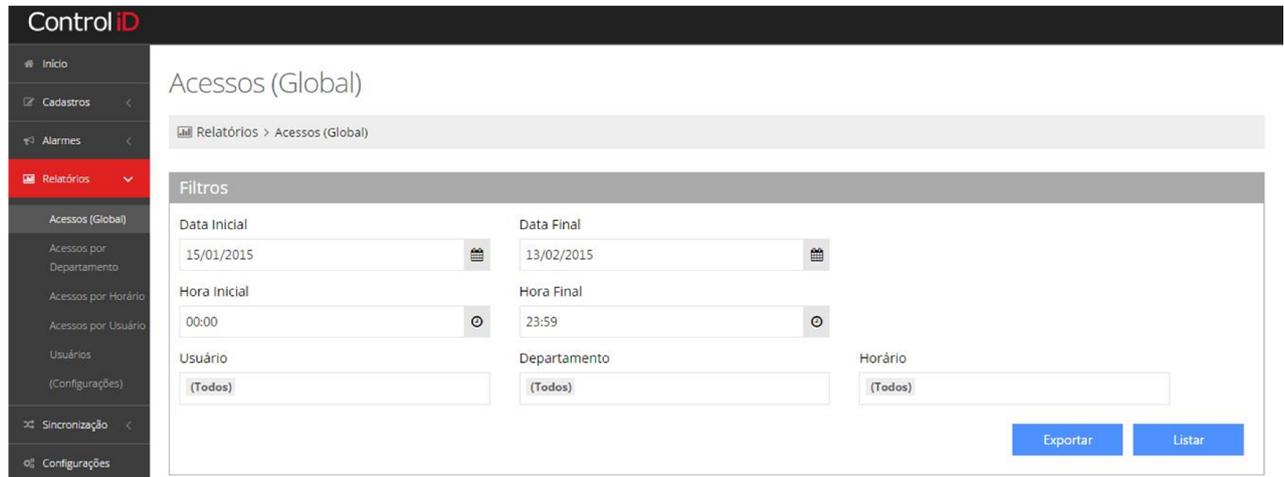
Clique em salvar para finalizar o cadastro da regra de acesso.

6. Relatórios

O iDAccess oferece várias opções para monitorar todas as tentativas de identificação que ocorrem nele, além de possibilitar que você exporte um relatório customizado, com as informações que achar mais relevantes.

6.1. Relatório padrão

Para gerar um relatório global de acessos clique em “Relatórios” e então em “Acessos (Global)”. Essa página permite obter um relatório global de acessos que pode ser filtrado por usuários, departamentos, horários, data e hora. Ainda é possível exportar o relatório no formato CSV.



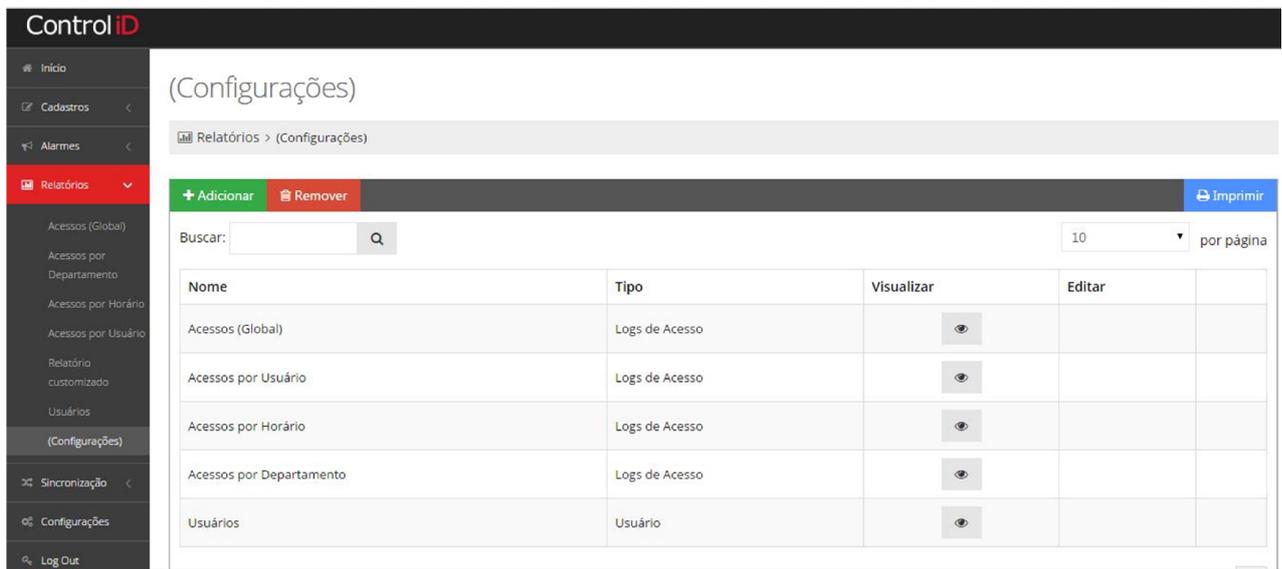
Data e Hora (Logs de Acesso)	Autorização (Logs de Acesso)	Código (Usuário)	Nome (Usuário)	Matrícula (Usuário)	Nome (Portal)	Nome (Horário)
12/02/2015 16:07:22	x	0				
12/02/2015 16:07:21	x	0				
12/02/2015 16:07:19	x	0				
12/02/2015 16:07:18	x	0				
12/02/2015 16:07:17	x	0				
12/02/2015 16:07:16	x	0				
12/02/2015 16:07:14	x	0				
12/02/2015 16:07:13	x	0				
12/02/2015 16:07:12	x	0				
12/02/2015 16:07:11	x	0				

Para gerar um relatório selecione o intervalo de datas que deseja apurar, em seguida selecione o intervalo de horas a ser mostrado em cada dia (e.g. das 8:00 às 17:00) em seguida selecione os departamentos que gostaria de visualizar, os usuários e por fim os horários. Clique em “Listar” para visualizar o relatório. Caso queira imprimir o relatório clique em “Imprimir”. Para salvar o relatório em formato CSV clique em “Exportar”.

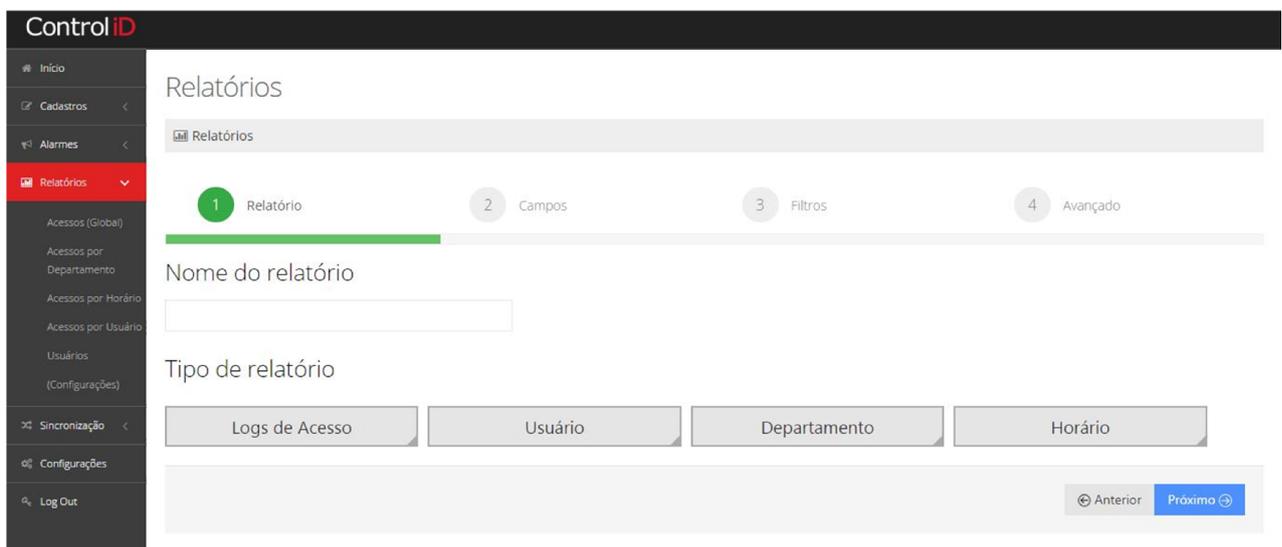
O mesmo procedimento pode ser adotado para gerar relatórios de “Acessos por departamentos”, “Acessos por horários”, “Acessos por usuário” e “Usuários”.

6.2. Relatório customizado

Uma das ferramentas mais poderosas do iDAccess é a capacidade de gerar relatórios totalmente customizáveis através da interface web. Para criar um relatório customizado clique em “Relatórios” e então em “(Configurações)”.



Clique em “Adicionar”



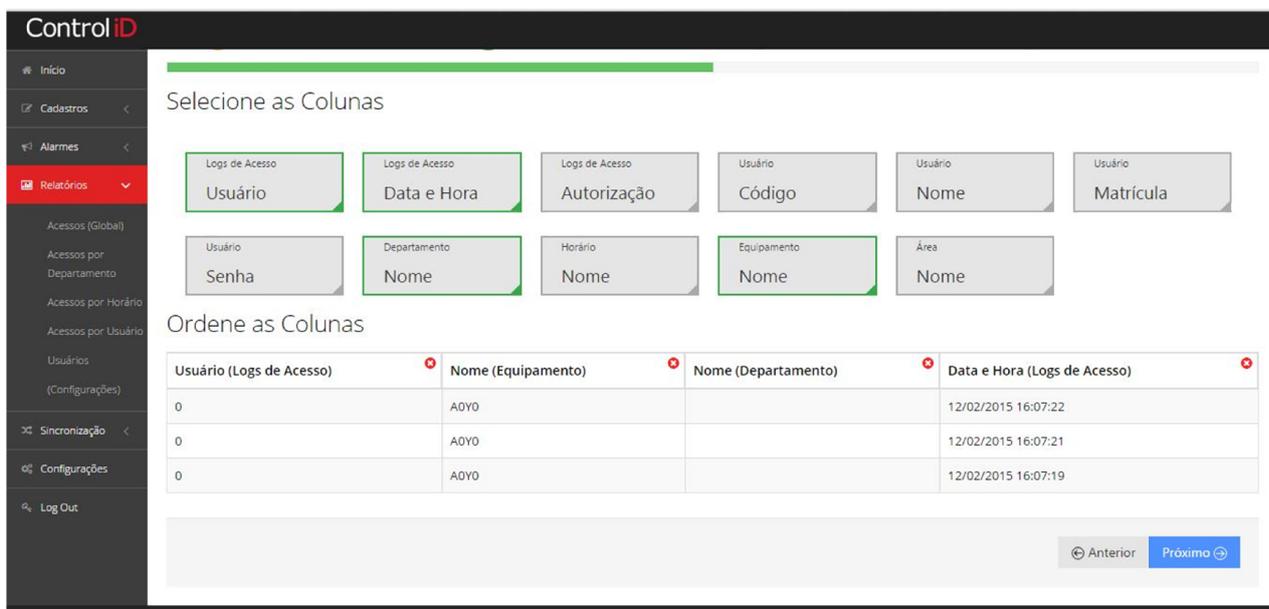
Para gerar o relatório customizado precisamos primeiro definir um nome, por exemplo, “Acessos (customizado)”.

Precisamos também definir o tipo de relatório, existem quatro tipos possíveis:

- **Logs de acesso:** registra todas as tentativas de acesso, autorizadas ou não, armazenadas no sistema.
- **Usuário:** registra todos os usuários cadastrados no sistema.
- **Departamento:** registra todos os departamentos cadastrados no sistema.
- **Horário:** registra todos os horários cadastrados no sistema.

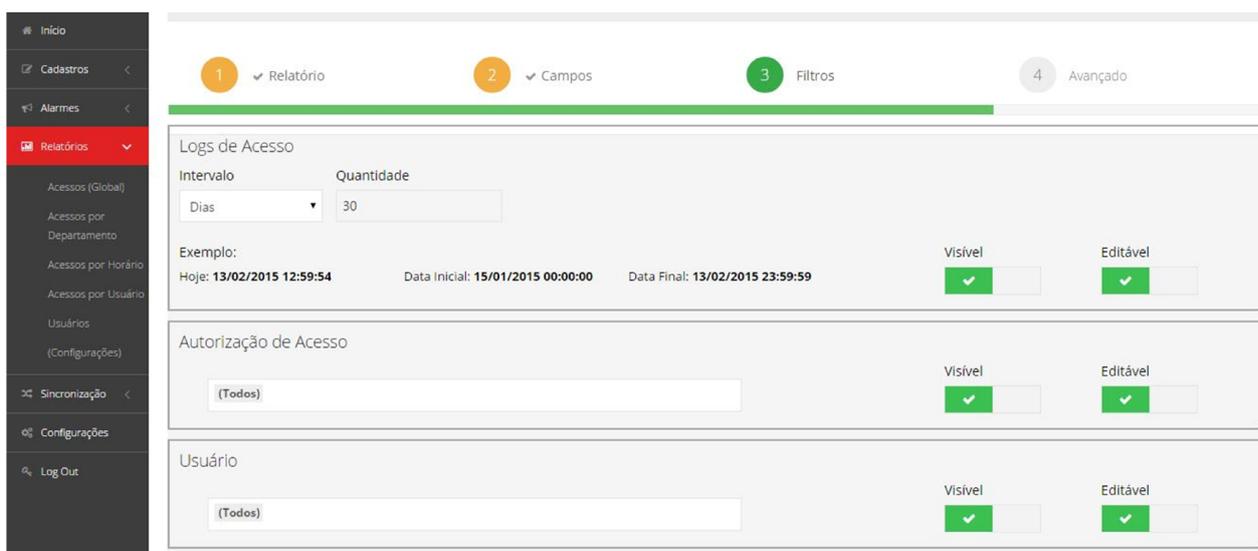
Como queremos um relatório de acessos então escolheremos “Logs de acesso” como tipo do relatório.

Clique em “Logs de acesso” e pressione “Próximo” para avançar para a próxima etapa.

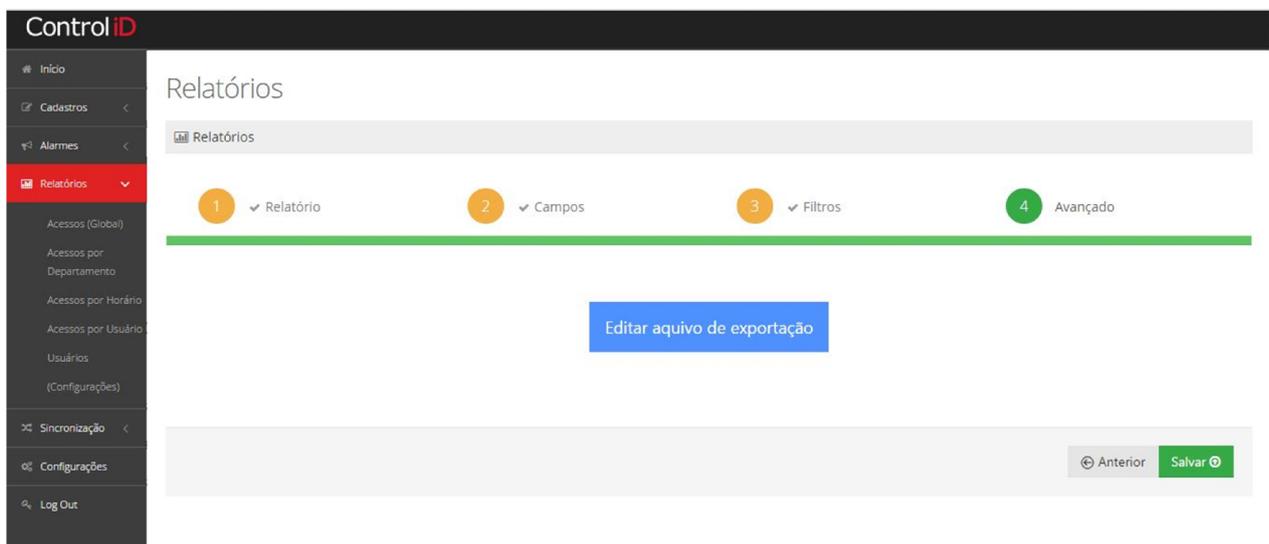


Agora devemos escolher quais colunas aparecerão no relatório, vamos escolher quatro delas (Usuário, Nome do usuário, Nome do departamento, Data e hora). Dependendo da ordem em que você clicou nas colunas, o seu relatório não estará com a mesma ordem apresentada na figura. Para resolver isso você pode reordenar as colunas clicando e arrastando cada uma delas.

Feito isso, clique em “Próximo” para seguir à etapa seguinte.



Nesta etapa iremos escolher quais filtros estarão presentes na hora de gerar o nosso relatório. Para desabilitar um filtro o desmarque como “Visível”. Se quiser que o filtro seja visível, porém não editável, basta desmarca-lo como “Editável”. Vamos manter um filtro de Logs de acesso e de Usuário, portanto, desabilite os demais filtros e cliquem em “Próximo”.



A próxima etapa nos permite editar o arquivo de exportação. Clique em “Editar arquivo de exportação”.



Esta página nos permite modificar vários aspectos do arquivo de exportação como o Nome, o separador das colunas, como serão as quebras de linha, qual será o cabeçalho, etc.



Estas configurações devem ser feitas apenas por usuários avançados do sistema, uma vez que a alteração de qualquer uma delas pode prejudicar a geração do relatório criado.

Vamos deixar todas estas configurações sem nenhuma alteração, por enquanto. Clique em “Salvar” para gerar seu relatório customizado.

(Configurações)

Relatórios > (Configurações)

+ Adicionar Remove Imprimir

Buscar: Q 10 por página

Nome	Tipo	Visualizar	Editar
Acessos (Global)	Logs de Acesso		
Acessos por Usuário	Logs de Acesso		
Acessos por Horário	Logs de Acesso		
Acessos por Departamento	Logs de Acesso		
Usuários	Usuário		
Acessos (customizado)	Logs de Acesso		

Perceba que agora há uma nova entrada no menu de relatórios, correspondendo ao relatório “Acessos (customizado)” que acabamos de criar. Clique nessa nova entrada.

Control ID

Acessos (customizado)

Relatórios > Acessos (customizado)

Filtros

Data Inicial: 15/01/2015

Data Final: 13/02/2015

Hora Inicial: 00:00

Hora Final: 23:59

Usuário: (Todos)

Departamento: (Todos)

Exportar Listar

10 por página

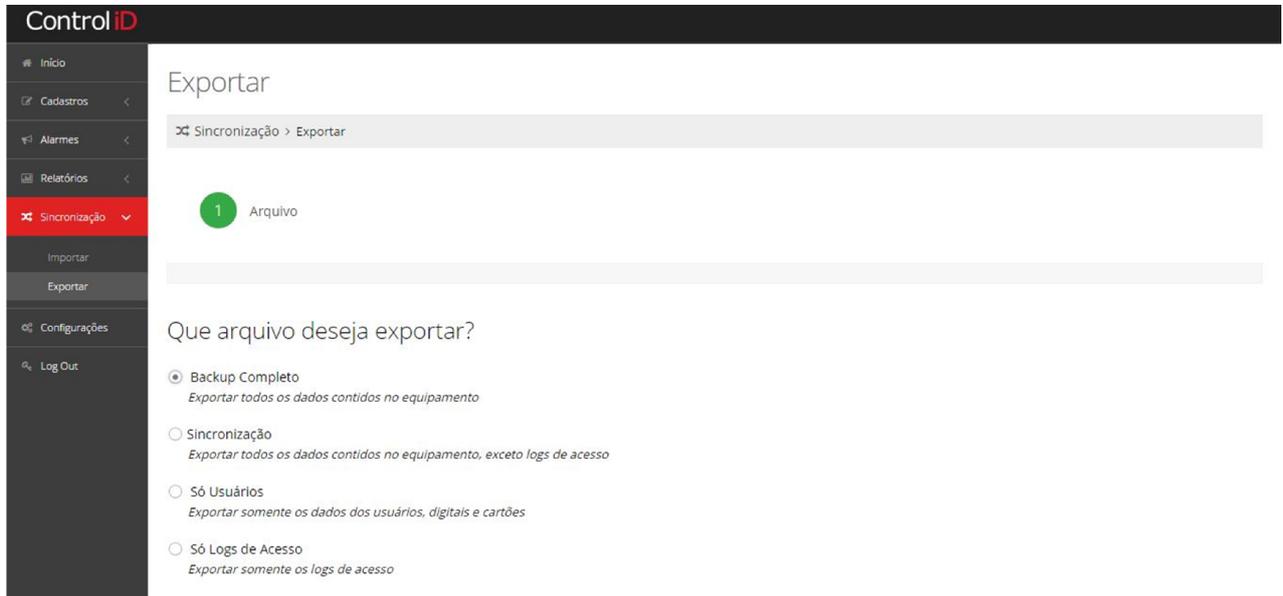
Pronto! Agora você pode gerar um relatório customizado da mesma maneira que um relatório padrão é gerado. Perceba que só os filtros habilitados na criação do relatório estão disponíveis. Além disso, ao exportar o arquivo, o tipo de arquivo, o nome e o formato de exportação estarão disponíveis no formato também definido, anteriormente, na criação do relatório.

7. Sincronização de dados

Muitas vezes durante a operação do sistema você vai querer exportar ou importar os dados cadastrados no iDAccess, seja para realizar backups, seja para transferir dados de um sistema para outro ou qualquer outra finalidade. Felizmente, a interface web do iDAccess torna isso algo muito fácil e rápido de se fazer, permitindo que você sincronize dados rapidamente quando necessário.

7.1. Exportação

Para acessar a página de exportação de dados clique em “Sincronização” e então em “Exportação”.



Existem quatro tipos possíveis de exportação:

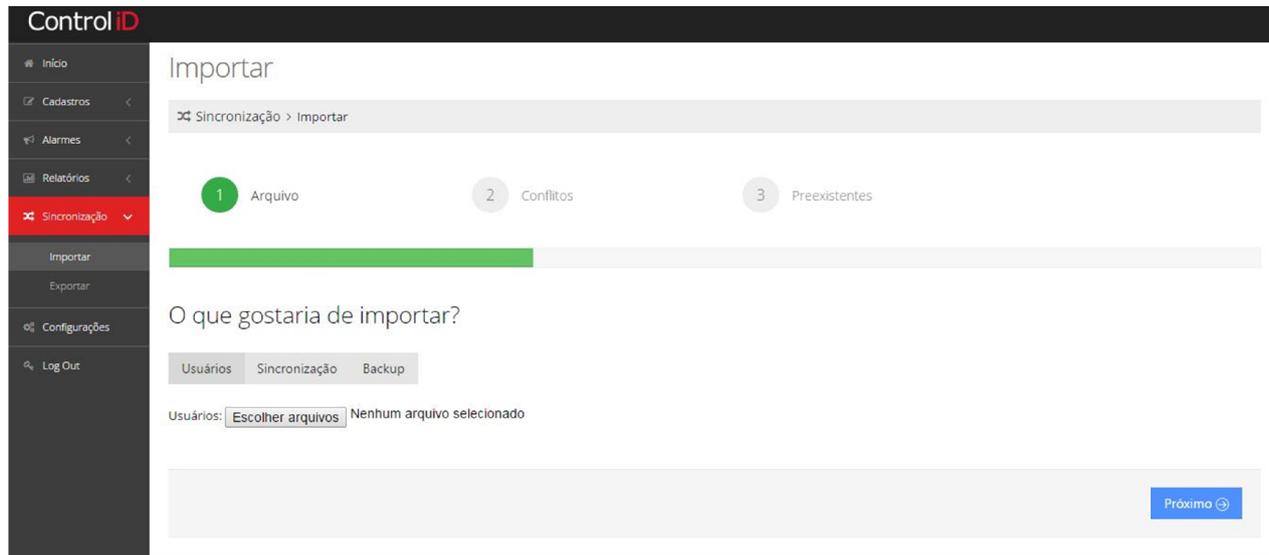
- **Backup Completo:** este é o tipo mais completo de exportação. Ele cria uma cópia completa do seu sistema, permitindo a recuperação dos dados em caso de falha.
- **Sincronização:** este tipo é semelhante ao backup, com a diferença de que os logs de acesso não são exportados. É utilizado para sincronizar os dados de um equipamento com outros.
- **Só usuários:** este tipo exporta somente os usuários cadastrados com todos os seus dados (nome, digitais, cartões, etc.), mas não copia departamentos e horários e tampouco mantém os vínculos desses usuários. É utilizado para exportar usuários para outros sistemas que necessitem destes dados.
- **Só Logs de Acesso:** este tipo exporta os logs de acesso registrados no equipamento. Também é utilizado para exportar logs para outros sistemas.

Para exportar um dos quatro tipos de arquivo é muito simples, basta selecionar o tipo desejado de exportação e clicar em “Exportar”. A título de exemplo vamos exportar os usuários cadastrados no sistema. Clique em “Só Usuários” e, então, clique em “Exportar”. Digite um nome para o arquivo como, por exemplo, “Usuarios_export.csv” e clique em “Salvar”.

7.2. Importação

Além de exportar seus dados também é possível importa-los em outros equipamentos ou mesmo importar arquivos provenientes de outros sistemas, desde que estes estejam no formato correto.

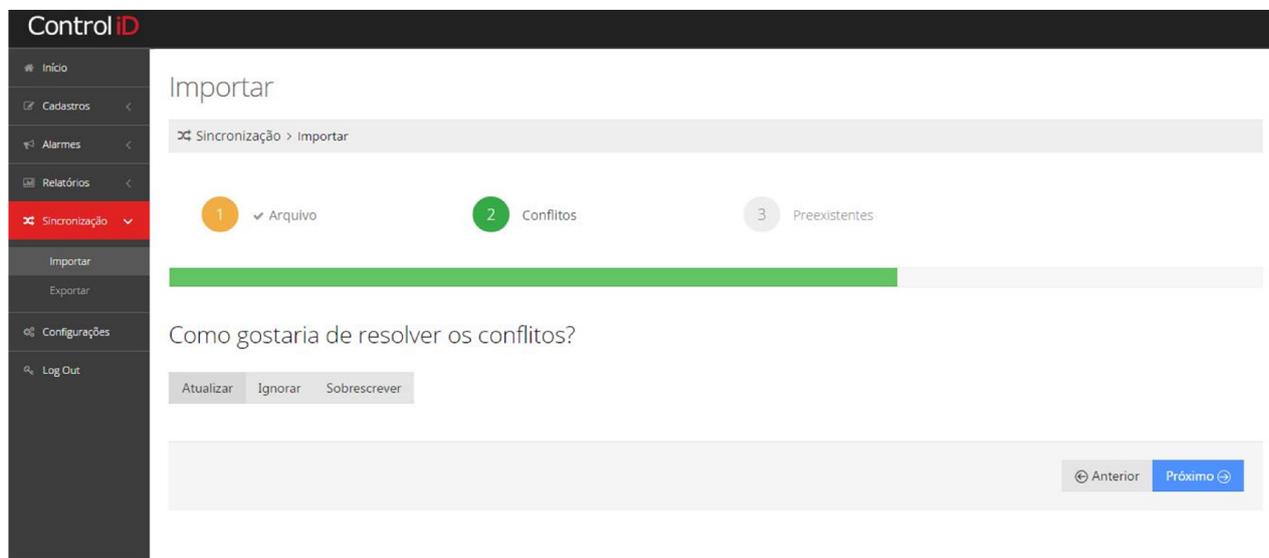
Para acessar a tela de importação clique em “Sincronização” e depois em “Importação”.



Novamente temos três tipos de arquivos de importação. Cada tipo refere-se ao tipo de exportação de mesmo nome, com exceção dos logs de acesso que não podem ser importados.

Vamos importar o arquivo de usuários gerado na seção anterior.

Clique em “Usuários” e em seguida clique em “Escolher arquivos”. Selecione o arquivo exportado previamente e clique em “Próximo” para prosseguir para a próxima etapa.



Agora devemos selecionar como vamos resolver os conflitos. Conflitos ocorrem quando tentamos importar dados já existentes no sistema (usuários, departamentos ou horários com o mesmo ID). Há três caminhos possíveis:

- **Atualizar:** neste caso, o sistema atualizará as informações existentes no sistema e que forem diferentes entre si.
- **Ignorar:** neste caso o sistema manterá os dados já existentes no sistema.

- **Sobrescrever:** neste caso o sistema apagará os dados existentes no sistema e gravará os novos dados no lugar.

Vamos selecionar “Sobrescrever” para que não haja nenhum problema de conflito. Selecione “Sobrescrever” e clique em “Próximo”.



Por fim devemos escolher o que faremos com os usuários que já estavam cadastrados no sistema e que não estavam no arquivo de exportação. Se escolhermos mantê-los o cadastro do sistema será composto dos usuários já cadastrados mais os usuários importados. Se escolhermos apaga-los, o cadastro do sistema será composto apenas dos usuários importados.

Vamos escolher apaga-los a fim de termos só os usuários importados. Clique em “Apagá-los” e então em “Importar” para finalizar o processo de importação.