Manual Defense IA 3.1

Controle de Acesso

Matriz: Rodovia BR 101, km 210 – Área Industrial – São José/SC – 88.104-800 – Fone: (48) 3281.9500 – Fax: (48) 3281.9505 **Filial SC**: Rodovia SC 281, Km 4,5 – Sertao do Maruim – São José/SC – 88.122-001 **Filial MG**: Rodovia BR 459, 1325, km 124 – Distrito Industrial – Santa Rita do Sapucaí/MG – 37.540-000 – Fone/Fax: (35) 3471.9840 **Filial AM**: Av. Tefé, 3105 – Japiim – Manaus/AM – 69.078-000

intelbras.com.br

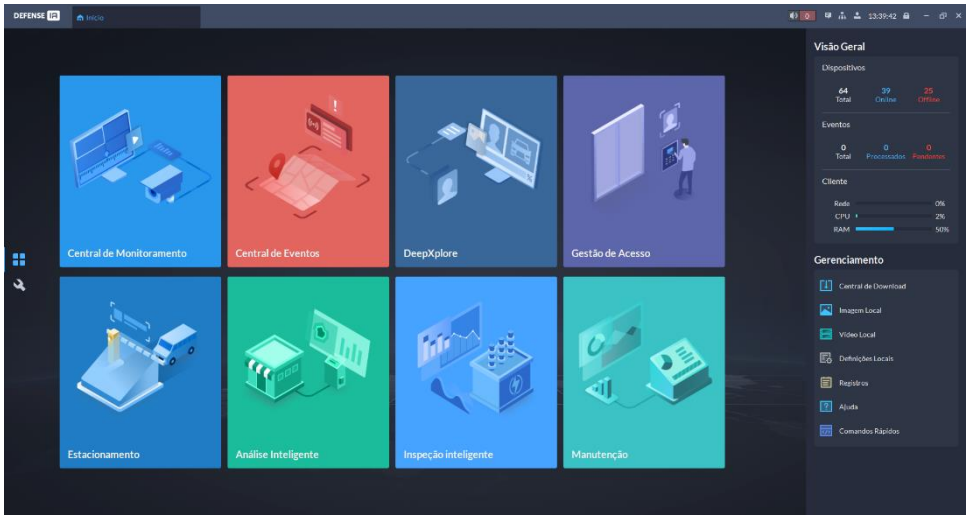
1. Defense IA

O Defense IA tem como foco gerir inteligência artificial dos equipamentos e fazer o vídeo-monitoramento do sistema de forma ágil. Monitore toda solução com um único software, compatível com CFTV, controladores de acesso, detectores de metais, Vídeo Wall e protocolo Onvif.

Tenha informações em tempo real da saúde do sistema e monitore os principais eventos através de dashboards, tornando o monitoramento mais eficiente.

Crie e acompanhe casos e operações a partir de imagens e gravações com registros de incidentes, gerando relatório com informações das ocorrências.

Interligue os sistemas da matriz, filiais e outras plantas de uma empresa, trazendo uma gestão unificada e inteligente do monitoramento.



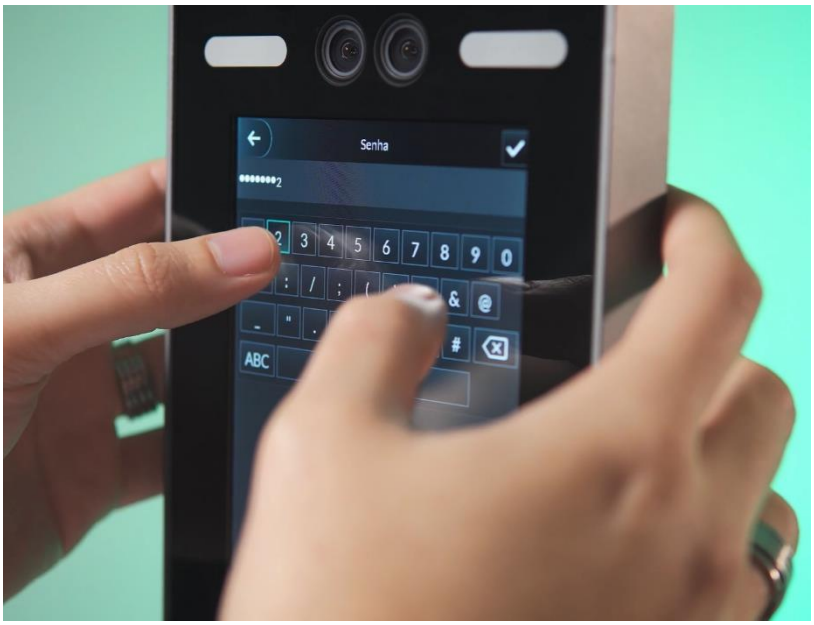
O Defense IA 3.1 é um sistema completo de segurança eletrônica. Este guia será focado na utilização das funções de **controle de acesso**.

Ex. de dispositivos da linha de controle de acesso: SS 5530 MF FACE, SS 5541 MF W, SS 1540 MF W

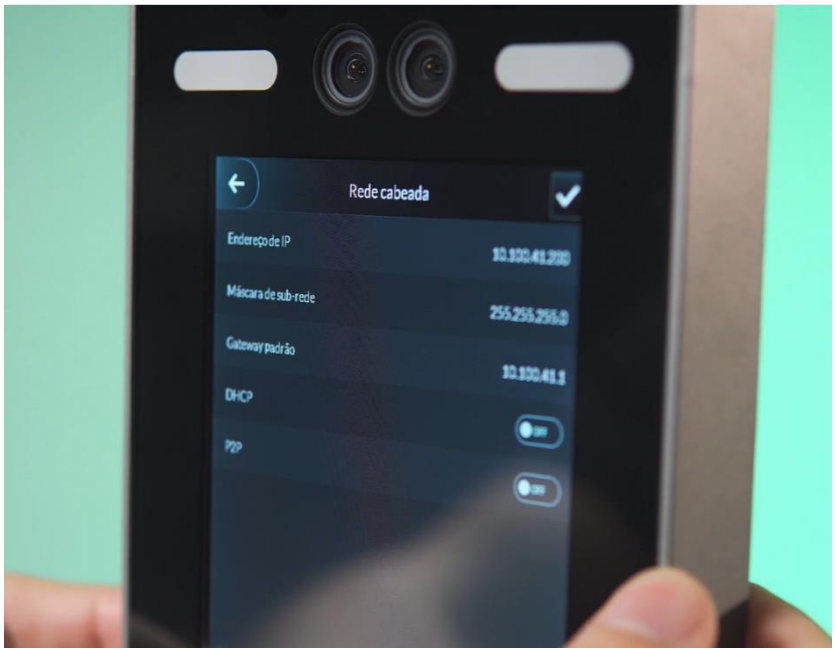
2. Adicionando dispositivo

2.1. Preparando o controlador de Acesso

Ligue o dispositivo. Alguns dispositivos suportam alimentação PoE, outros é necessário alimentar através de fonte 12V (para mais informações consulte o manual de usuário de cada equipamento). Após, realize as primeiras configurações, inserindo a nova senha de acesso e um email para recuperação de senha. Por padrão, o usuário do controlador é **admin**.



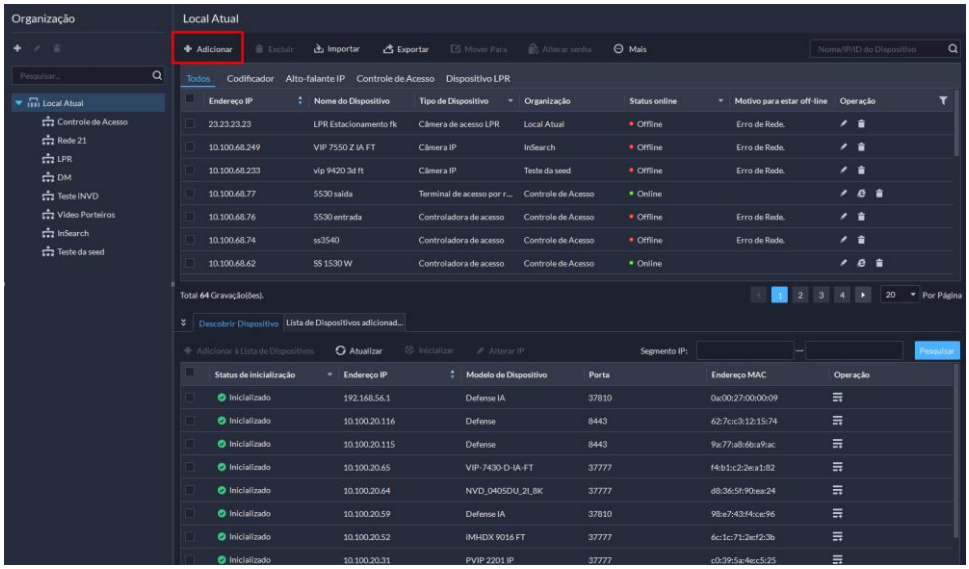
Após inicializar o dispositivo, vá para as configurações de rede. Lá, será possível identificar ou configurar o IP do dispositivo. Os controladores de acesso suportam função DHCP, caso habilitado a rede fornecerá um IP livre para a utilização do dispositivo de controle de acesso.



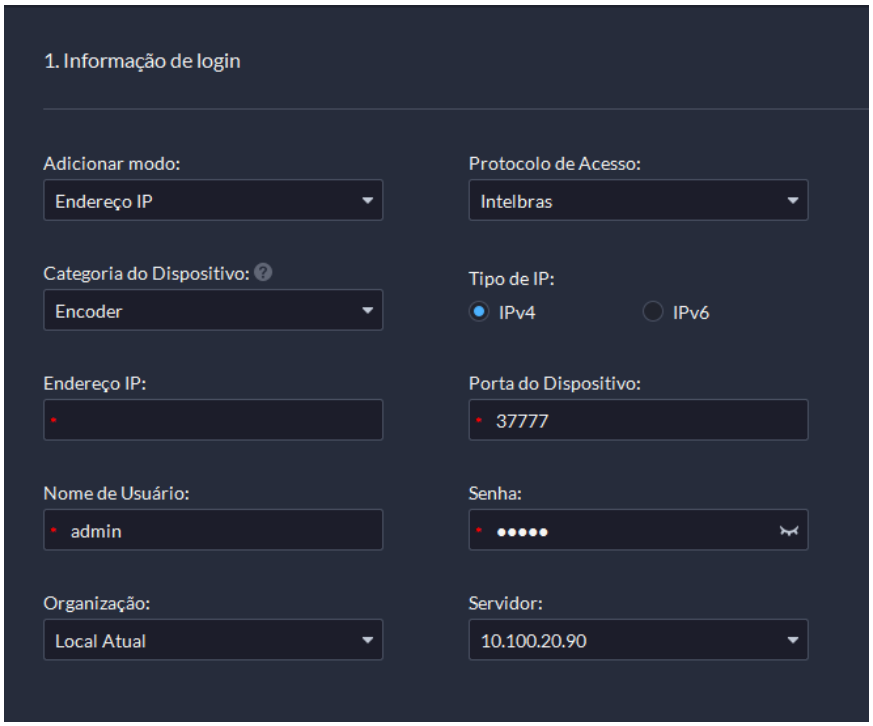
2.2. Adicionando o dispositivo ao Defense IA 3.1

Para adicionar um controlador de acesso previamente configurado, acesse o menu configurações e em seguida Dispositivos.

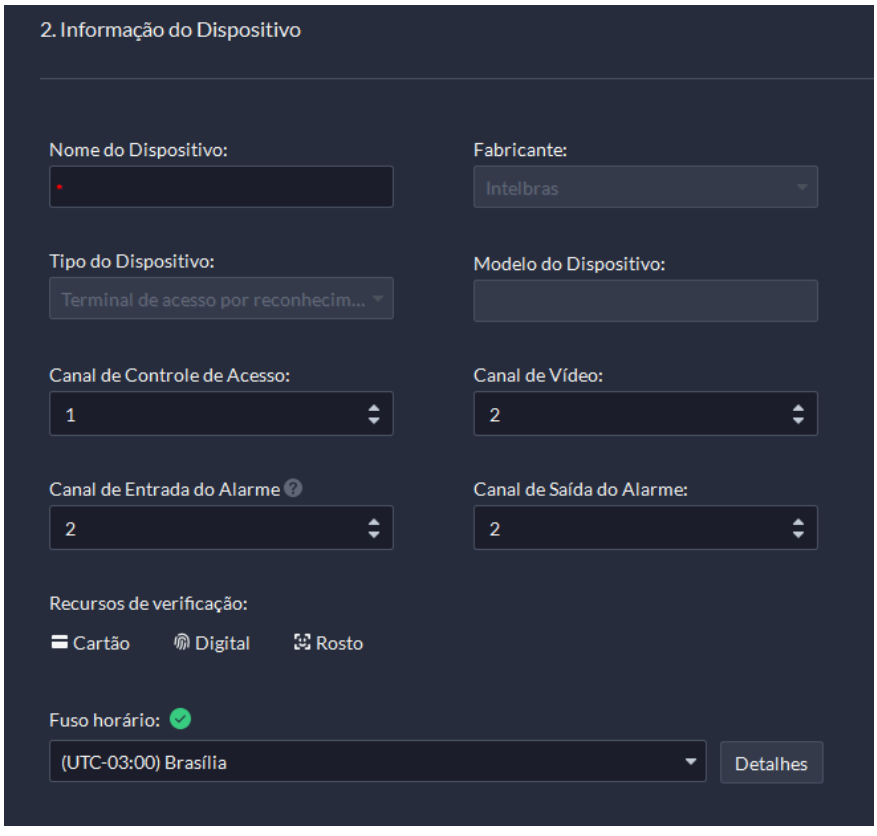
Crie uma organização de dispositivos (barra lateral esquerda) e adicione novos dispositivos. O Defense IA 3.1 irá identificar de forma automática dispositivos dentro de uma faixa de rede configurada, facilitando assim a adição dos dispositivos (barra inferior).



Após clicar em adicionar, uma janela de informações do dispositivo será aberta. Nela, lembre-se de configurar a **categoria do dispositivo** como **Controlador de Acesso**. Insira as autenticações do dispositivo e selecione a organização que o dispositivo irá pertencer.

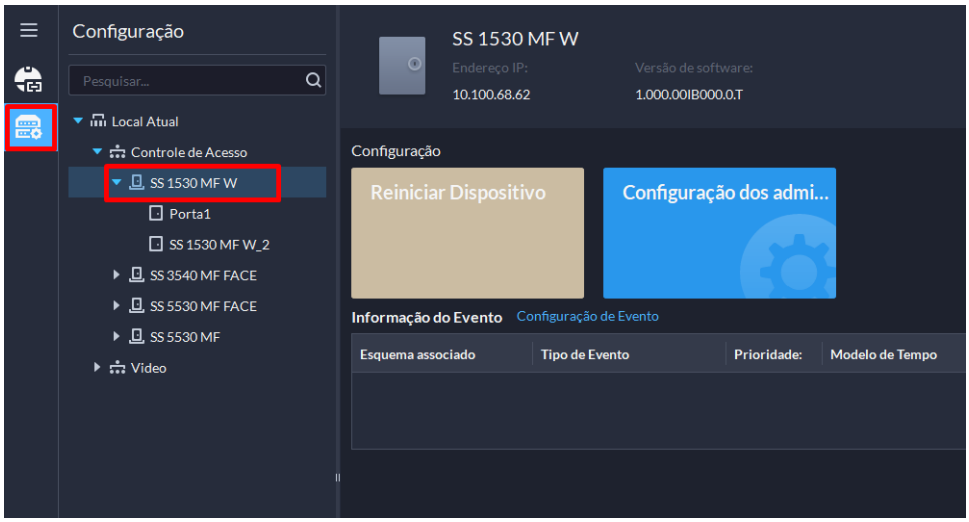


Após as primeiras configurações, insira o nome de identificação do dispositivo no sistema, o número de canais de controle de acesso que o dispositivo possuí (ex: CT 3000 4P são 4 canais), quantos canais de vídeo o dispositivo possuí (será consumido licença de vídeo caso habilitado o vídeo da controladora; os snapshots dos eventos de acesso da controladora são capturados mesmo se for inserido 0 canais de vídeo), canais de entrada e canais de saída de alarme.



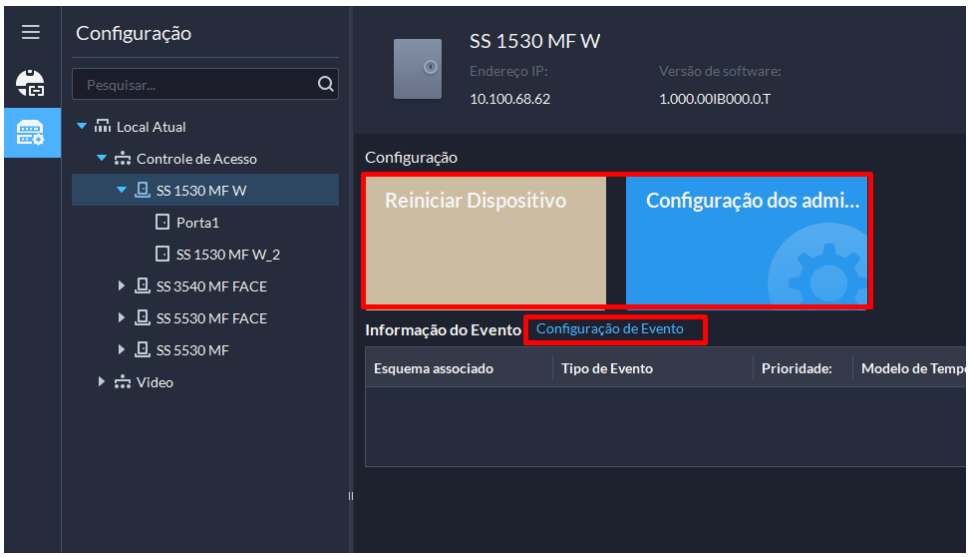
2.3. Configurando um dispositivo

Diversas configurações podem ser feitas em um controlador de acesso. Para iniciá-las acesse o menu configuração de dispositivos na barra lateral esquerda, e selecione o dispositivo de controle de acesso que se deseja configurar.



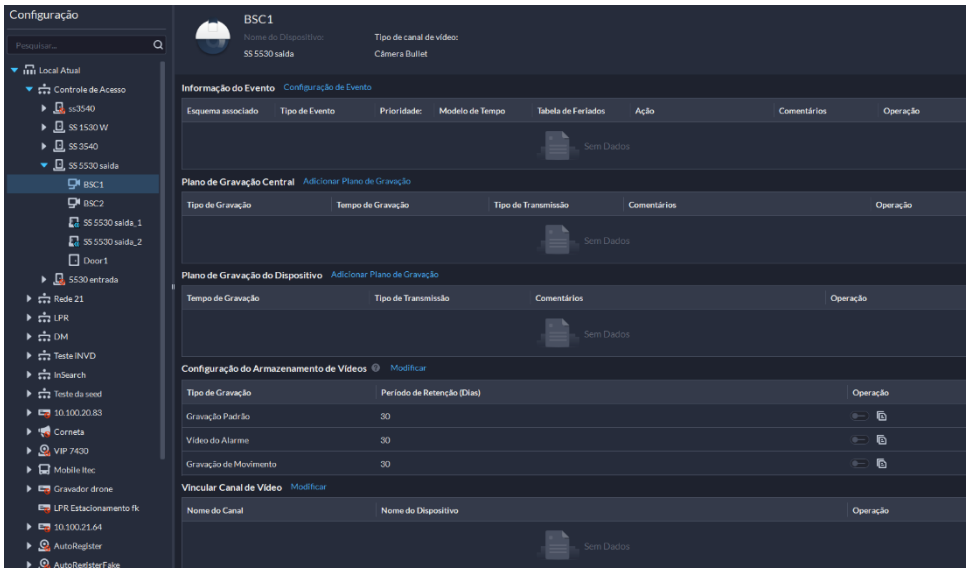
As primeiras operações que podem ser feitas no dispositivo de controle de acesso é a reinicialização remota do dispositivo e adição de usuários que terão a função de administrador do controlador de acesso.

Através dessa janela também é possível adicionar dois tipos de **eventos** que geram alarmes: **Desconexão do dispositivo** e **alarme de violação do dispositivo**. Ao criar o evento é possível vincular diversas ações no Defense IA 3.1 (ex: gravação de vídeo, saída de alarme, ação PTZ, entre diversos outros), além de selecionar quais os operadores serão informados.

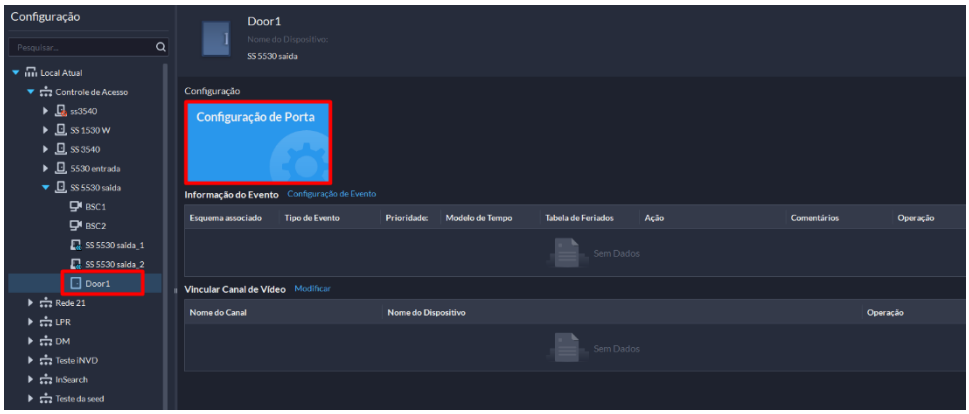


É possível configurar os canais de vídeo do controlador de acesso, vinculando outros canais de vídeo de interesse e adicionando planos de gravação. É possível também configurar diversos eventos de vídeo para o controlador (só são gerados eventos que o dispositivo é compatível. Ex: Se configurado

um evento para mascaramento de vídeo e o dispositivo não tiver esse recurso nenhum evento será gerado).



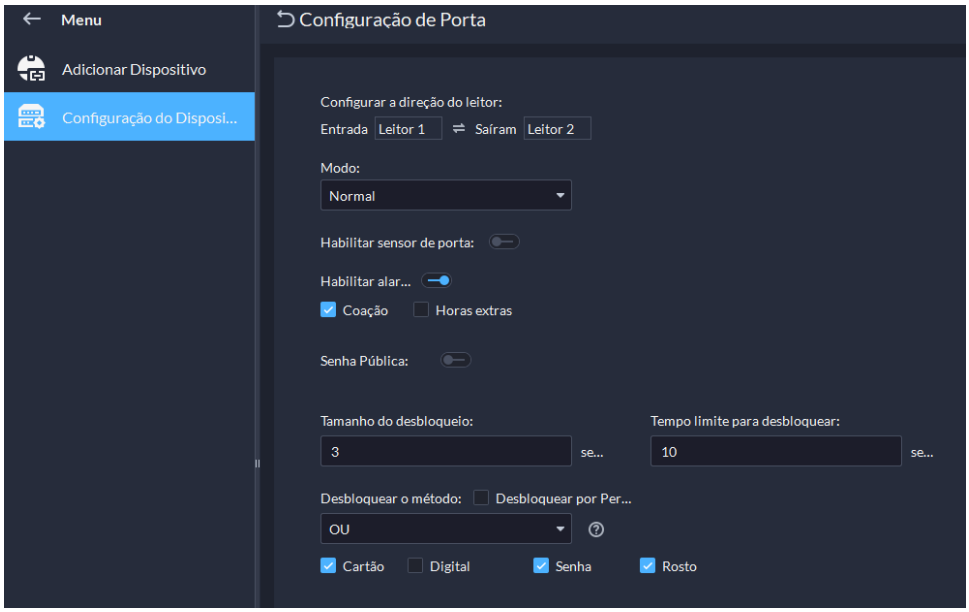
Ao selecionar a porta do controlador de acesso na barra lateral esquerda, novas opções serão disponibilizadas. A primeira delas, na parte superior, são algumas configurações do ponto de acesso específico que se está selecionado.



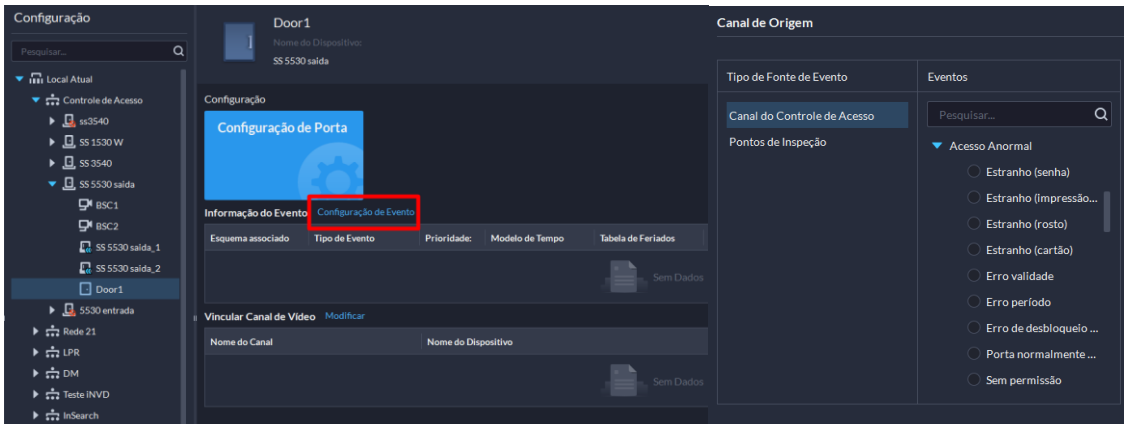
Ao acessar o menu de configuração de porta, as informações abaixo serão listadas, entre elas:

- **Configurar a direção do leitor:** Leitor 1 indica o sentido. Caso desejado que este ponto seja uma saída, configurar o Leitor 1 do lado da opção Saíram.
- **Modo:** Normal, *a porta permanece fechada até haver uma autenticação, depois retorna ao estado fechado.*; Normalmente fechado, *mantém sempre fechado*; Normalmente aberto, *mantém a porta sempre aberta*.
- **Habilitar sensor de porta:** Permite gerar eventos de entrada forçada e de porta aberta por tempo excedente
- **Habilitar alarme:** Permite gerar eventos de coação e de tentativas repetidas de acesso negado.
- **Senha pública:** Ao habilitar o dispositivo irá permitir a abertura com senha pública
- **Tamanho do desbloqueio:** Tempo em que o controlador irá manter a porta aberta após a abertura da mesma

- **Tempo limite para desbloquear:** Tempo em que a controladora aguarda para verificar se a porta foi fechada. Caso a porta permaneça aberta após este tempo será gerado um alarme (se configurado para).
- **Debloqueio por método:** Permite configurar o que o controlador irá exigir como autenticação. Podendo variar entre e/ou cartão, digital, senha e face.
- **Desbloquear por período:** Permite até 4 configurações distintas de métodos de debloqueio por dia.



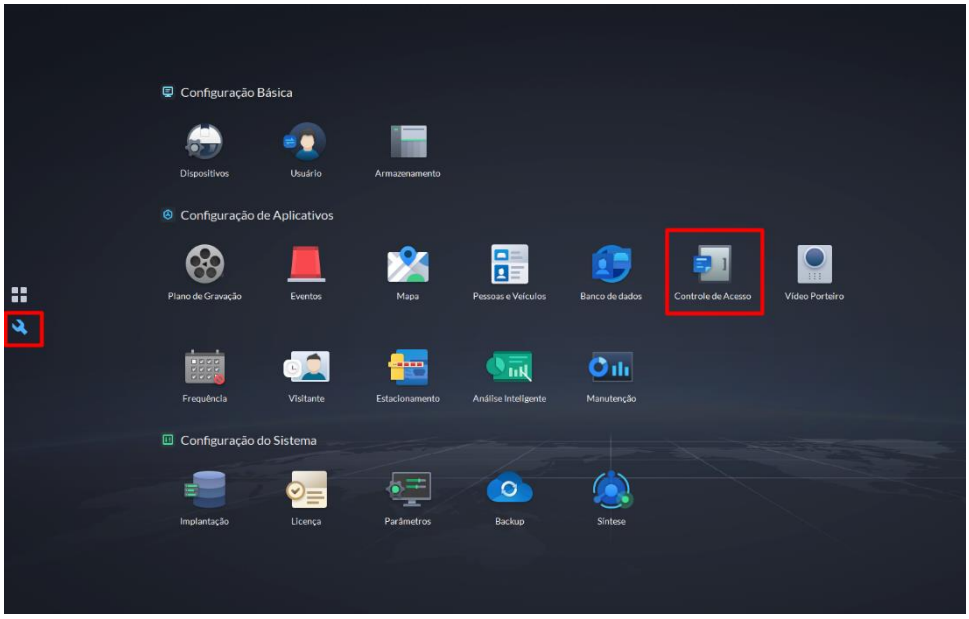
Nas configurações de portas é possível criar eventos relacionados às tentativas de acesso dos usuários. Diversos tipos de eventos podem ser configurados para cada ponto de acesso dos controladores (só são gerados eventos que o dispositivo é compatível. Ex: Se configurado um evento de alarme de senha incorreta e o dispositivo não tiver esse recurso nenhum evento será gerado).



3. Controle de Acesso

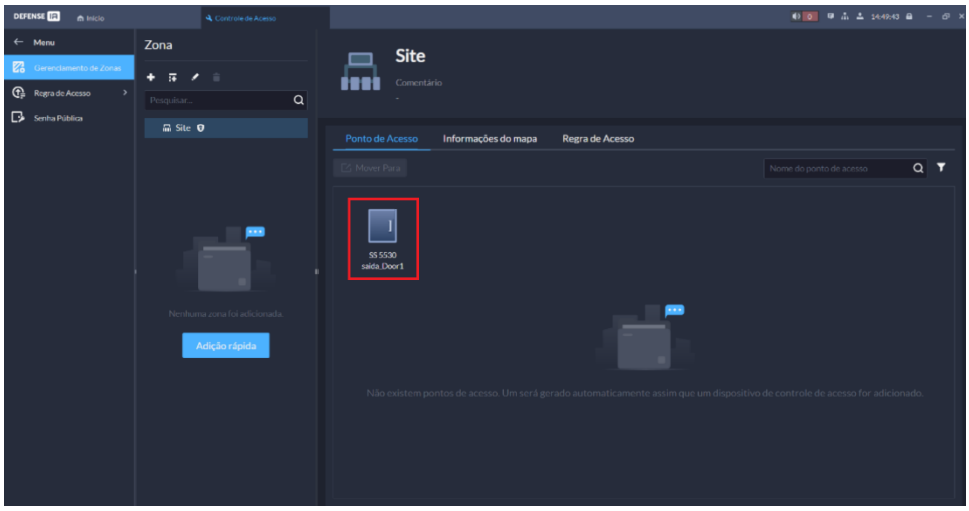
3.1. Configuração de Zonas de Acesso

Para configurar as Zonas de acesso (ambientes), vá para a aba configurações e acesse o menu Controle de Acesso.

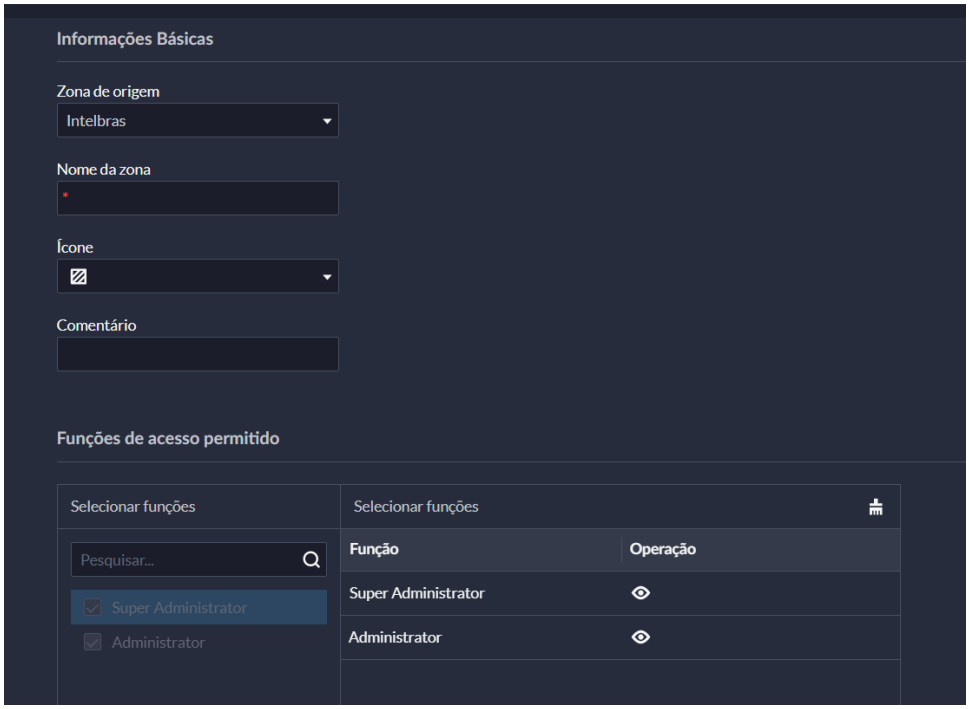


Neste menu temos na primeira aba a esquerda o gerenciamento de **Zonas de acesso**. Estas, **representam o ambiente físico do local**. Os pontos de acesso devem ser vinculados a cada Zona ou Sub-zona correspondente.

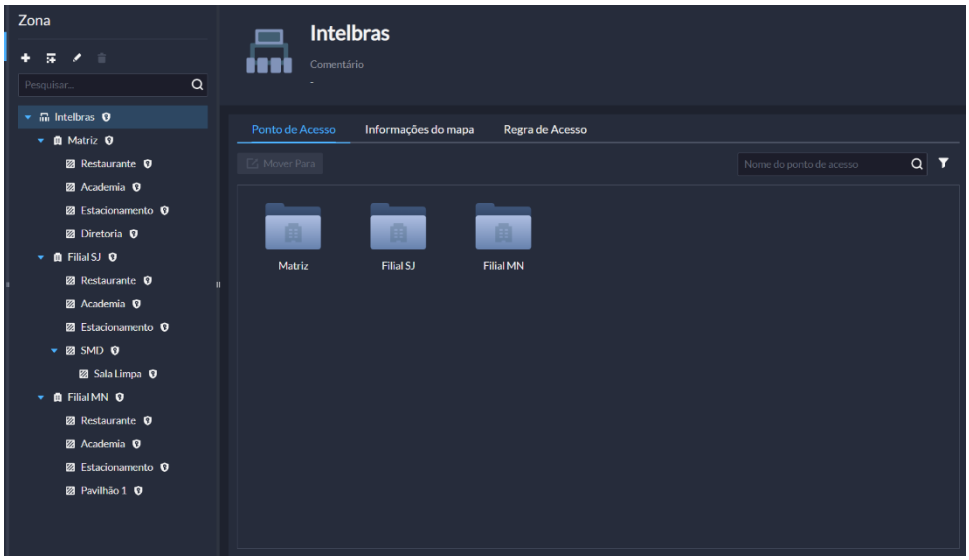
Por padrão, cada novo dispositivo de controle de acesso adicionado, terá os seus pontos de acesso (portas) vinculados ao ambiente raiz. Nesta janela ainda é possível mover cada ponto de acesso a sua respectiva nova zona e/ou também defini-lo como limite (botão direito em cima do ponto de acesso, definir como limite). Definir um ponto de acesso como limite é necessário para as funções de contagem de pessoas por ambiente.



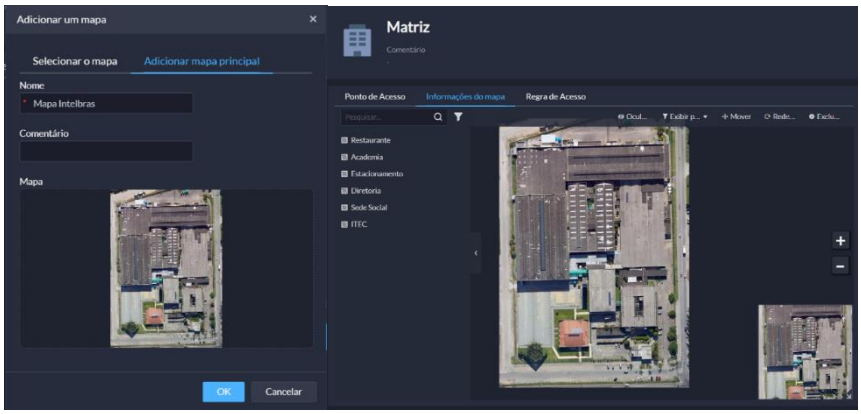
Ao criar uma Zona de Acesso, é necessário dizer qual é a Zona de origem e designar um nome a nova Zona. É possível também adicionar um comentário e vincular quais os perfis de operadores terão permissão de visualizar esta Zona específica (Se um grupo de operadores não for selecionado, eles não poderão visualizar os acessos em tempo real das pessoas que cruzarem pontos de acesso vinculados àquela zona específica nem realizar algumas outras operações).



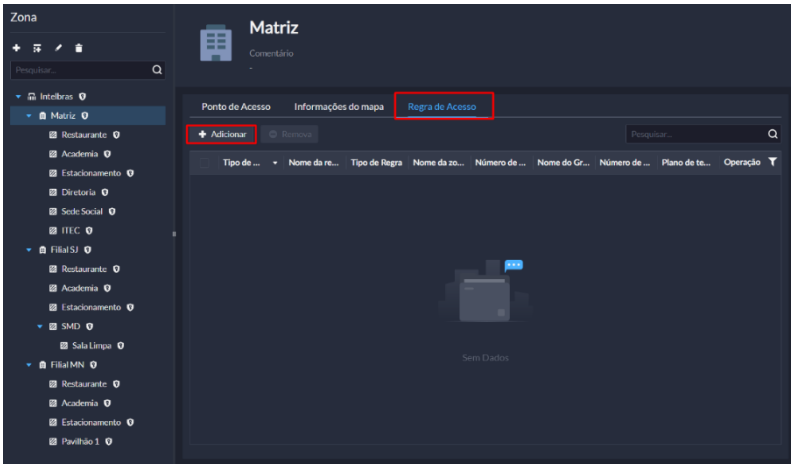
Após criado uma representação física do ambiente em questão, a árvore que organiza os ambientes ficará similar ao da imagem abaixo (barra lateral esquerda).



No gerenciamento de ambientes, é possível adicionar um mapa que represente cada ambiente específico. Neste mapa, pontos de acesso podem ser vinculados para indicar exatamente dentro do mapa onde os acessos estão localizados (este mapa também irá aparecer para o operador na operação de visualização de acessos em tempo real que será explicado adiante).

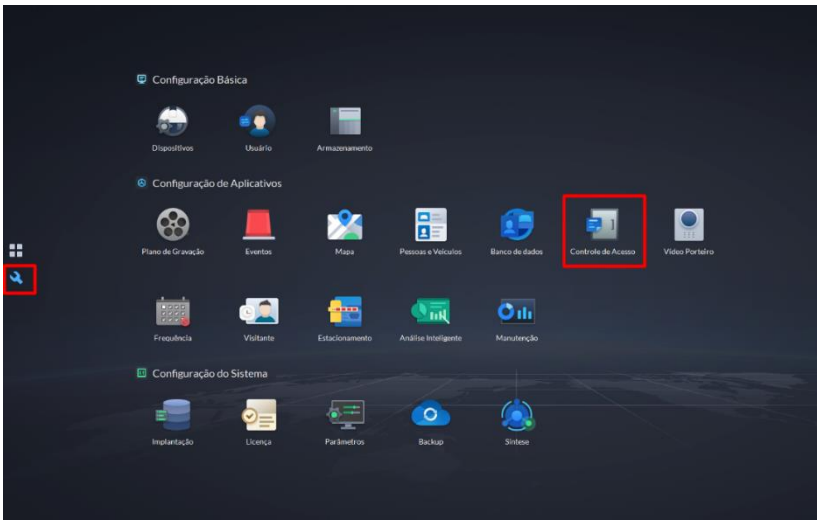


É possível também vincular regras de acesso diretamente a um ambiente (caso alguma pessoa já esteja vinculada a esta regra de acesso, poderá acessar este ambiente em questão).



3.2. Regras de Acesso

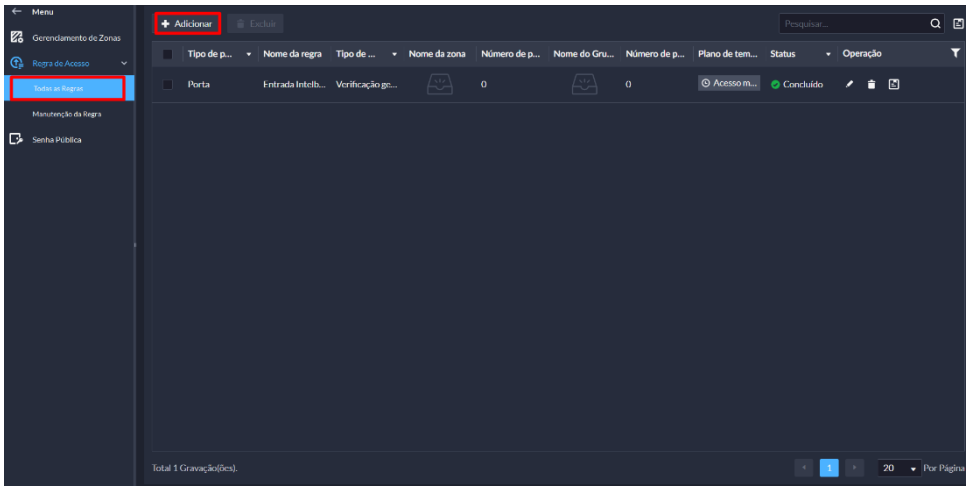
Para acessar as regras de acesso, entre na aba configurações de no menu Controle de Acesso.



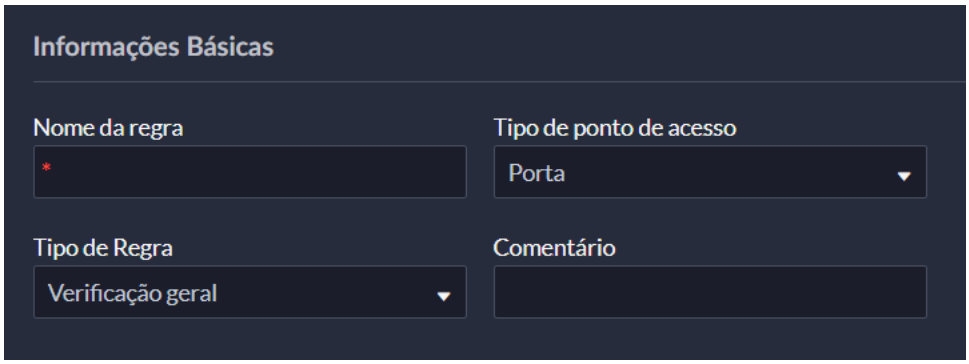
3.2.1. Todas as Regras

Ao acessar o menu Todas as Regras. Será listado as regras de acesso já criadas, sendo possível criar novas regras de Acesso.

Regras de acesso são a base para permitir acesso de pessoas a ambientes (zonas de acesso). É através da regra de acesso que é possível definir **quem**, **onde**, **quando** e de **que modo** poderá realizar acessos.



Ao criar uma nova regra de acesso, algumas informações precisam ser configuradas.



Informações básicas:

- **Nome da regra:** Não pode ser repetido
- **Tipo de ponto de acesso:** porta ou elevador (atualmente a Intelbras tem como produtos correntes apenas dispositivos do tipo porta)
- **Tipo de Regra:** Verificação geral, *Acesso normal, seguindo as regras configuradas na regra de acesso*;

  Normalmente aberto, m*antém um ponto de acesso sempre aberto sem exigir autenticação;*

  Normalmente fechado, *mantém um ponto de acesso sempre fechado mesmo que pessoas tentem se autenticar*;

  Desbloqueio da primeira pessoa, *exige que uma ou mais pessoas configuradas como principal realize o acesso no início do dia para que o restante das pessoas também possam realizar o*

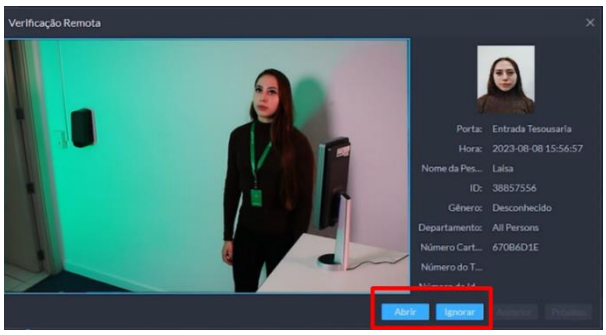
acesso (também é possível configurar para que após o acesso da primeira pessoa o ponto de acesso fique durante o restante do dia sempre aberto;

Desbloqueio de várias pessoas, *possível configurar grupos de múltipla autenticação para abertura de porta. Nestes grupos é possível inserir uma ou mais pessoas para que se exija a autenticação de todas para a abertura da porta (exige no máximo 5 pessoas). Ex: Criado grupo de desbloqueio de várias pessoas com 10 pessoas. Será exigido 5 (ou menos) destas 10 pessoas realizando o acesso para que haja a abertura da porta. Também pode-se criar um grupo com 2 pessoas, será exigido a autenticação destas duas pessoas para a abertura da porta.*

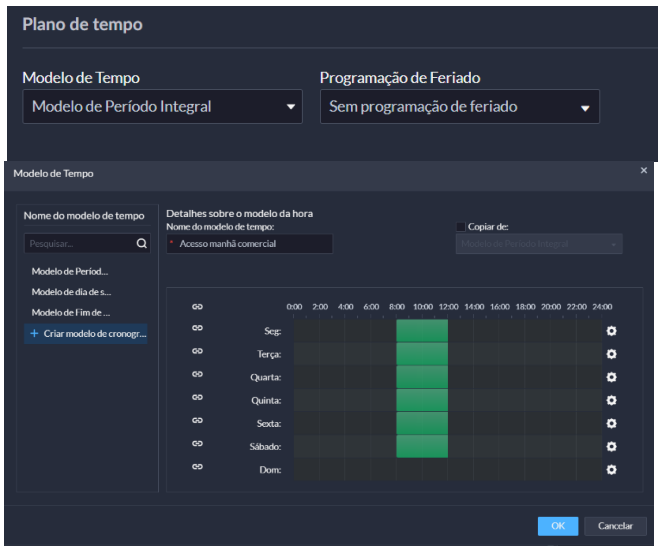
Antipassback, possível criar regra que impede a dupla passagem da mesma pessoa. Necessário para funcionar que seja utilizado apenas em um mesmo dispositivo. Antipassback global necessita de um módulo a parte para funcionamento.

Intertravamento, permite criar um grupo de intertravamento e adicionar diversos dispositivos dentro deste mesmo grupo. Após configuração apenas um dispositivo dentro do grupo poderá ser aberto ao mesmo tempo.

Verificação remota, possível selecionar um ponto de acesso para verificação remota. Após configurado e uma pessoa tente realizar o acesso, uma solicitação será aberta na central de monitoramento para que o operador responsável possa fazer a abertura ou não do ponto de acesso em questão.

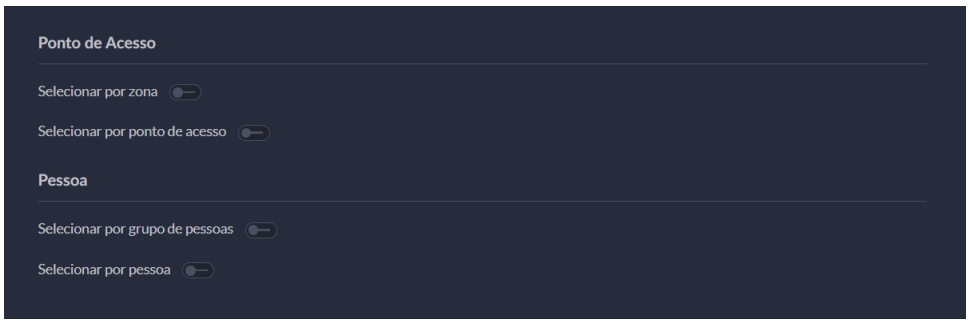


- **Comentário:** Algum comentário para descrever esta regra de acesso



Plano de tempo:

- **Modelo de tempo:** Descreve **quando** as pessoas poderão realizar o acesso quando utilizando esta regra de acesso. É possível criar diversos períodos de tempos configurados para melhor se adaptar aos cenários específicos.
- **Programação de Feriado:** Possível escolher os dias em que mesmo tendo o acesso permitido, as pessoas perderão o acesso neste dia por conta do feriado.



Ponto de Acesso:

- **Selecionar por zona:** Possível vincular a regra de acesso diretamente a certas zonas de acesso. Pessoas que receberem esta regra de acesso posteriormente, poderão acessar as zonas aqui selecionadas.
- **Selecionar por ponto de acesso:** Possível vincular a regra de acesso diretamente a pontos de acesso específicos (uma porta de uma controladora). Desta forma, pessoas vinculadas a esta regra poderão acessar aqueles pontos e acesso aqui selecionados.

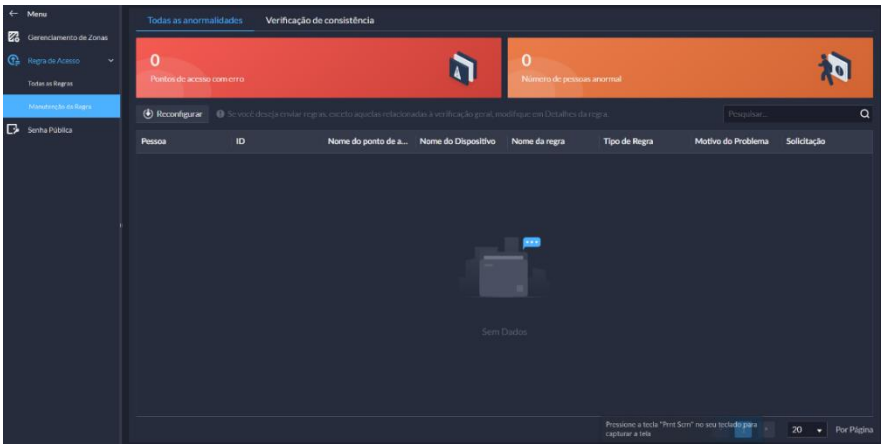
Pessoa:

- **Selecionar por grupo de pessoas:** Vincula a regra de acesso diretamente a um grupo de pessoas, sem precisar posteriormente fazer esta vinculação.
- **Selecionar por pessoa:** Vincula a regra de acesso diretamente a uma pessoa específica. Sem precisar posteriormente fazer esta vinculação.

3.2.2. Manutenção da Regra

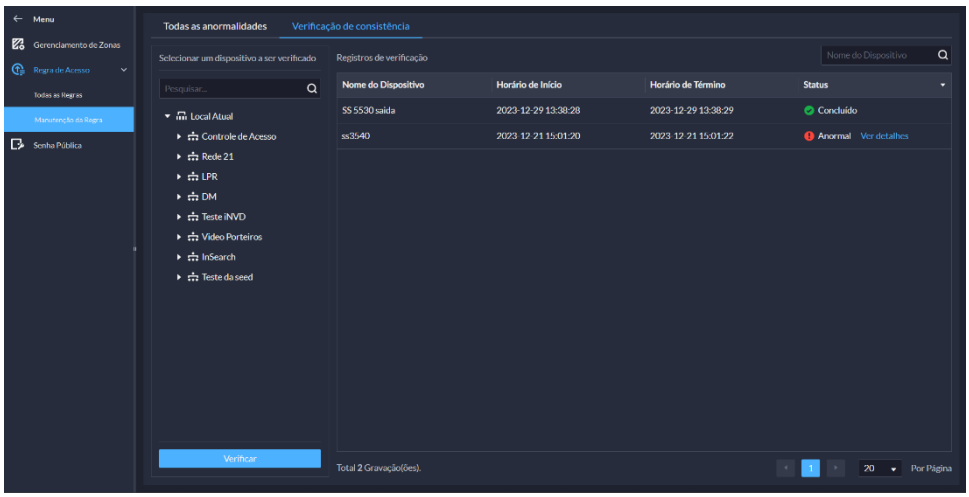
Todas as anormalidades:

Sempre que algum erro na sincronização entre regra de acesso e controlador de acesso ocorra, este será listado aqui. É possível verificar detalhes do erro e tentar sincronizar os cadastros novamente em lote apenas pelo clique de um botão.



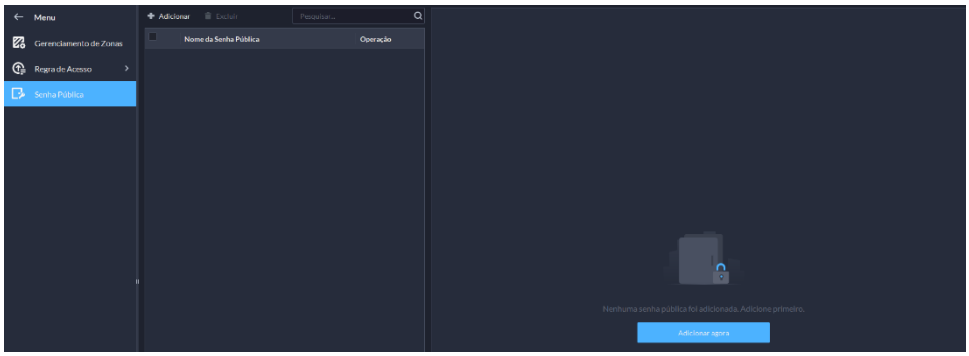
Verificação de Consistência:

Verifica eventos ou cadastros que estão dentro da controladora de acesso e não estão listados no servidor. Ex: Caso alguém seja cadastrado manualmente direto no controlador de acesso, ao utilizar esta função e selecionar o dispositivo específico, será informado que esta pessoa não está cadastrada no Defense IA 3.1.



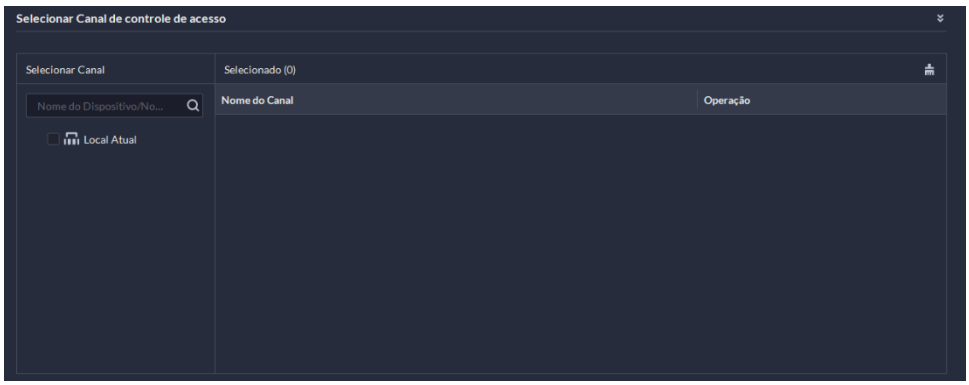
3.3. Senha Pública

Permite que qualquer pessoa que possua a senha pública criada realize o acesso nos controladores de acesso. Necessário habilitar a função de senha pública nos dispositivos de controle de acesso.

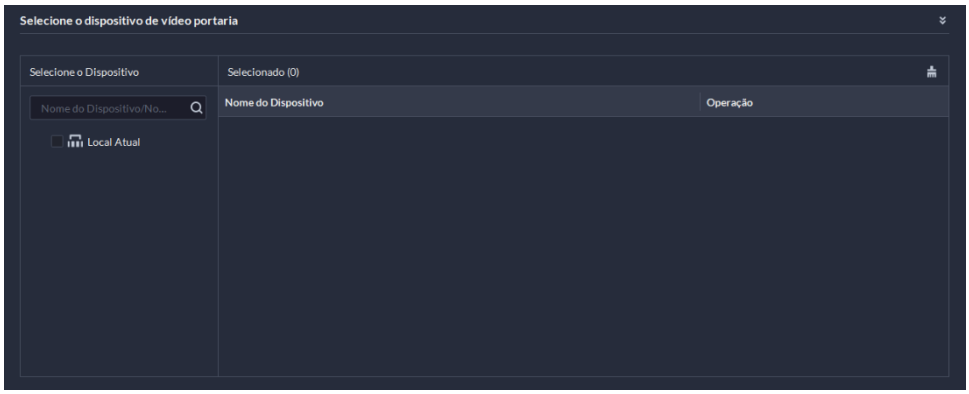


Ao criar uma senha pública, insira um nome para identificação. Insira uma descrição caso desejado e insira qual a senha pública (a senha pública deve conter apenas números e não pode exceder 6 dígitos).

Em seguida, selecione os controladores de acesso disponíveis para vincular a senha pública.

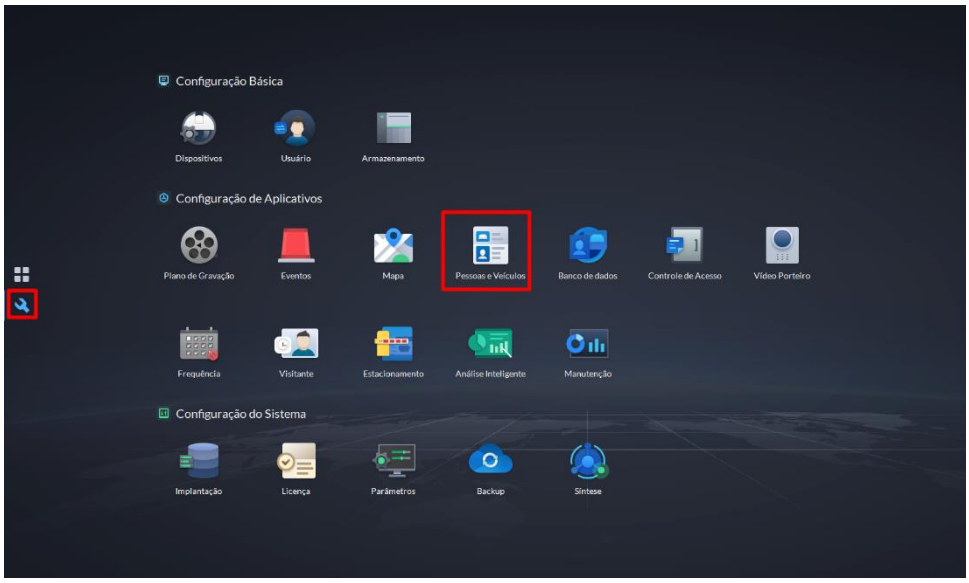


Dispositivos vídeo porteiros também podem ser vinculados para receberem a senha pública para abertura.



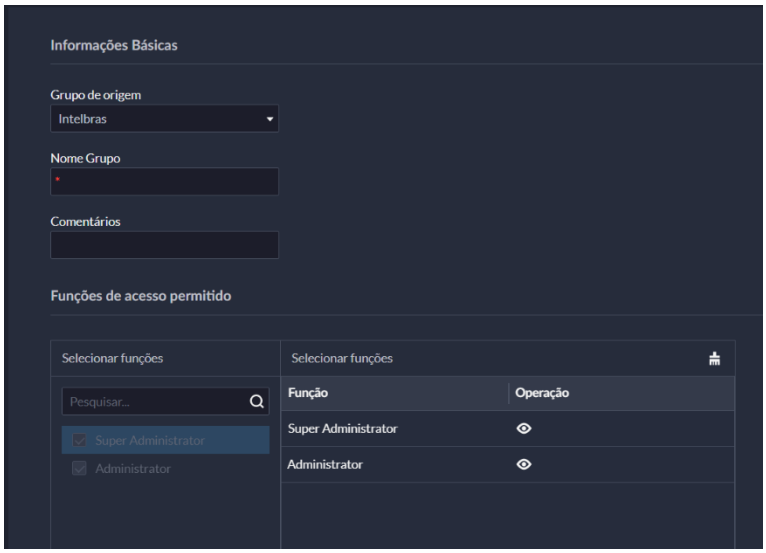
4. Pessoas e veículos

Para acessar o menu pessoas e veículos, vá até a aba configurações e acesse o menu pessoas e veículos.

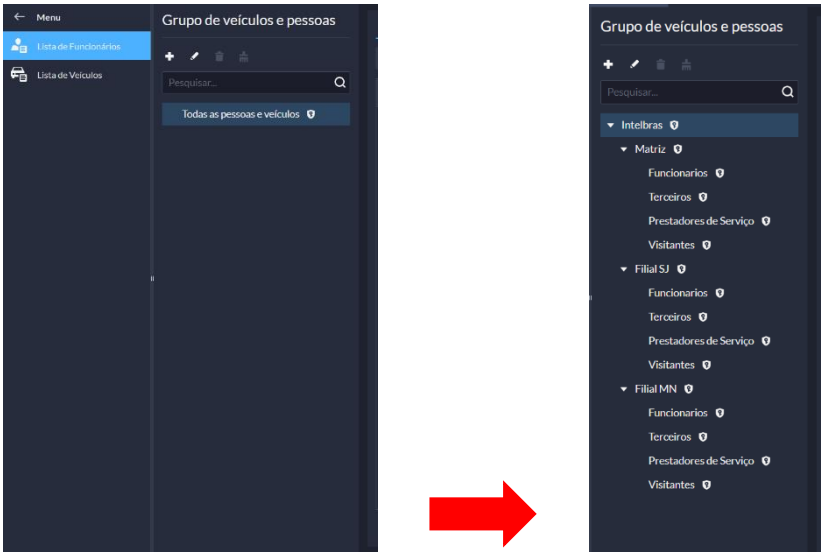


Dentro do menu pessoas e veículos, é possível criar uma árvore organizacional para distribuição dos cadastros realizados. Esta árvore vem apenas com um grupo raiz chamado Todas as pessoas e veículos, mas pode ser configurado para melhor se adaptar ao cenário desejado.

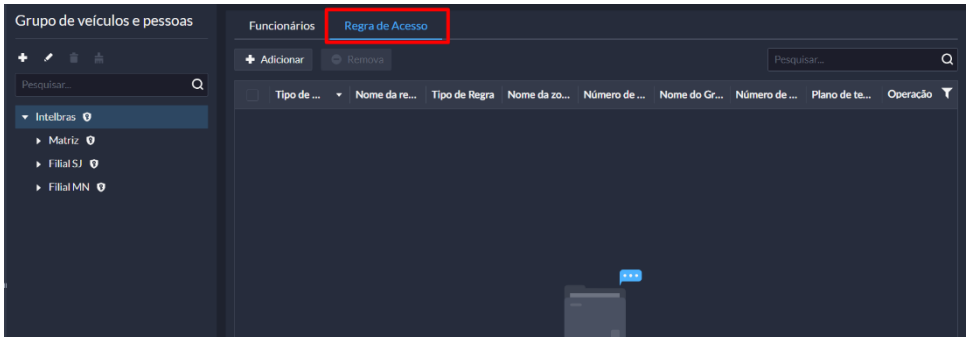
Ao criar um novo grupo de pessoas, é necessário dizer o grupo origem do que está sendo criado (necessário para organizar a árvore de pessoas e veículos). Dar um nome ao grupo de pessoas e veículos e caso desejado, inserir um comentário para o grupo. Também é possível dizer quais grupos de operadores terão acesso aquele grupo de pessoas. **Operadores sem permissão** ao grupo de pessoas **não poderão visualizar as pessoas** daquele grupo específico.



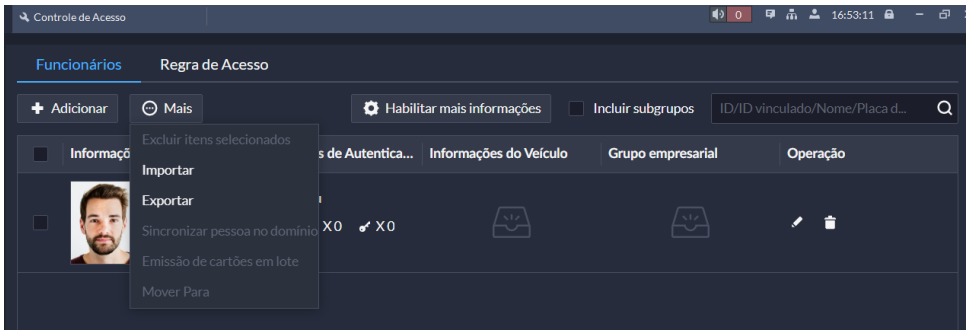
Após a configuração da árvore de pessoas, a disposição irá representar o cenário onde o Defense IA foi instalado.



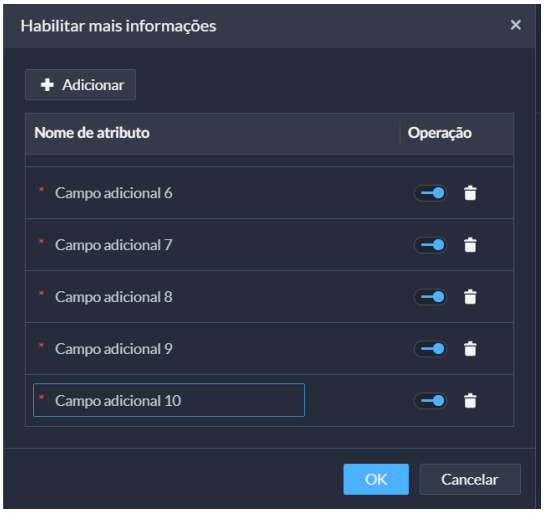
Ainda no gerenciamento do grupo de pessoas e veículos, há uma aba onde é possível vincular uma regra de acesso àquele grupo de pessoas. Ao vincular uma regra de acesso ao grupo, todas as pessoas dentro daquele grupo receberão a regra de acesso, recebendo as suas permissões. Ao remover a regra de acesso do grupo de pessoas, todas perderão aquela regra e o direito de acessar os pontos que antes podiam.



Dentro do gerenciamento de funcionários, também é possível **exportar** e **importar pessoas** para dentro dos grupos de pessoas específicos. Quando importando, será possível fazer o download de um arquivo template modelo, explicando como deve ser preparado o arquivo de importação.

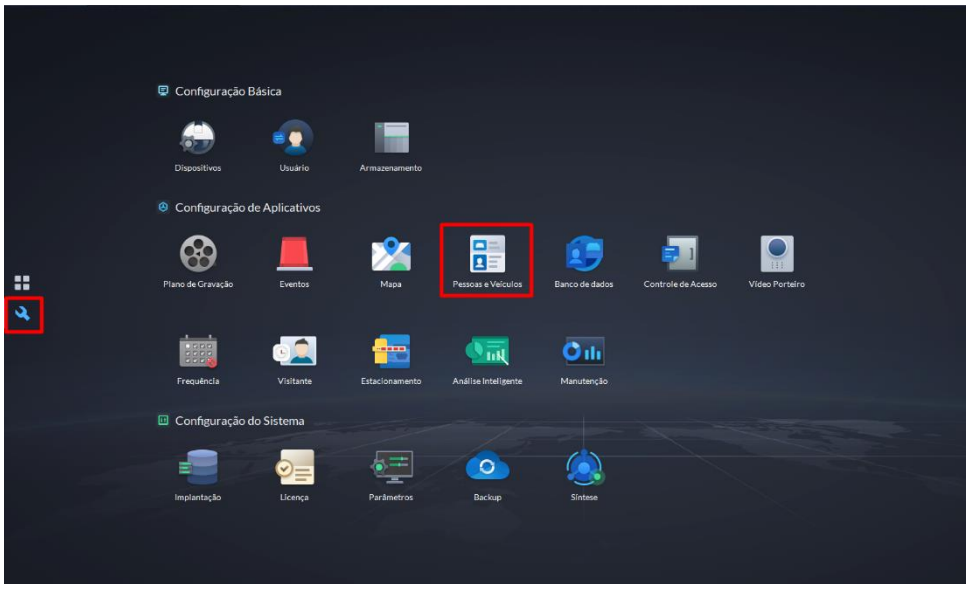


A versão 3.1 do Defense IA traz a nova função de campos adicionais para o cadastro de pessoas. Ao clicar em “Habilitar mais informações” será aberto uma janela onde os campos adicionais poderão ser criados. Esta função permite ao usuário ter campos que melhor representam o local onde o sistema foi instalado.

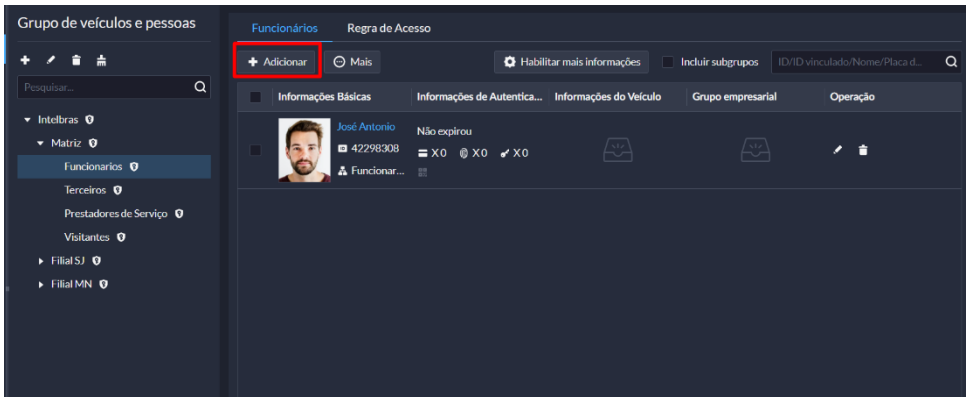


5. Criando cadastro

Para criar um cadastro, vá até o menu Pessoas e veículos, dentro da aba configuração.

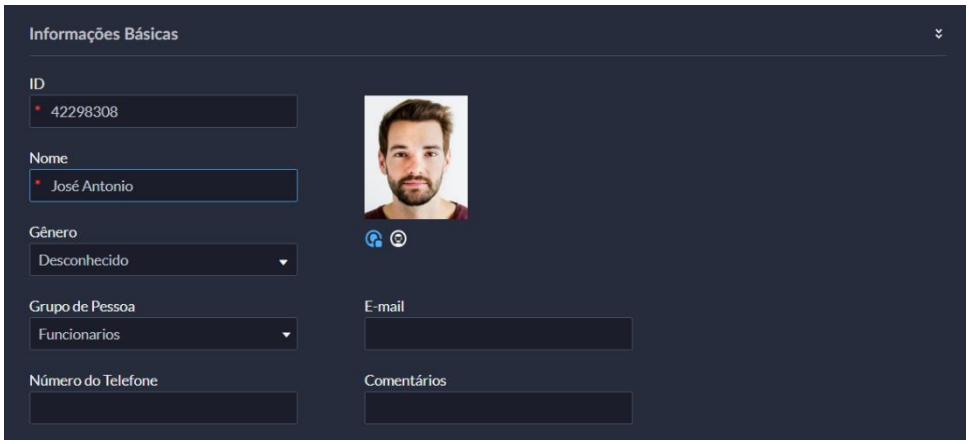


Após selecionar o grupo de pessoas específico, clique em criar novo cadastro.

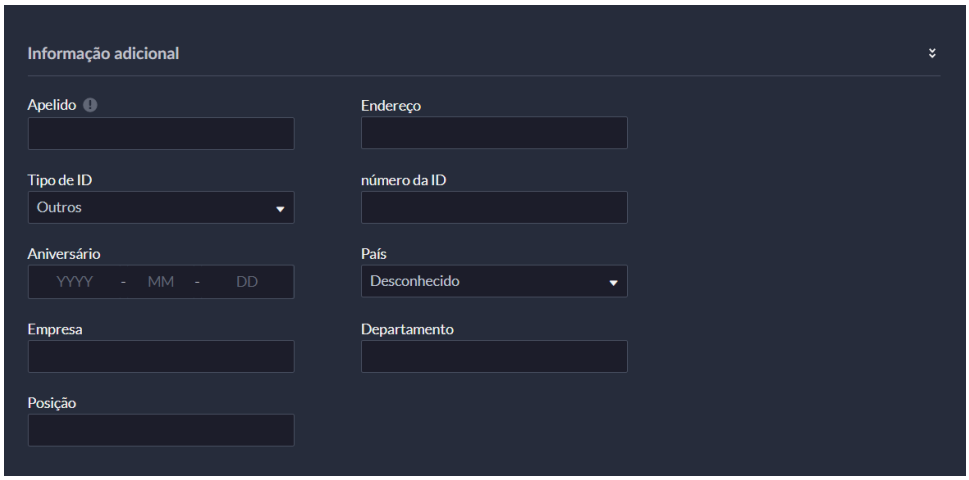


O cadastro de pessoas é dividido em grupos de informação.

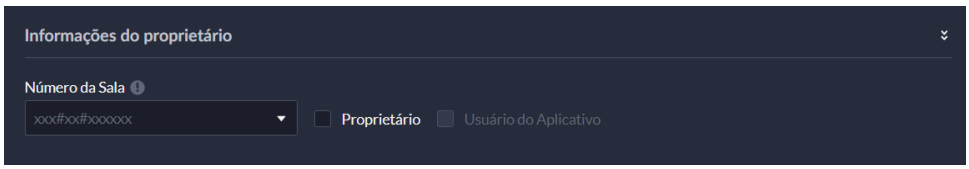
Informações básicas: Informações básicas do cadastro do usuário. A imagem utilizada no perfil será utilizada de forma automática para o reconhecimento facial.



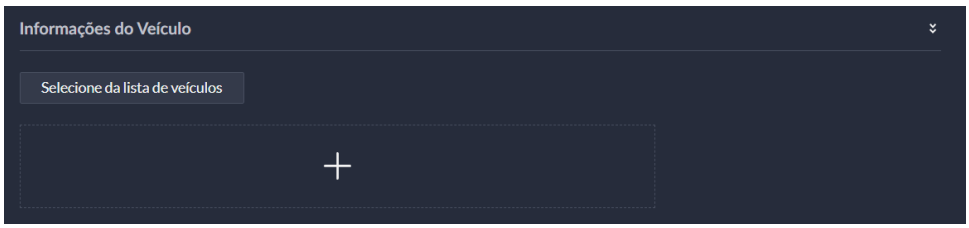
Informações adicionais: Quando configurado os campos adicionais para um cadastro (até 10), estes campos serão exibidos neste espaço.



Informações do proprietário: Utilizado junto a dispositivos de Vídeo Porteiro.

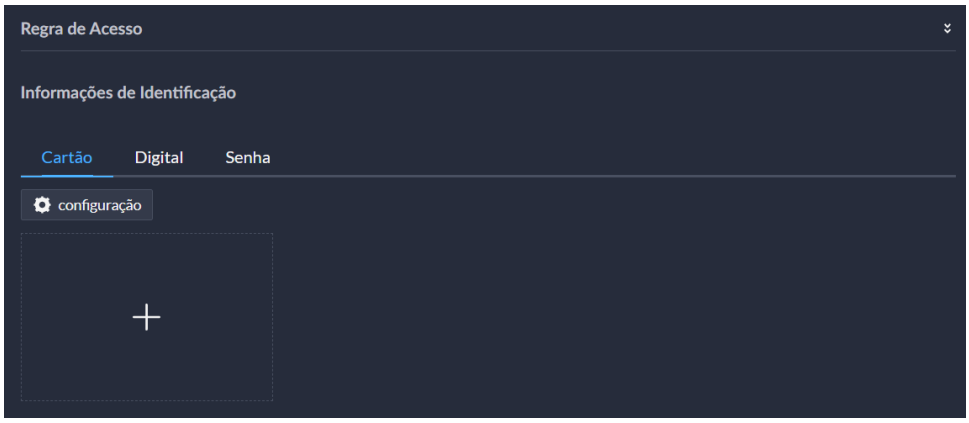


Informações do veículo: Adiciona um veículo a pessoa. Novo ou de uma lista previamente cadastrada.



Regras de Acesso: Possível inserir até 5 cartões a pessoa (um cartão pode ser de coação, gerando alerta no sistema quando utilizado para realizar o acesso), 3 digitais (uma digital pode ser de coação, gerando alerta quando utilizada para realizar o acesso), e 1 senha (a senha quando utlizada para desbloqueio e adicionando um 0 no final funciona como senha de coação gerando alerta no sistema).

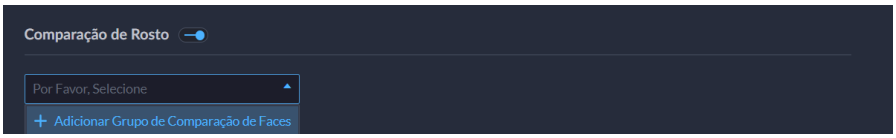
Pode-se utilizar os próprios dispositivos de controle de acesso para coleta do cartão e digital. Ou utilizar um cadastrador de mesa CM-100 (cartões) ou CM-3410 BIO (digitais).



Detalhes da Regra: Onde se vincula a forma de acesso, período de validade e regras de acesso.

- **Tipo de acesso:** Visão Geral, *Tipo de acesso normal*; VIP, *pessoa VIP ignora as regras de acesso (ex: mesmo que seja exigido o acesso apenas com face, o VIP pode utilizar cartão para o acesso, ou acessar em período de acesso diferente);* Visitante, *possuí limite de acesso com créditos de acesso (ao cessar os créditos o visitante perde o acesso)*; Rastreamento, *utilizado para ronda, registra um evento de ronda ao usuário realizar o "acesso").*; Lista negra, *gera um evento de pessoa em lista de bloqueados*; Tempo de acesso estendido, *ao realizar o acesso, mantém a porta aberta por mais tempo para facilitar o acesso de pessoas com limitações de mobilidade*.
- **Período de validade da regra de acesso:** Indica o início e o fim da validade de acesso do cadastro. Ao se exceder, o usuário perderá o acesso.
- **Regra de acesso:** Necessário vincular uma regra de acesso ao usuário. A regra de acesso criada previamente indica **onde**, **quando** e **como** o usuário poderá realizar o acesso em determinados ambientes ou pontos de acesso.

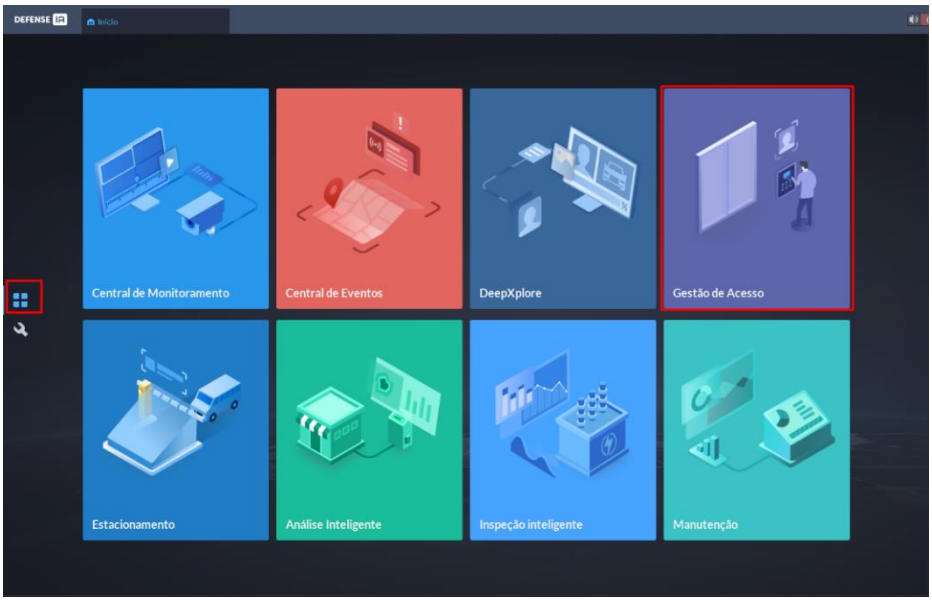
Comparação de Rosto: Possibilita adicionar a pessoa a algum grupo de comparação facial existente. Ao ser adicionada, a face dessa pessoa passa a ser verificada por outros dispositivos de reconhecimento facial do sistema (câmeras, iNVUs).



Grupo de Acesso ao Estacionamento: Define à pessoa cadastrada a quantidade de vagas de estacionamento que esta pode ocupar. Clicando em "Adicionar", vincula a pessoa cadastrada e seus veículos a grupos de veículos. Veja Estacionamento para mais informações sobre como gerenciar grupos de veículos.

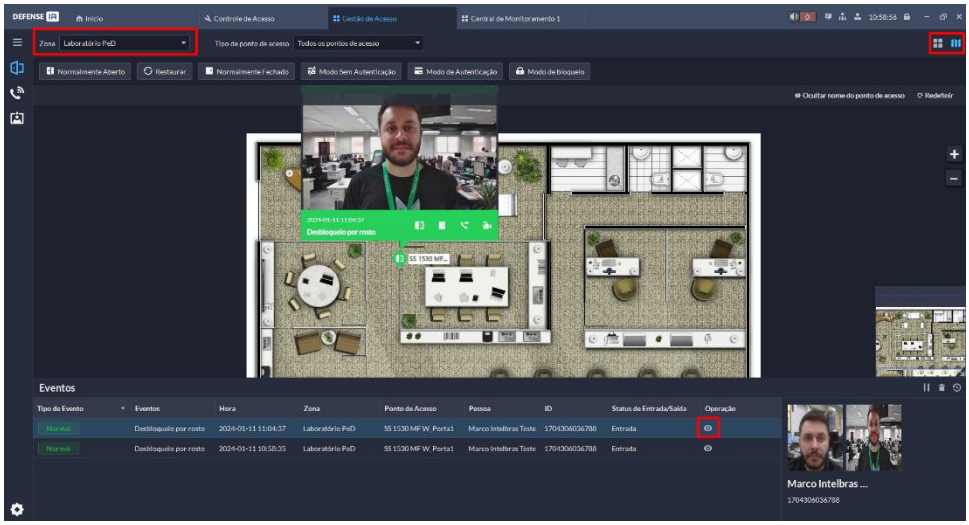
6. Visualização de registros de acesso

Para visualizar os registros de acesso, acesse o menu de operação e Gestão de Acesso.

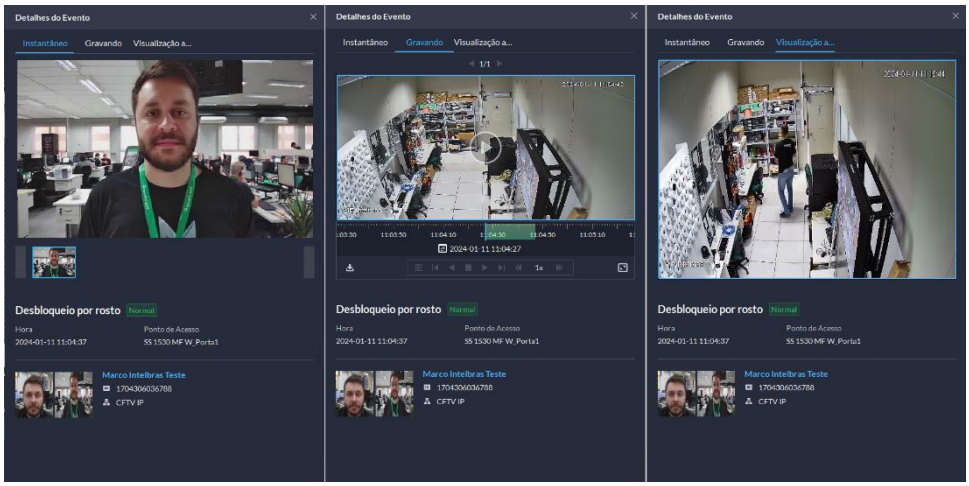


6.1. Registros em tempo real

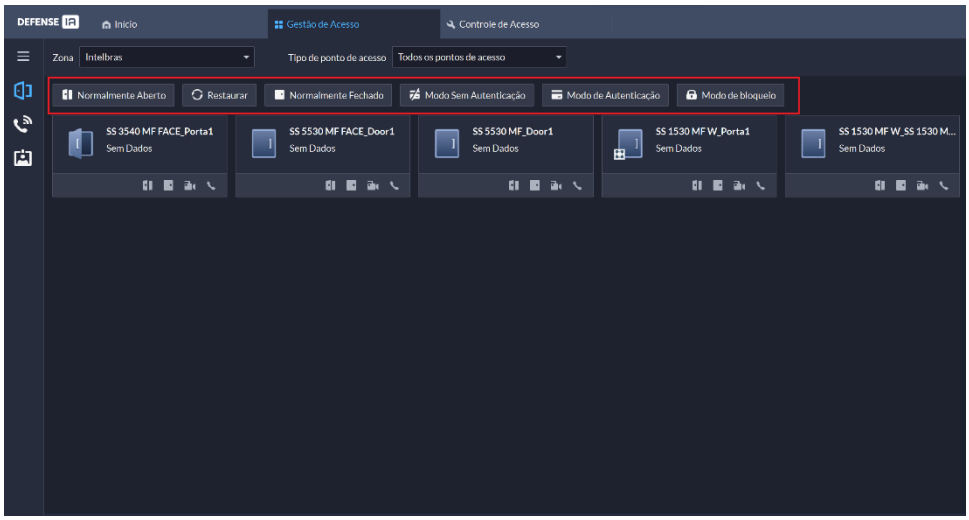
Esta função permite acompanhar de forma dinâmica em tempo real todos os registros de acesso realizados. O modo de exibição permite visualizar o mapa de cada ambiente, visualizando em qual ponto de acesso cada acesso foi realizado. Em cada acesso, uma foto da pessoa é exibida, acessos negados ou alertas também são registrados.



Clicando nos detalhes do registro de acesso ( ) é possível verificar a captura da face no momento acesso, além de uma gravação de uma câmera de contexto e a visualização ao vivo daquele local (caso configurado)



Nesta janela há também uma barra de operações globais. É possível fazer uma abertura global por exemplo em caso de uma evacuação. É possível também manter todos os dispositivos fechados, ou deixar de exigir autenticação para abertura, ou voltar a exigir autenticação e por último manter todos os dipositivos bloqueados sem que se permita o acesso.



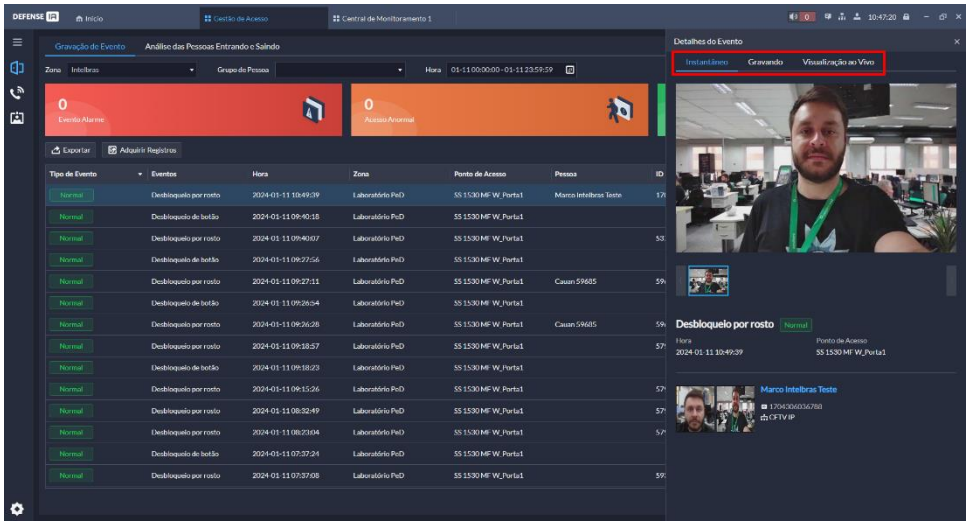
6.2. Registros de acesso

Dentro do menu registros de acesso é possível fazer uma pesquisa de todos os registros dentre um período de 30 dias. Estes registros podem ser filtrados por Zonas e por grupo de pessoas fazendo com que os filtros auxiliem e só tragam os resultados de interesse na busca.

Após a busca ainda é possível exportar o relatório de registros em excel.

Também há a função de aquisição de registros das controladoras de acesso. Esta função é muito útil quando há desconexão entre controlador de acesso e o sistema Defense IA. É possível fazer uma aquisição de registros manual (geral ou por dispositivo específico) ou programado. A programação pode ser agendada para ser feita diariamente a qualquer horário do dia.

Ao selecionar os detalhes do evento é possível visualizar mais informações como a foto do momento, gravação e visualização ao vivo de uma câmera de contexto.

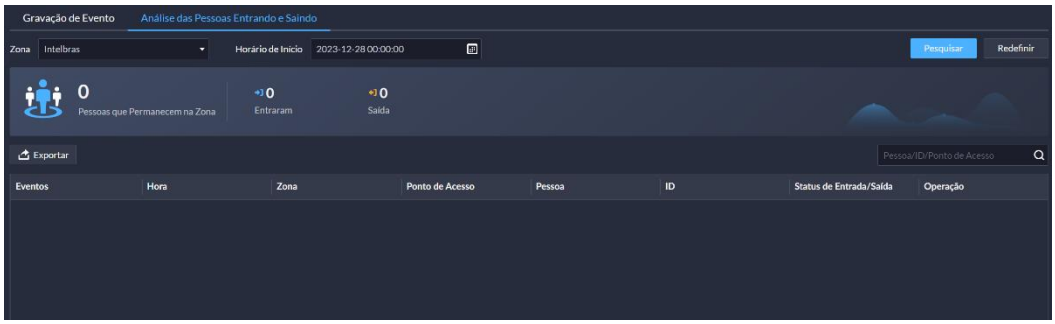


6.3. Pessoas por ambiente

O Defense IA 3.1 agora conta com a função de pessoas por ambiente. Após termos os dispositivos configurados de forma correta (entrada, saída e limite) a função irá começar a funcionar de forma automática.

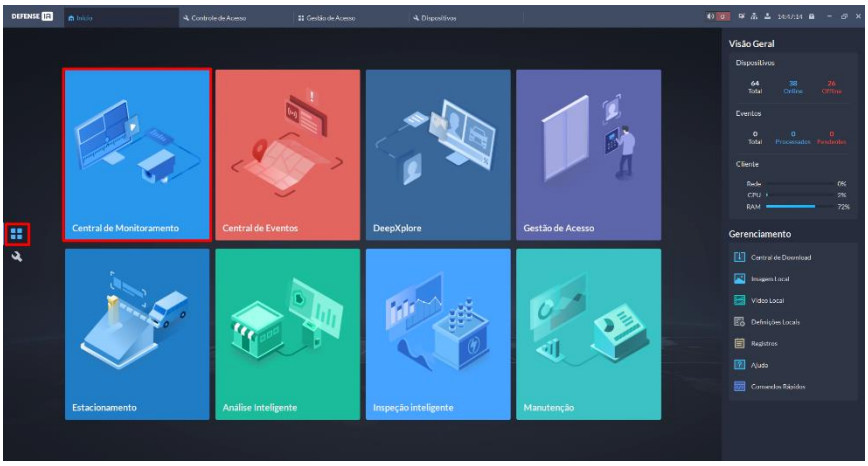
É possível selecionar um ambiente (zona de acesso), um período inicial, e ao buscar o sistema irá retornar quantas pessoas estão dentro do ambiente no momento atual e o número de quantas pessoas (diferentes) fizeram a entrada e saída daquele ambiente em questão. Uma lista será gerada com todos os eventos de entrada e saída.

É possível também exportar o relatório que contém estas informações.



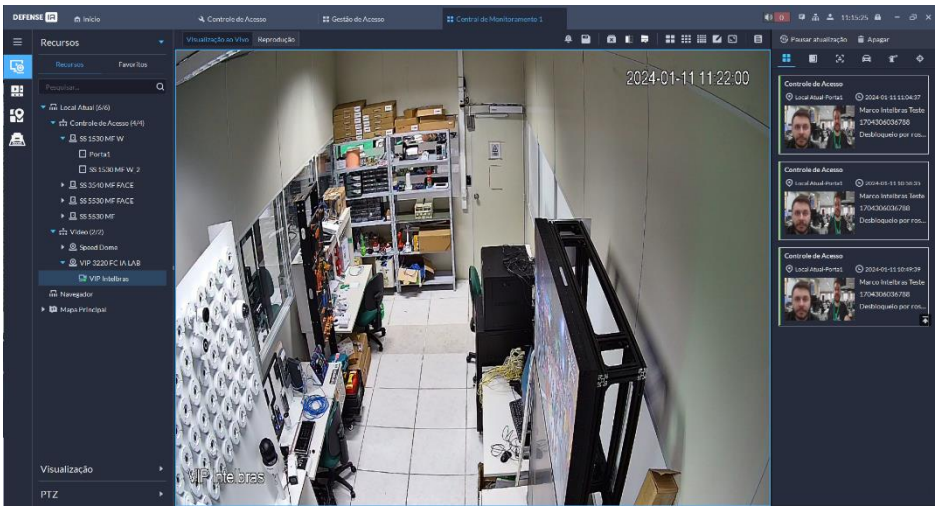
7. Visualização ao vivo

Para acessar a função de visualização ao vivo, vá até a aba de operações e acesse Central de Monitoramento.



Um dos diferenciais do Defense 3.1 é ter a possibilidade de realizar grande parte das operações dentro de uma única janela. Dentro de central de monitoramento é possível visualizar câmeras de vídeo, dispositivos de controle de acesso, video porteiros, LPRs, comando PTZs entre outros.

Se tratando de controle de acesso. É possível abrir o canal de vídeo da controladora ou de uma câmera de contexto para acompanhar o fluxo de pessoas. Nota-se também na barra de notificações na direita, que eventos de acesso são exibidos em tempo real para o operador.



Na visualização do canal de vídeo da controladora. Temos as mesmas funções que um canal de vídeo comum. Além da possibilidade da abertura remota da porta através da própria central de monitoramento, evitando que o operador tenha que se deslocar até outra função para cumprir tal operação.