Manual do Usuário

ZKBio CVAccess

Data: Janeiro, 2024

Versão: 1.0

Português

Obrigado por escolher nosso produto. Por favor, leia atentamente as instruções antes da operação. Siga estas instruções para garantir que o produto esteja funcionando adequadamente. As imagens mostradas neste manual são apenas para fins ilustrativos.

Para obter mais detalhes, visite o site da nossa empresa:

www.zkteco.com.br.

Copyright © 2023 ZKTECO CO., LTD. Todos os direitos reservados.

Marca Registrada

ZKTeco é uma marca registrada da ZKTeco. Outras marcas comerciais envolvidas neste manual são propriedade de seus respectivos proprietários.

Responsabilidade

Este manual contém informações sobre a operação e manutenção dos produtos ZKTeco. Os direitos de propriedade intelectual de todos os documentos, desenhos, etc., em relação aos produtos fornecidos pela ZKTeco são de propriedade da ZKTeco.

O conteúdo deste documento não deve ser usado ou compartilhado pelo receptor com terceiros sem a permissão expressa por escrito da ZKTeco. O conteúdo deste manual deve ser lido na íntegra antes de iniciar a utilização e manutenção do produto adquirido. Se algum dos conteúdos do manual parecer pouco claro ou incompleto, entre em contato com a ZKTeco antes de iniciar a utilização e/ou manutenção do referido produto.

É um pré-requisito essencial para a operação e/ou manutenção corretas/adequadas, que a equipe que irá utilizar e/ou dar manutenção, esteja totalmente familiarizado com o projeto e que esta equipe tenha recebido um treinamento completo da utilização e/ou manutenção da máquina / unidade / produto. É ainda essencial para a utilização segura da máquina / unidade / produto que a equipe tenha lido, compreendido e seguido as instruções de segurança contidas no manual.

Em caso de qualquer conflito entre os termos e condições deste manual e as especificações de fichas-técnicas, desenhos, folhas de instruções ou quaisquer outros documentos acordados entre as partes relacionados ao produto, as condições de tais documentos devem prevalecer em relação ao manual.

A responsabilidade da ZKTeco em relação ao presente manual e ao produto está detalhada nos termos de sua respectiva Garantia.

A ZKTeco reserva-se o direito de adicionar, apagar, alterar ou modificar as informações contidas no manual de tempos em tempos, independente de aviso prévio, por meio de circulares, cartas, notas e/ou novas edições do manual, visando a melhor utilização e/ou segurança do produto.

Os mais recentes procedimentos de utilização e documentos relevantes estão disponíveis em http://www.zkteco.com.br/ sendo de responsabilidade do usuário verificar eventuais atualizações e informes, especialmente se o produto indicar problemas no funcionamento ou se restarem dúvidas sobre sua instalação, manejo, armazenamento, operação e/ou manutenção.

Se houver algum problema relacionado ao produto, entre em contato conosco.

ZKTeco filial Brasil

Endereço Rodovia MG-010, KM 26 - Loteamento 12 - Bairro Angicos - Vespasiano - MG - CEP: 33.206-240.

Telefone +55 31 3055-3530

Para dúvidas relacionadas a negócios, escreva para nós em: comercial.brasil@zkteco.com

Para saber mais sobre nossas filiais globais, visite www.zkteco.com.br.

Sobre a Empresa

A ZKTeco é uma dos maiores fabricantes mundiais de leitores RFID e biométricos (Cartão, Facial, Veia do dedo). As ofertas de produtos incluem leitores e painéis de controle de acesso, câmeras de reconhecimento facial de alcance próximo e distante, controladores de acesso para elevadores/andares, catracas, controladores de portão de Reconhecimento de Placas de Veículos (LPR) e produtos de consumo, incluindo fechaduras de porta com leitor de cartão e reconhecimento facial operadas por bateria. Nossas soluções de segurança são multilíngues e localizadas em mais de 18 idiomas diferentes. Na instalação de fabricação ISO9001 certificada de última geração da ZKTeco, com 700.000 pés quadrados, controlamos a fabricação, o design de produtos, a montagem de componentes e a logística/envio, tudo sob o mesmo teto.

Os fundadores da ZKTeco têm se dedicado à pesquisa independente e ao desenvolvimento de procedimentos de autenticação biométrica e à criação de produtos baseados em SDK de autenticação biométrica, que inicialmente foram amplamente aplicados em segurança de PC e autenticação de identidade. Com o contínuo aprimoramento do desenvolvimento e diversas aplicações de mercado, a equipe gradualmente construiu um ecossistema de autenticação de identidade e um ecossistema de segurança inteligente, ambos baseados em técnicas de autenticação biométrica. Com anos de experiência na industrialização de verificações biométricas, a ZKTeco foi oficialmente estabelecida em 2007 e agora é uma das principais empresas do mundo no setor de autenticação biométrica, detendo várias patentes e sendo selecionada como Empresa Nacional de Alta Tecnologia por 6 anos consecutivos. Seus produtos são protegidos por direitos de propriedade intelectual.

Sobre o Manual

Este manual apresenta as operações do **ZKBioCVAccess.**

Todas as imagens exibidas são apenas para fins ilustrativos. As imagens neste manual podem não ser exatamente consistentes com os produtos reais. Recursos e parâmetros marcados com ★ não estão disponíveis em todos os dispositivos.

Este produto pode conter um ou mais módulos listados abaixo, de acordo com o modelo adquirido por você.

Convenções de Documentos

As convenções usadas neste manual estão listadas abaixo:

Convenções de Interface Gráfica

Para Software	
Padrão	**Descrição**
Bold	Usado para identificar nomes de interface de software. Por exemplo, **OK, Confirmar, Cancelar**.
>	Os menus de vários níveis são separados por esses colchetes. Por exemplo, Arquivo > Criar > Pasta.
Para Dispositivo	
Padrão	**Descrição**
< >	Nomes de botões ou chaves para dispositivos. Por exemplo, pressione <OK>
[ ]	Nomes de janelas, itens de menu, tabela de dados e nomes de campos estão entre colchetes. Por exemplo, abra a janela [Novo usuário]
/	Os menus de vários níveis são separados por barras de encaminhamento. Por exemplo, [Arquivo / Criar / Pasta].

Símbolos

Padrão	Descrição
	Implica sobre o aviso ou para ter atenção, no manual
	Informações gerais que ajudam a realizar as operações mais rapidamente
	Informação importante
	Cuidado para evitar perigos ou erros
	Declaração ou evento que avisa sobre algo ou que serve como um exemplo de advertência

Índice

1 Introdução

Atualmente, a preocupação das empresas modernas com a segurança aumentou rapidamente. Para alcançar isso, a ZKTeco traz para você o ZKBio CVAccess, que ajuda os clientes a integrar as operações de controle de acesso e frequência em uma única plataforma. O sistema é dividido em quatro módulos, a saber: Pessoal, Acesso, Frequência e Gestão de Sistemas.

Recursos:

- Pode gerenciar cerca de 6.000 dados de pessoal.
- Possui uma capacidade poderosa de processamento de dados.
- Os dados dos usuários são mais seguros com gerenciamento em vários níveis baseados em funções.
- Pode rastrear eventos e operações em tempo real para garantir feedbacks adequados dos dados para a administração.

Requisitos de Configuração:

- Processador dual-core com velocidade de 2,4GHz ou superior.
- Memória do sistema de 4GB ou superior.
- Espaço disponível de 10GB ou superior. Recomendamos usar a partição de disco rígido NTFS como diretório de instalação do software.
- Resolução do monitor de 1024 x 768px ou superior.

Sistema Operacional:

- Sistemas Operacionais Suportados: Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11 / Windows Server 2008/2013 (32/64).
- Banco de Dados Suportado: PostgreSQL.
- Versão do Navegador Recomendada: IE 11+/Firefox 27+/Chrome 33+/Edge.

1.1 Módulo de Pessoal

O módulo de Pessoal é usado para configurar os detalhes das pessoas e seus departamentos. Ele consiste principalmente em duas partes: Configurações de Gerenciamento de Departamento, usadas para definir o organograma da empresa; Configurações de Gerenciamento de Pessoal, usadas para adicionar informações pessoais, atribuir departamentos, manter e gerenciar detalhes pessoais.

1.2 Módulo de Controle de Acesso

O módulo de Controle de Acesso é um sistema de gerenciamento baseado na web que permite funções normais de controle de acesso, gerenciamento de painéis de controle de acesso interconectados via computador e gerenciamento unificado de acesso pessoal. O sistema de controle de acesso define o tempo de abertura de portas e os níveis para os usuários registrados.

1.3 Módulo de Frequência

O Módulo de Frequência consiste em gerenciamento de horários, turnos e escalas, gerenciamento de frequência inter-regional. Você também pode gerenciar outras exceções como faltas, atrasos, horas extras etc. Ao mesmo tempo, o controle de acesso pode ser configurado juntamente com o gerenciamento de frequência para gerar registros de frequência.

1.4 Módulo de Visitantes

O Módulo de Visitantes oferece um sistema completo para gerenciar visitas e reservas. Com ele, é possível realizar o check-in e check-out dos visitantes, definindo quais portas eles podem acessar e por quanto tempo terão esse acesso. Além disso, o módulo inclui funcionalidades de vinculação que permitem enviar um QR Code de acesso ou outras informações relevantes por e-mail tanto para o visitante quanto para o anfitrião.

1.5 Módulo de Vigilância por Vídeo Inteligente

O Módulo de Vigilância por Vídeo Inteligente pode ser usado em conjunto com NVR, dispositivo IPC, como uma plataforma de gerenciamento de vídeo profissional, ele pode alcançar funções como pré-

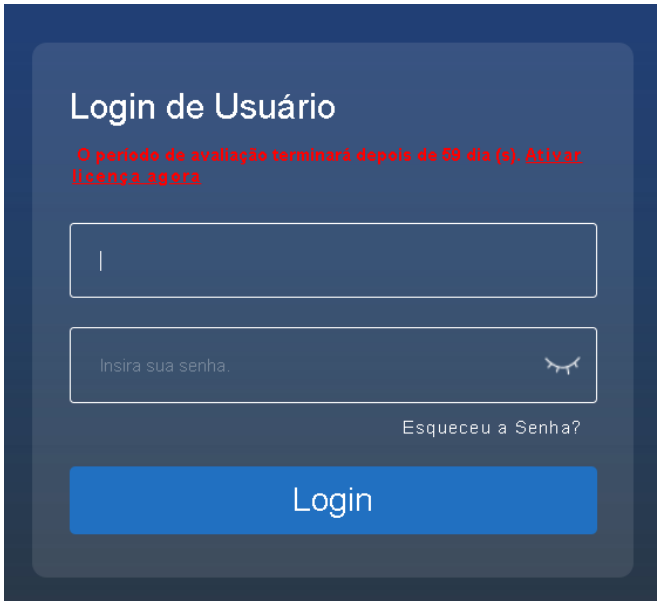
visualização, reprodução, exibição de parede de vídeo, configuração de mapa, configuração inteligente, patrulha de vídeo, intercomunicador visual, estatísticas e relatórios de alarme, e outras características de gerenciamento.

1.6 Módulo de Gerenciamento de Sistema

O Gerenciamento de Sistema é principalmente usado para atribuir usuários do sistema e configurar os papéis dos módulos correspondentes, gerenciar bancos de dados como backup, inicialização e recuperação, e definir parâmetros do sistema e gerenciar os registros de operação do sistema.

2 Operações do Sistema

2.1 Login



Após instalar o software, clique duas vezes no ícone do ZKBio CVAccess para abrir o software. Você também pode abrir o navegador recomendado e inserir o endereço IP e a porta do servidor na barra de endereços. O endereço IP padrão é http://127.0.0.1:8098. Se o software não estiver instalado em seu servidor, você pode inserir o endereço IP e a porta do servidor na barra de endereços.

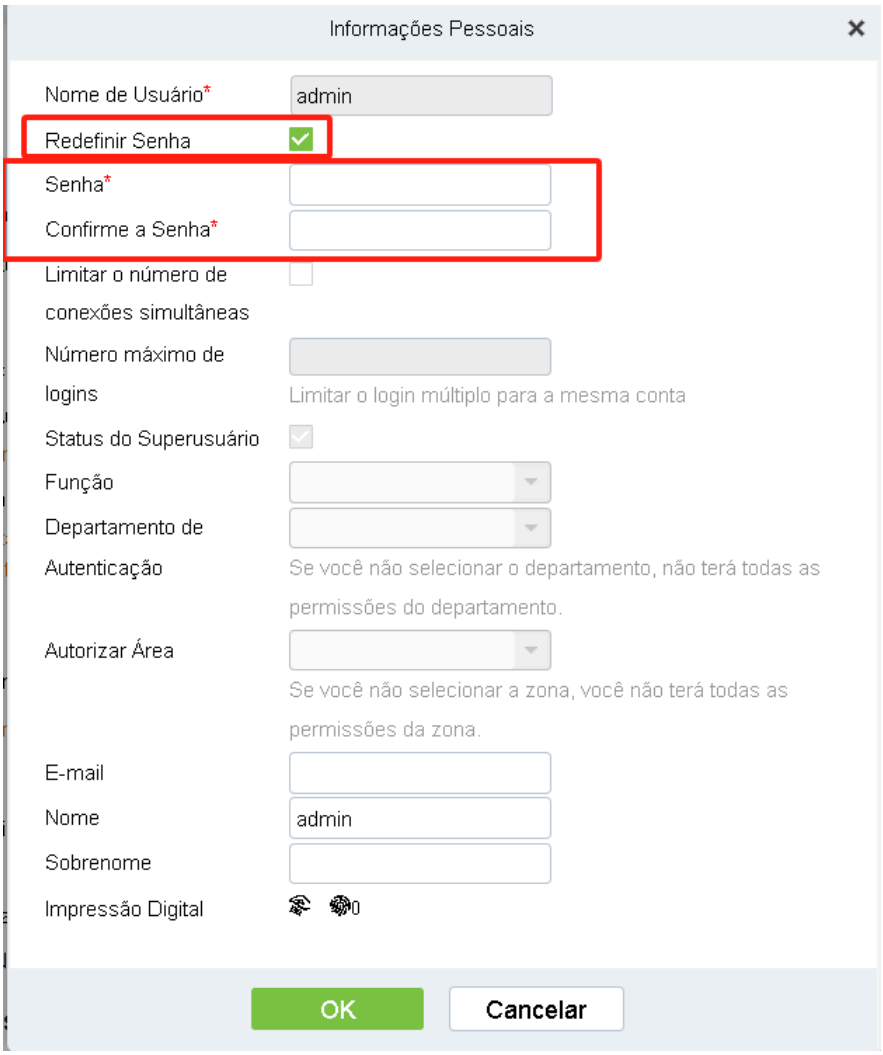
Observação: O nome de usuário do superusuário **é [admin]**, e a senha é **[admin]**. Em seguida, clique em **[Login]**. Após fazer o login pela primeira vez, você precisará redefinir sua senha.

2.2 Ativar o Sistema

Consulte o documento de ativação de licença correspondente.

2.3 Modificar Senha

Você pode modificar a senha de login em **[Informações Pessoais]**. Clique na imagem do perfil no canto superior direito.



Selecione a caixa de seleção **[Redefinir Senha]** para modificar a senha.

Observação: Tanto o Superusuário quanto o novo usuário são criados pelo superusuário (a senha padrão para os novos usuários é 111111). O nome de usuário não diferencia maiúsculas de minúsculas, mas a senha é sensível a maiúsculas e minúsculas.

2.4 Sobre

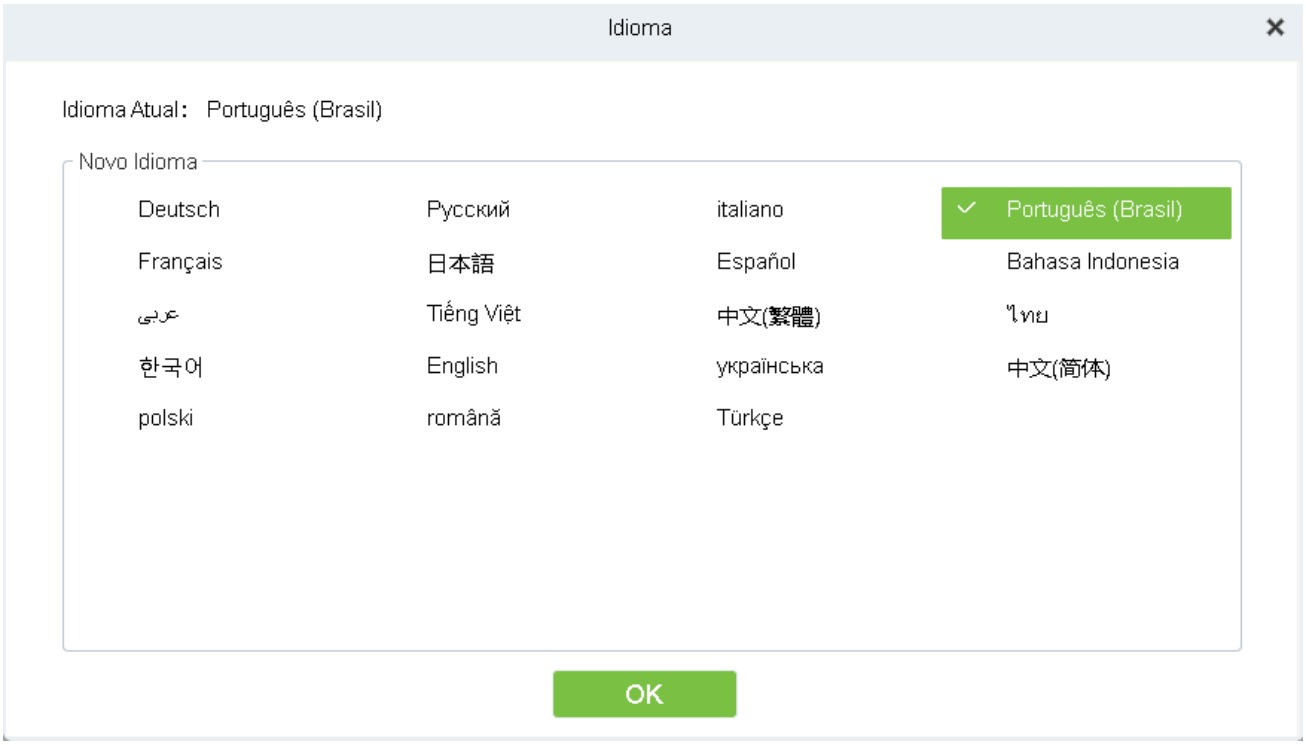
Clique no botão **[Sobre]** no canto superior direito da interface para verificar todas as informações sobre a versão do software e a licença.

2.5 Ajuda

Clique no botão **[Ajuda]** no canto superior direito da interface para visualizar o manual do usuário.

2.6 Idioma

Clique no botão **[Idioma]** no canto superior direito da interface para alternar o idioma.

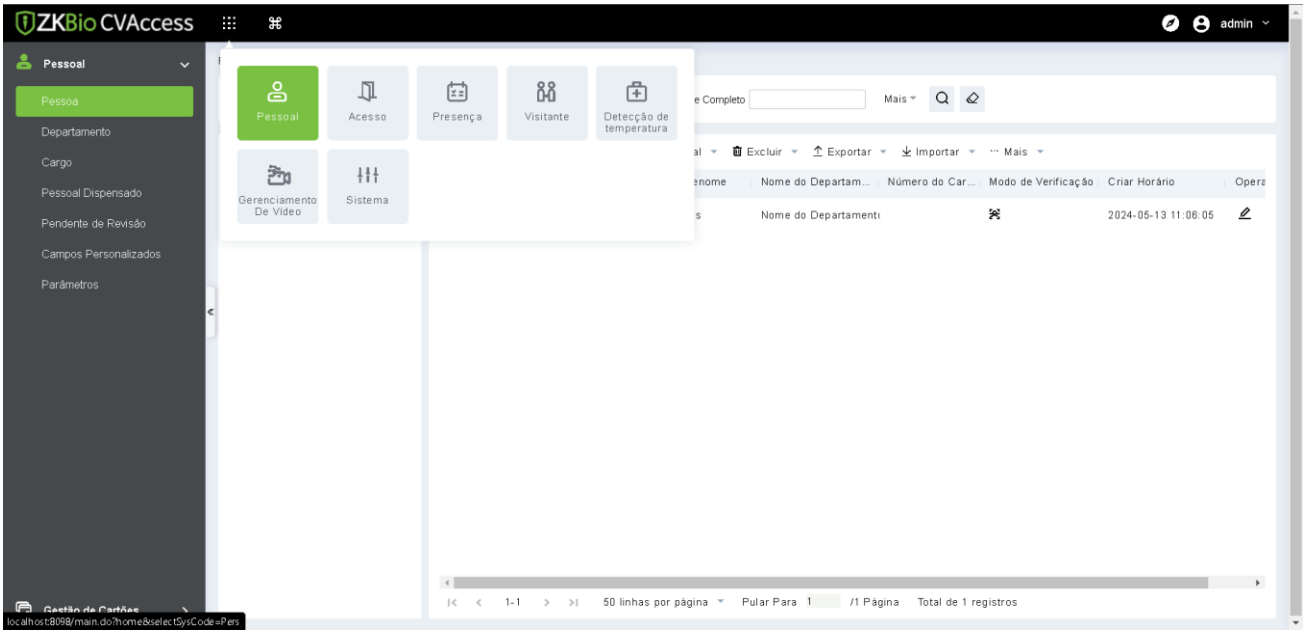


2.7 Sair do Sistema

Clique no botão [Logout] no canto superior direito da interface para sair do sistema.

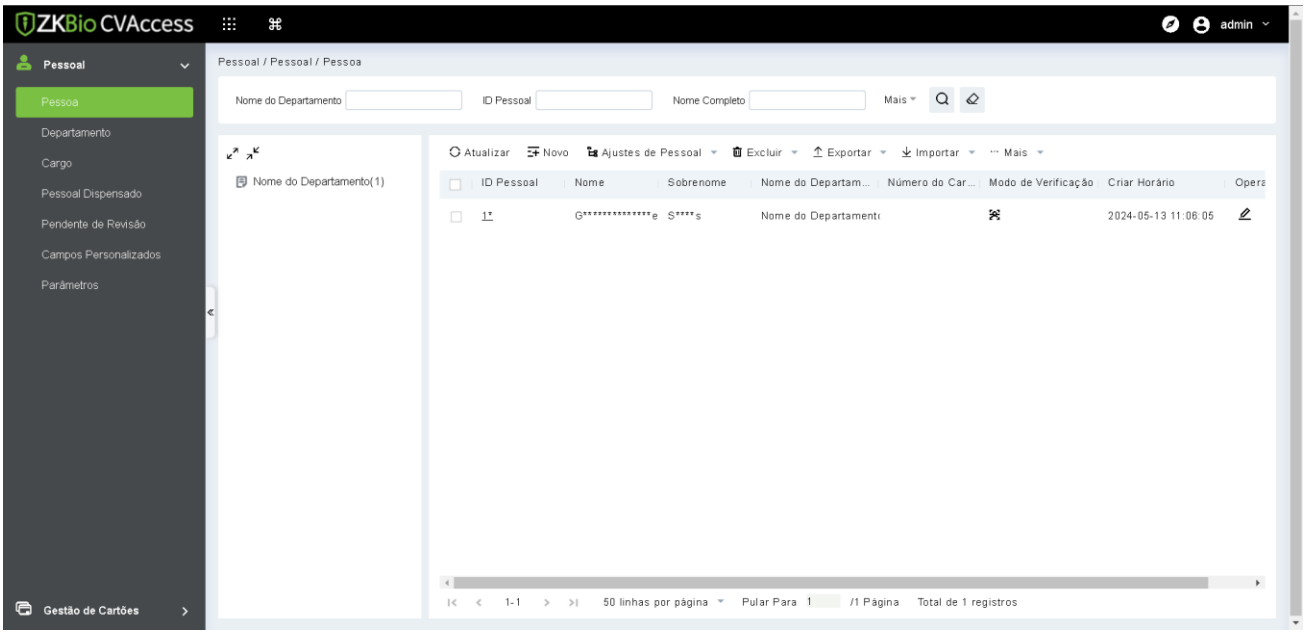
3 Pessoal

Você pode configurar o Gerenciamento de Pessoal e o Gerenciamento de Cartões neste módulo.



3.1 Gerenciamento de Pessoal

O gerenciamento de pessoal inclui estes módulos: Pessoal, Departamento, Cargo, Pessoal Demitido, Revisão Pendente, Atributos Personalizados e Parâmetros.

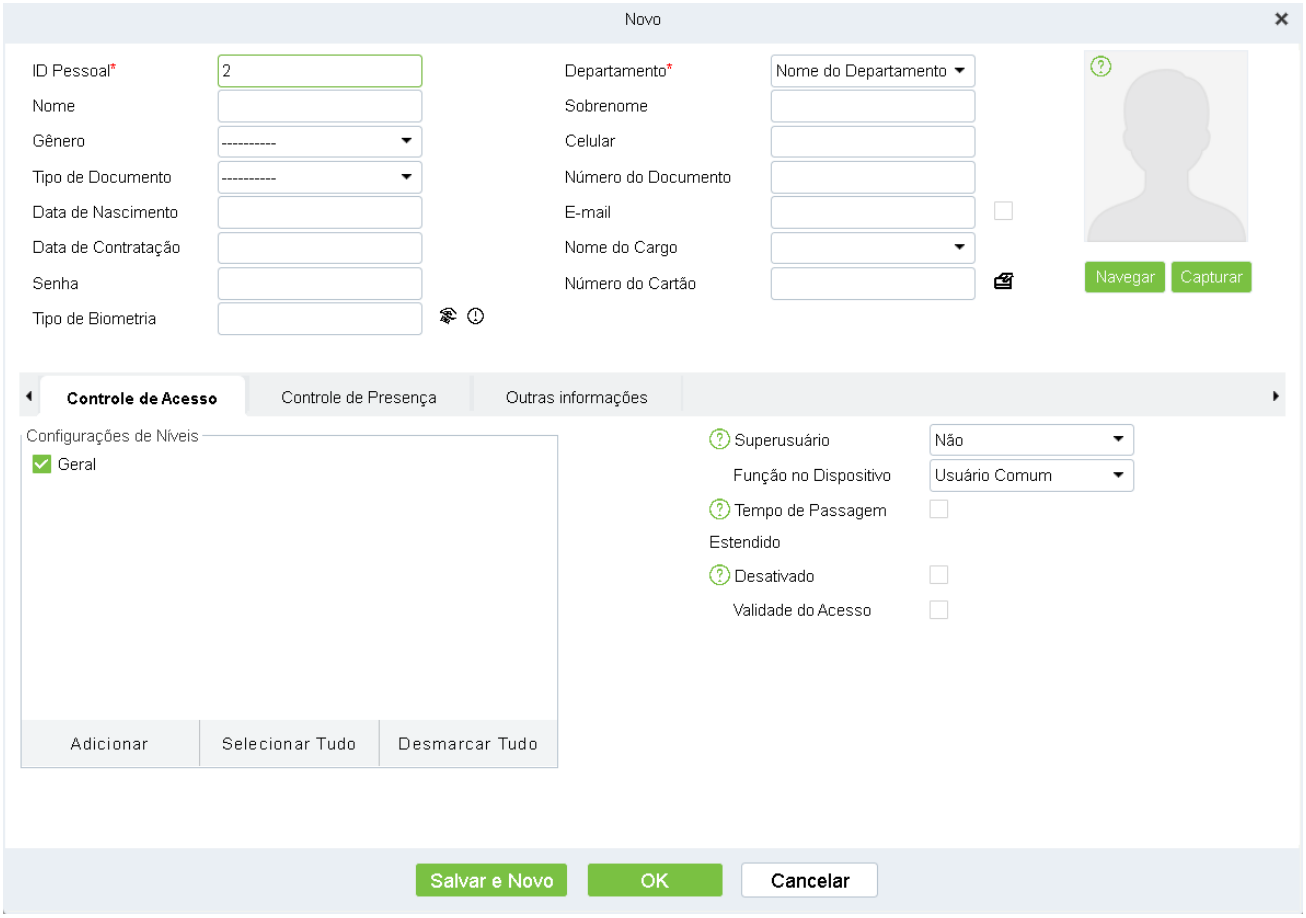


3.1.1 Pessoal

Ao usar este gerenciamento, o usuário deve registrar o pessoal no sistema ou importar as informações de pessoal de outro software ou arquivo para este sistema. Para detalhes, consulte Operações Comuns. As principais funções do Gerenciamento de Pessoal incluem Adicionar, Editar, Excluir, Exportar e Importar pessoal, e Ajustar Departamento.

3.1.1.1 Adicionar Pessoal

Clique em [**Gerenciamento de Pessoal**] > [**Pessoal**] > [**Novo**].



Os campos são os seguintes:

- **ID Pessoal:** Um ID pode ter até 9 caracteres, dentro da faixa de 1 a 79999999. Pode ser configurado conforme suas necessidades. O ID do Pessoal contém apenas números por padrão, mas também pode incluir letras.

Notas:

Ao configurar um número de pessoal, verifique se o dispositivo atual suporta o comprimento máximo e se letras podem ser usadas no ID do Pessoal.

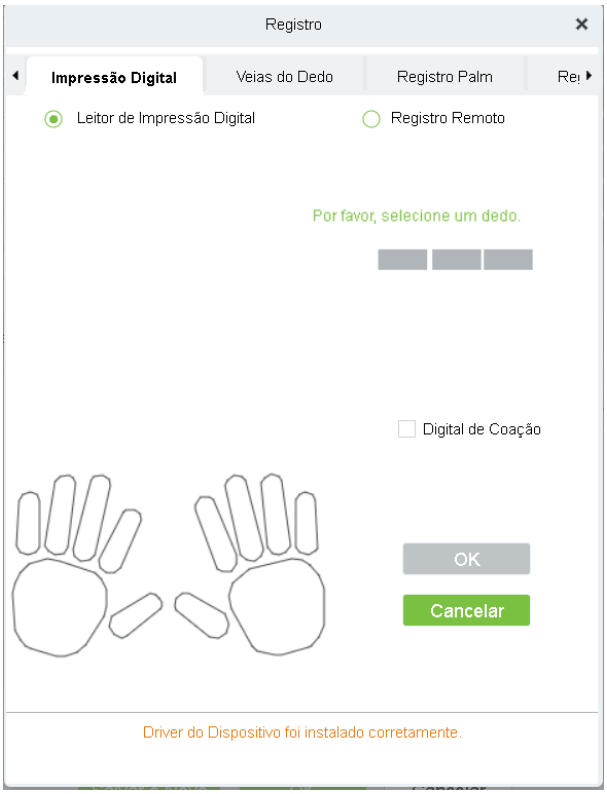
Para editar as configurações do número máximo de caracteres de cada número de pessoal e se letras também podem ser usadas, clique em Pessoal > Parâmetros.

- **Departamento:** Selecione no menu suspenso e clique em [OK]. Se o departamento não foi configurado anteriormente, aparecerá apenas um departamento chamado [Nome da Empresa].
- **Nome/Sobrenome:** O número máximo de caracteres é 50.
- **Gênero:** Defina o gênero do pessoal.
- **Celular:** Insira o número de telefone do usuário.
- **Tipo de Documento:** Existem quatro tipos de certificados: RG, Passaporte, Carteira de Motorista e Outros.
- **Número do Documento:** Insira o número do documento.
- **Data de Nascimento:** Insira a data de nascimento real do funcionário.
- **E-mail:** Insira o Email do funcionário. O comprimento máximo é 30.
- **Senha:** Defina a senha para verificar no dispositivo usando contas de pessoal. Pode conter apenas até 6 dígitos. Não pode ser igual à senha de outro usuário e à senha de coação.
- **Número do Cartão:** O comprimento máximo é 10 e não deve ser repetido.
- **Foto Pessoal:** A função de visualização da imagem é fornecida, suportando formatos de imagem comuns, como jpg, jpeg, bmp, png, gif, etc. O melhor tamanho é 120×140 pixels.

- **Procurar:** Clique em [Procurar] para selecionar uma foto em seu disco local para fazer upload.

- **Capturar:** Tirar foto pela câmera é permitido quando o servidor está conectado a uma câmera.

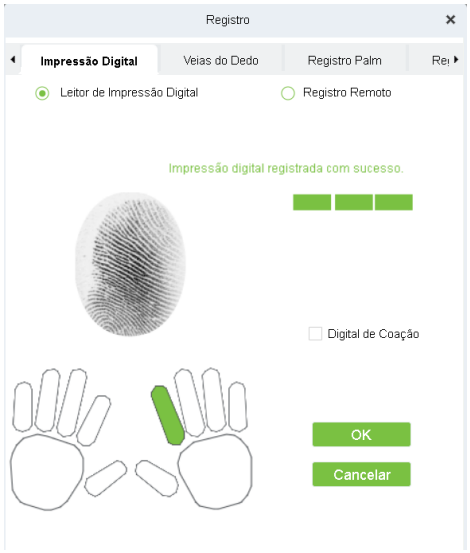
- **Registrar Impressão Digital / Veia do Dedo / Palma / Rosto:** Inscreva a Impressão Digital, Veia do Dedo, Palma ou Rosto do Pessoal. Para disparar o alarme e enviar o sinal para o sistema, escaneie a Impressão Digital de Coação.



Registrar Impressão Digital:

1) Mova o cursor para a posição do ícone de impressão digital, uma janela pop-up de registro ou uma caixa de diálogo de download de driver aparecerá, clique em [Registrar].

2) Selecione uma impressão digital, pressione o dedo no sensor três vezes, então "Impressão digital registrada com sucesso" será exibido.
3) Clique em [OK] para completar o registro.



Notas:

1) Clique em uma impressão digital para excluir.
2) Se precisar registrar uma impressão digital de coação, selecione a caixa de seleção "**Impressão Digital de Coação**".
3) Se as impressões digitais estiverem duplicadas, "**Não repita a entrada da impressão digital**" será exibido.
4) Se o driver do sensor de impressão digital não estiver instalado, clique em **[Instalar driver]** e o sistema solicitará o download e a instalação do driver.
5) Após instalar o driver do sensor de impressão digital, se o botão de registro de impressão digital estiver cinza no navegador IE enquanto estiver normal em outros navegadores (como Firefox, Google), você pode alterar as configurações do navegador IE, conforme abaixo:

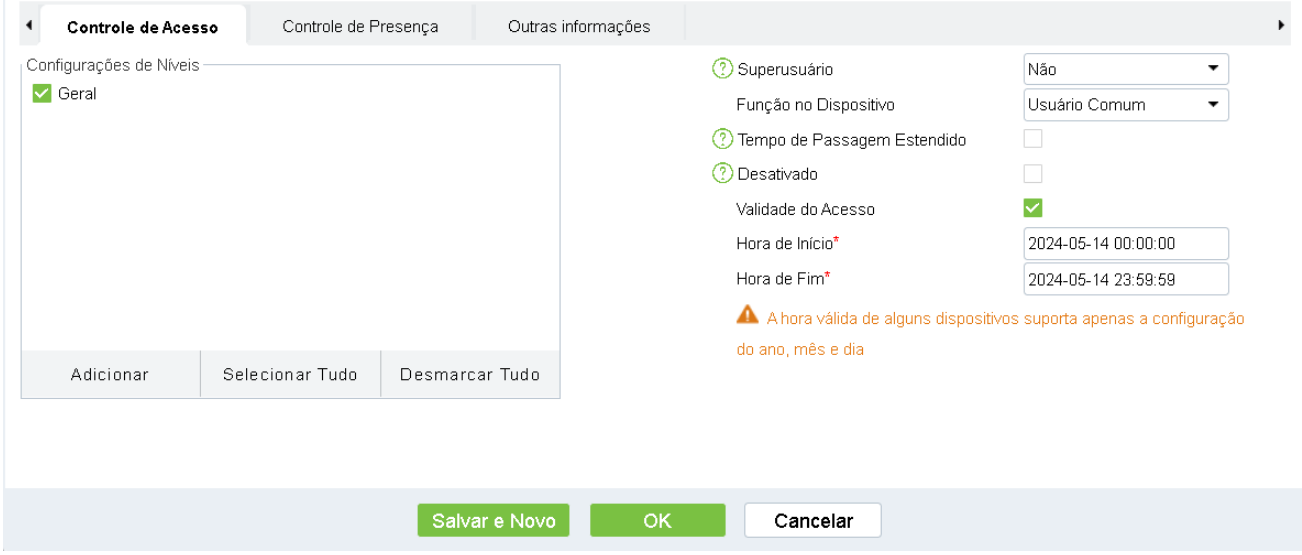
a. No Internet Explorer, clique em **[Ferramentas] > [Opções da Internet]** > **[Segurança]** > **[Sites Confiáveis]**, adicione http://localhost aos sites confiáveis, depois reinicie o Internet Explorer.
b. No Internet Explorer, clique em **[Ferramentas]** > **[Opções da Internet]** > **[Avançadas]** > **[Redefinir]** para abrir uma caixa de diálogo de Redefinir Configurações do Internet Explorer, clique em **[Redefinir]** para confirmar; depois reinicie o Internet Explorer (você pode tentar quando o Ponto 1 não ajudar).
c. Se todas as configurações acima não funcionarem, execute as seguintes operações (usando o navegador IE11 como exemplo): clique em **[Ferramentas]** > **[Opções da Internet]** > **[Avançadas]** > **[Segurança],** marque a opção de "**Permitir que o software seja executado ou instalado**

mesmo que a assinatura seja...", e remova a seleção "**Verificar a revogação do certificado do servidor**", depois reinicie o IE.

d. Se o navegador for anterior ao IE8, a página de registro de impressão digital será diferente.

e. O sistema suporta acesso do dispositivo de impressão digital Live20R e a função de prevenção de impressão digital falsa.

Configure os parâmetros de Controle de Acesso para o pessoal. Clique em [**Regra de Acesso**].



Configure os parâmetros de Controle de Acesso para o pessoal. Clique em [Regra de Acesso].

Os campos são os seguintes:

Configurações de Nível: Clique em **[Adicionar],** depois defina as regras de passagem de posições especiais em diferentes fusos horários.

- **Superusuário:** No funcionamento do controlador de acesso, um superusuário não é restrito pelas regulamentações de fusos horários e tem prioridade de abertura de porta extremamente alta.
- **Função no Dispositivo:** Definirá o nível de autoridade no dispositivo do usuário.
- **Desativado:** Desativa temporariamente o nível de acesso do pessoal.
- **Válidade do Acesso:** As portas podem ser configuradas para abrir apenas dentro de certos períodos de tempo. Se a caixa de seleção não estiver marcada, a porta estará sempre ativa.

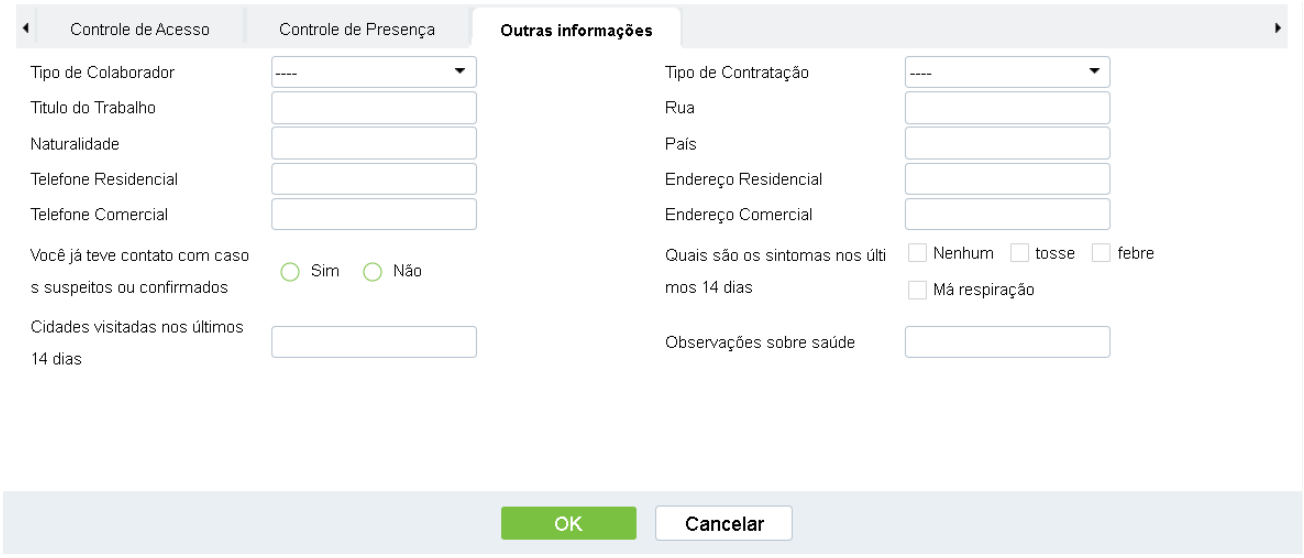
Nota: O sistema automaticamente buscará pelos números relevantes na biblioteca de partida durante a verificação.

A Lista de Informações do Pessoal, por padrão, é exibida como uma tabela. Se a Exibição Gráfica for selecionada, fotos e números serão mostrados. Coloque o cursor sobre uma foto para ver detalhes sobre o pessoal.

Notas:

1) Nem todos os dispositivos suportam a função "Desativado". Quando um usuário adiciona um dispositivo, o sistema notificará o usuário se o dispositivo atual suporta essa função ou não. Por favor, atualize o dispositivo para usar essa função.
2) Nem todos os dispositivos suportam a função "Definir Horário Válido". Alguns dispositivos permitem apenas aos usuários definir o ano, mês e dia do horário local. Quando um usuário adiciona um dispositivo, o sistema notificará o usuário se o dispositivo atual suporta essa função ou não. Por favor, atualize o dispositivo para usar essa função.

Clique em **[Detalhes do Pessoal]** para acessar os detalhes e a interface de edição e inserir informações.



Após inserir as informações, clique em **[OK]** para salvar e sair, os detalhes pessoais serão exibidos na lista adicionada.

3.1.1.2 Editar Pessoal

Clique em **[Pessoal]** > **[Pessoa],** então selecione uma pessoa e clique em **[Editar].**

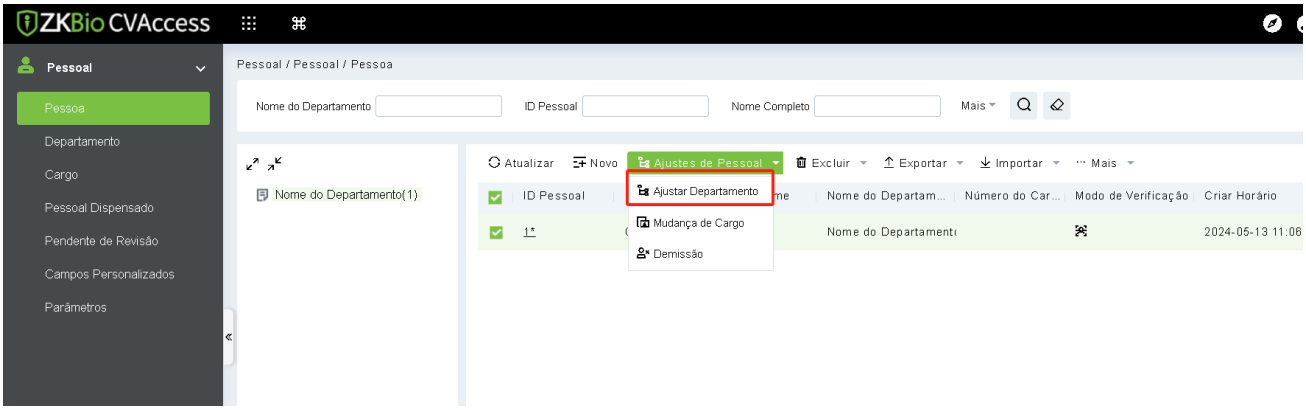
3.1.1.3 Excluir Pessoal

Clique em **[Pessoal]** > **[Pessoa]**, então selecione uma pessoa e clique em **[Excluir]** > **[OK]** para excluir.

Nota: Todas as informações relevantes sobre a pessoa serão excluídas.

3.1.1.4 Ajustar Departamento

1) Clique em **[Pessoal]** > **[Pessoa],** então selecione uma pessoa e clique em **[Ajustar Departamento].**

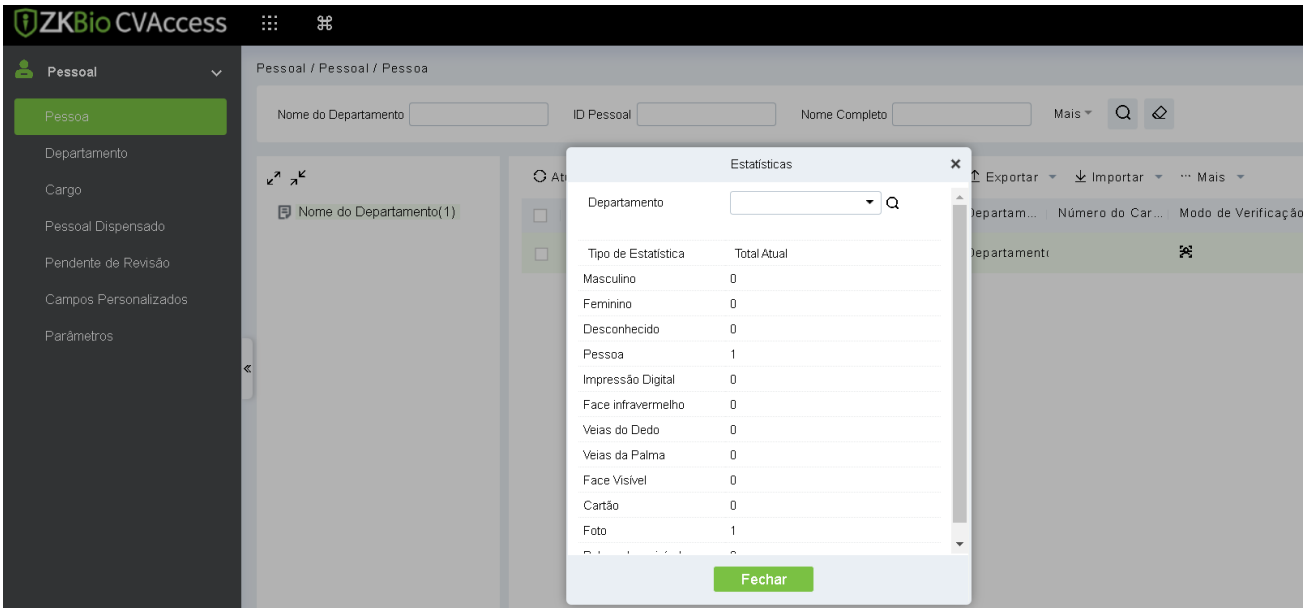


Selecione na lista suspensa de "Novo Departamento".

Clique em **[OK]** para salvar e sair.

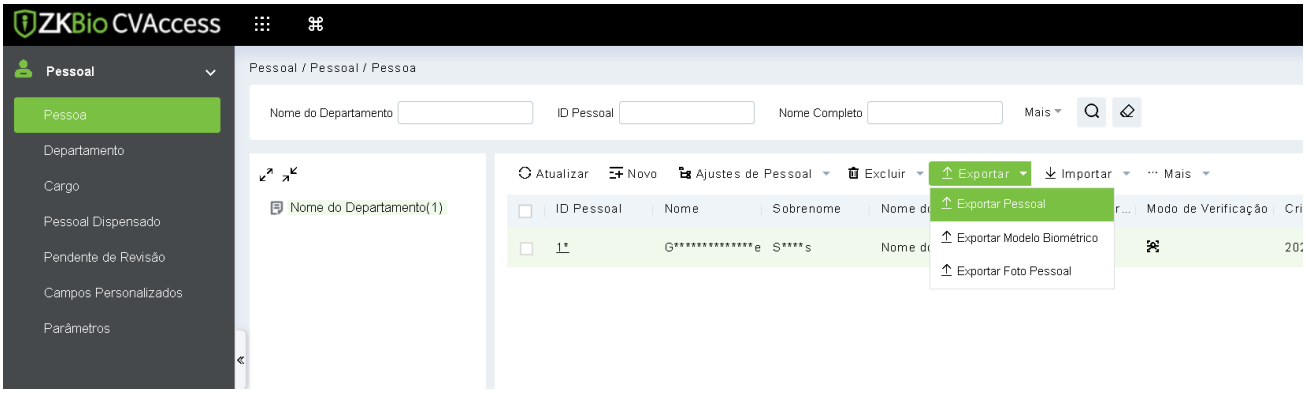
3.1.1.5 Estatísticas

Clique em **[Pessoal]** > **[Pessoa]** > **[Estatísticas].** Visualize o número de pessoal, o número de impressões digitais, templates de rosto, veias do dedo cadastradas, números de cartão, gênero e outras informações estatísticas.

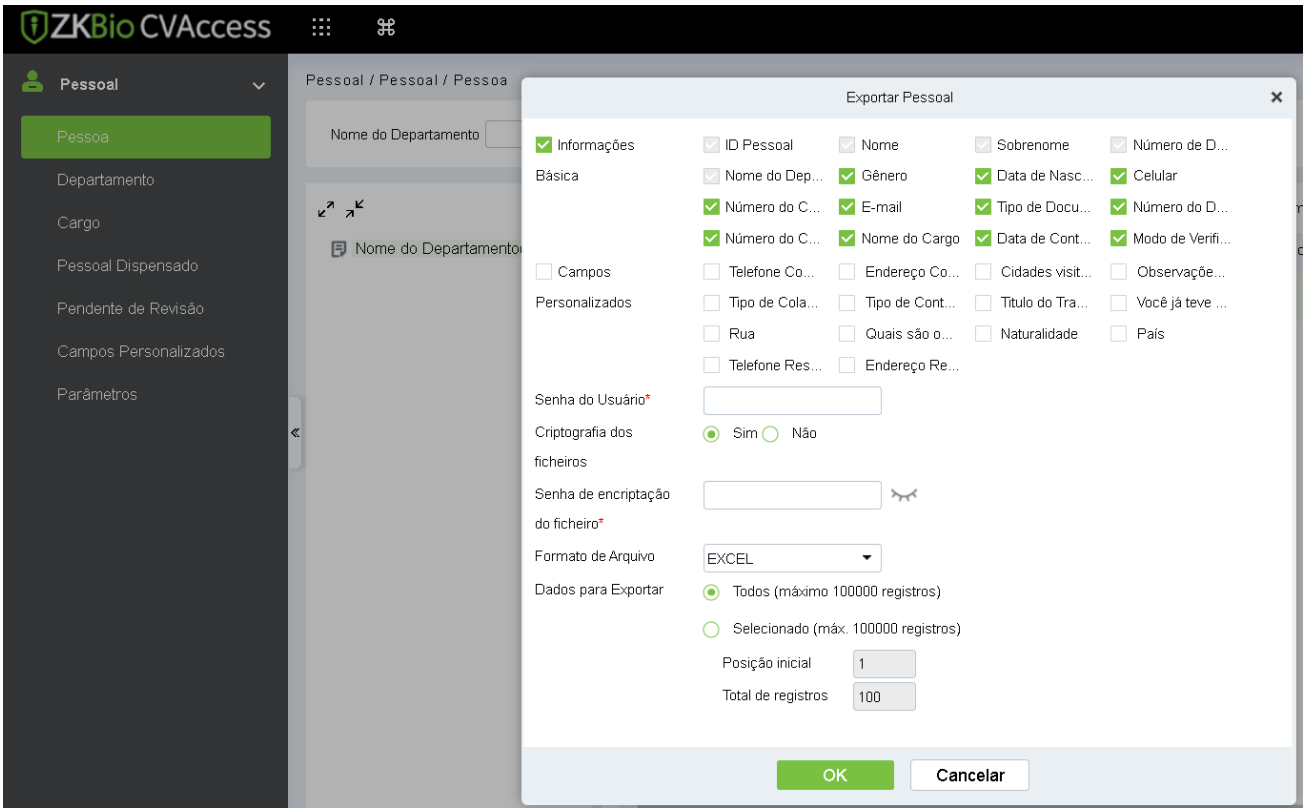


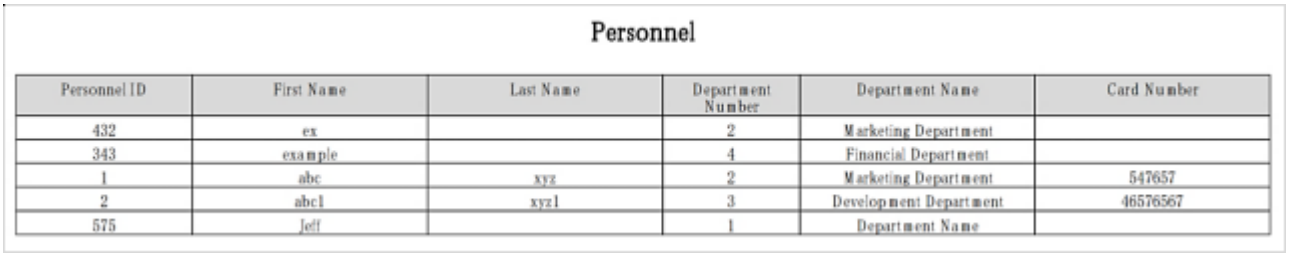
3.1.1.6 Exportar

Clique em **[Pessoal] > [Pessoa] > [Exportar]** para exportar informações de pessoal, templates biométricos de pessoal e fotos de pessoal.



Selecione o tipo de arquivo e o modo de exportação conforme necessário.

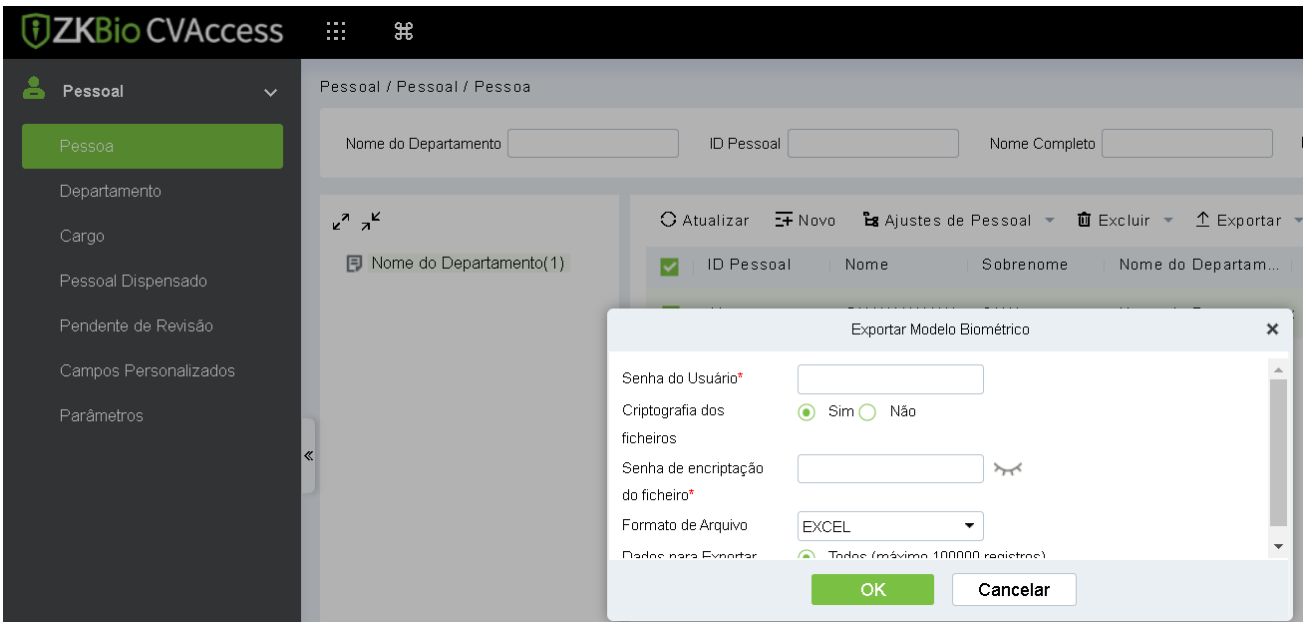


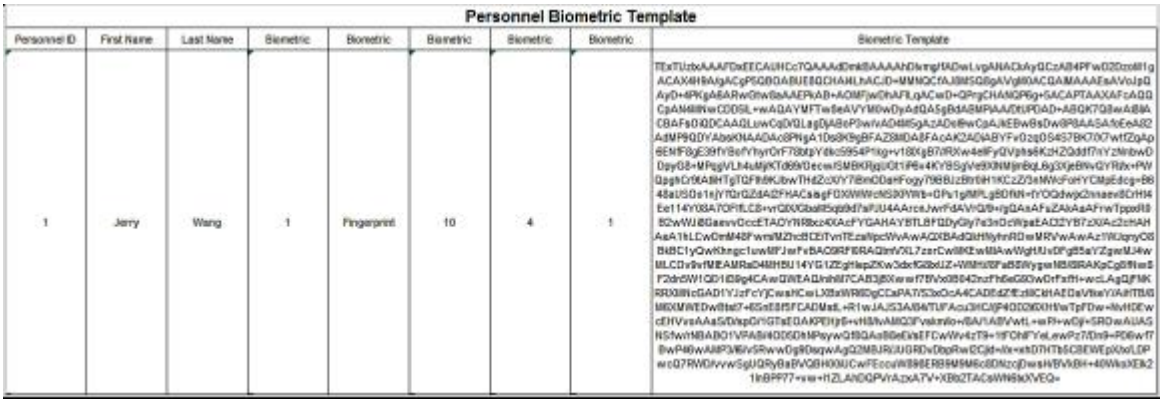


Personnel

Personnel ID	First Name	Last Name	Department Number	Department Name	Card Number
432	ex		2	Marketing Department	
343	example		4	Financial Department	
1	abc	xyz	2	Marketing Department	547657
2	abc1	xyz1	3	Development Department	46576567
575	Jeff		1	Department Name	

Exportar o Template Biométrico.

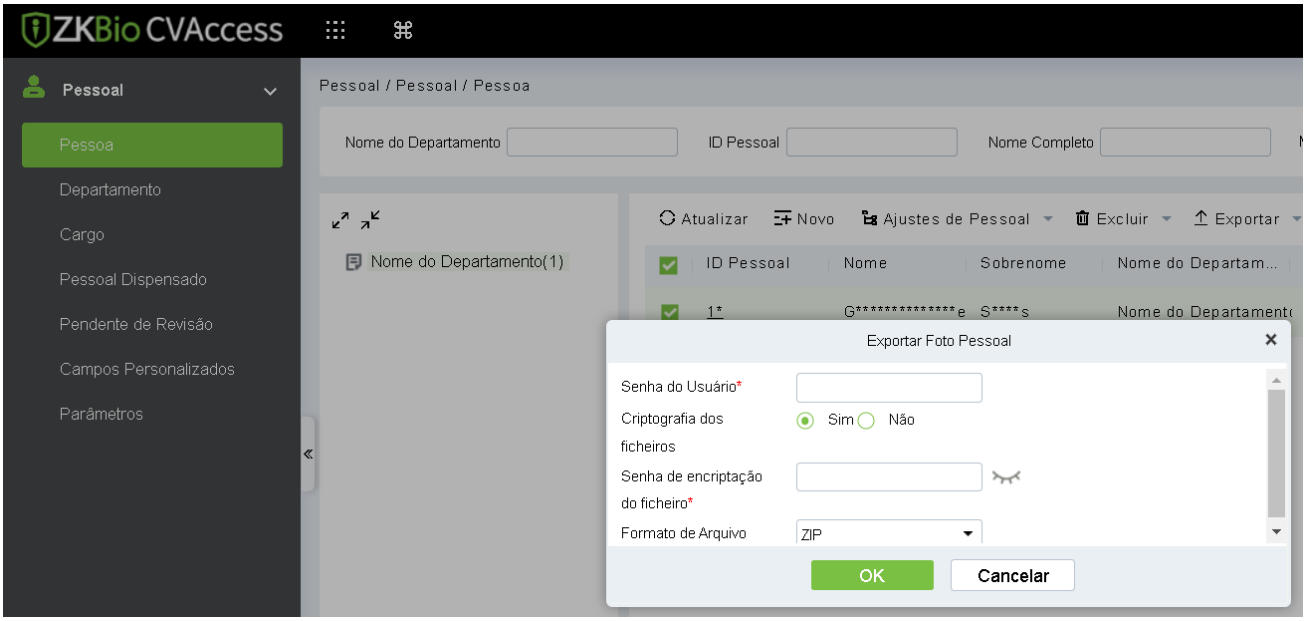




Personnel Biometric Template

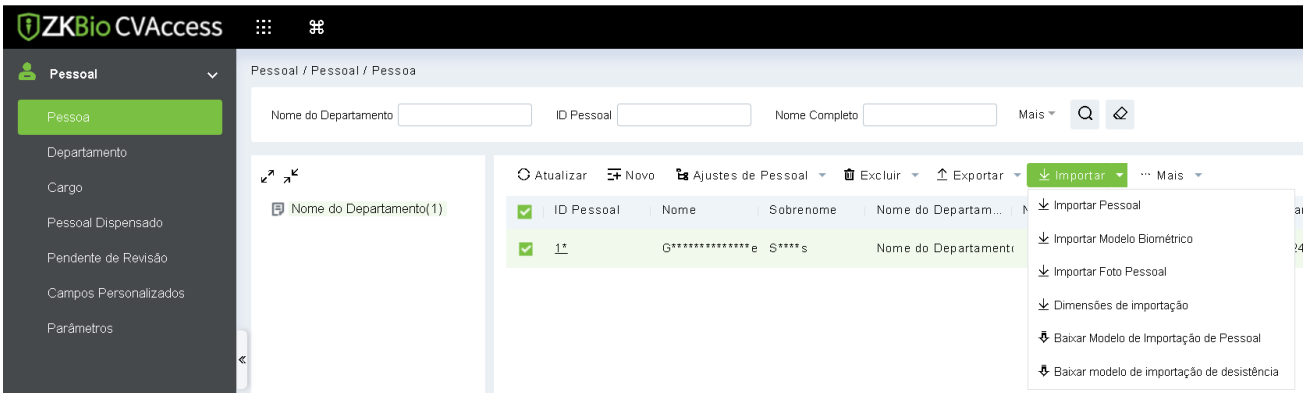
Personnel ID	First Name	Last Name	Biometric	Biometric	Biometric	Biometric	Biometric	Biometric Template
1	Jerry	Wang	1	Fingerprint	10	4	1	TExTUzbAAAFDaEECAIIHCcTQAAAvBmkBAAAANDkmg/tADwLvgANACbAyQCzA8MPFw020zo8IgACAX4HBAIgACgP5Q0GABUE8QCHAHLhACJD=MMkOCfAJ8MSQ8gAVg880ACQAMAAAAEaAVoJpQAyD+4PKgA6ARwGhv8aAAEPkAB+AO8MjwDhAFLgACwD+QPrgCHAMQP6g+5ACAPTAAXAFzAQDCpAM4BWwCDDSL+wAQAYMFTw8eAVYM6wDyAdQA5gBdABMPAAvDtPDAD+A8QK7Q8wABACBAFs0IQDCAAQLuwCqDYDLagDjABePSwIvAD4M5gAzADeBwCpAJkEBwBsDw0P8AA5A5vEeA82AdMP9QDYAbqKHAADAc8PNgA1Ds8K9gBFAZ38IDABFAcAK2ACjAABYFv0zg0S4S7BKO7OWttZQAp6EM/F8gE39fYBefYhyrOrF78btpYdkc5954P1kg+v180gB7/RXw4elFyQVpbs8KzHZQddf7nYzNrbwD0qy08+MPgjVLh4uMjKTd69Y0ecwI5MBKRjgUO1iP6+4KY8SgVe9XNMjlrBqL6g3XjeBRvQYRzk+PWQpgNDr9AIIHTgTQFIh6KJbwTHdZcXlY7IEmDaeFogyi9BBJzBrbH1KCzZ/3aMVkFoHYCMpEdcg+BB48aU5G0s1sjYf2rGZd4AfZFHACsagF0XWMrcNS9XPWtB+DPs1gMPLgBDfkN+fYOGdwjx2nsaev8CrH14Ee114Y08A7OFtELC8+vrGDXGbaIf5qq9d7aFJU44Arcs/wrFdAVrQ5h+rgDAsAFsZAkAaAFrwTppxdI8ZwWJBGaesvOccETADYNRbcz4XAcFYGAHAYBTLBFtDyGly7e3nOcWpaEADZYB7zXiAc2crHAHAeA1bLCwDmM48FwmMZhcBCEiTvnTEzaRpcWvAwAQXBAdQkHfiyhnRDwMRVwAwAz1WJqryO8BtBC1yQwKbngc1uwMFJwFvBAO9RFBRAQbmV3L7zerCwBKEwBAwWgMJUvDFg85aYZgwMJ4wMLCDv9vfMEAMRaD4MHBU14YGJZgHapZKw3dcfG0bdJZ+WMhi0FwBBWygwMBI0RAKpCg0fiwsBF2drOW1QD1D0g4CAwQWEADJnhM7CAB3j0XwrwI7BVx03542nzfhEeG0OwDrFxfH+wcLAgQjFMKRRX0IlcGAD1YJzFcYjCwsNCwIJ0bWR0DgCCaPATV53zOcA4CADEdZfEzdBCtIAEDaVtwYAiNTBd0MEXMWEDwBtd7+65s83f5FCADMdL+R1wJAJ3AN4TUFAcd3HCiJF4D0D0KNHfwTpFDw+MvHDEwcEHVvsAAa5/D/kpOr/GTaEOAKPEHj6+vH8/fvAM0Z3Fvakrdlo+/BA/IA8VWtL+wP+wCji+SRDwAUAG5NSfWrMBABO1VRA8vl4QD6DtHPsywvQ19QAa86eEaEFCwWv4zT9+1fFCNFYeLewPz7/Dn9+PD6wfTBwP46wAMP3W6VSRww0g9DsqwAgQ2MBJRjUGRDvDbpRwDCjdt+ltx+ehD7HTb5CBEWEpXboLDPwcQ7RWDAvvwSgUQRy6aBVQBH00UCwFEcouW896EB9M6M6c8DNzcjDwsHBVkBH+40Wks3Eb21InBPP7+ww+rI1ZLAnDQPVrAzpxA7V+XB9ZTACsWN6kXVEQ=

Exportar Foto do Pessoal.

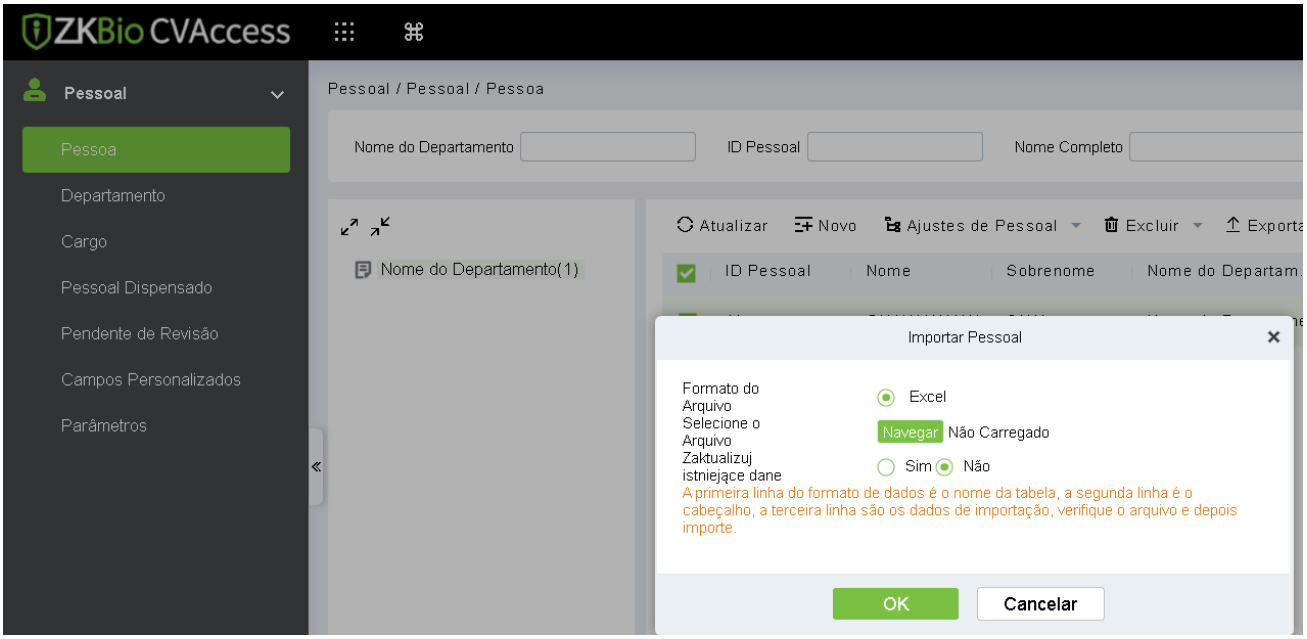


3.1.1.7 Importar

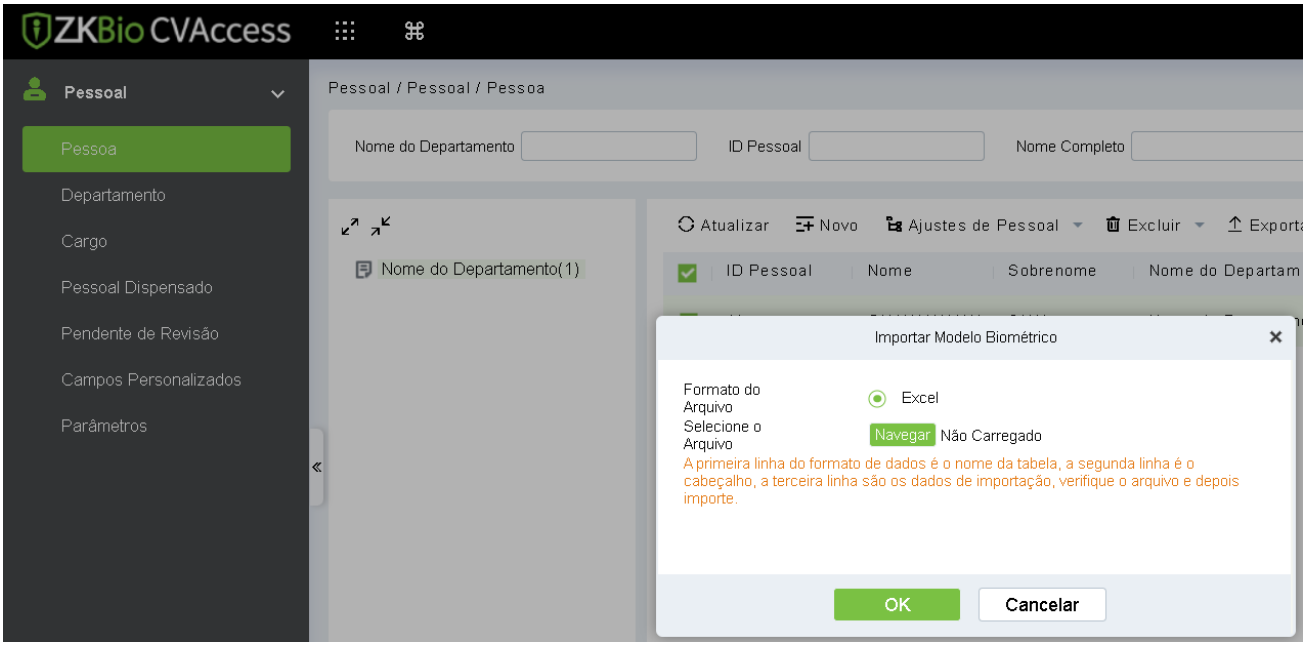
Clique em **[Pessoal]** > **[Pessoa]** > **[Importar]** para importar informações de pessoal e templates biométricos de pessoal. Ele suporta apenas templates de informações de pessoal para importação.



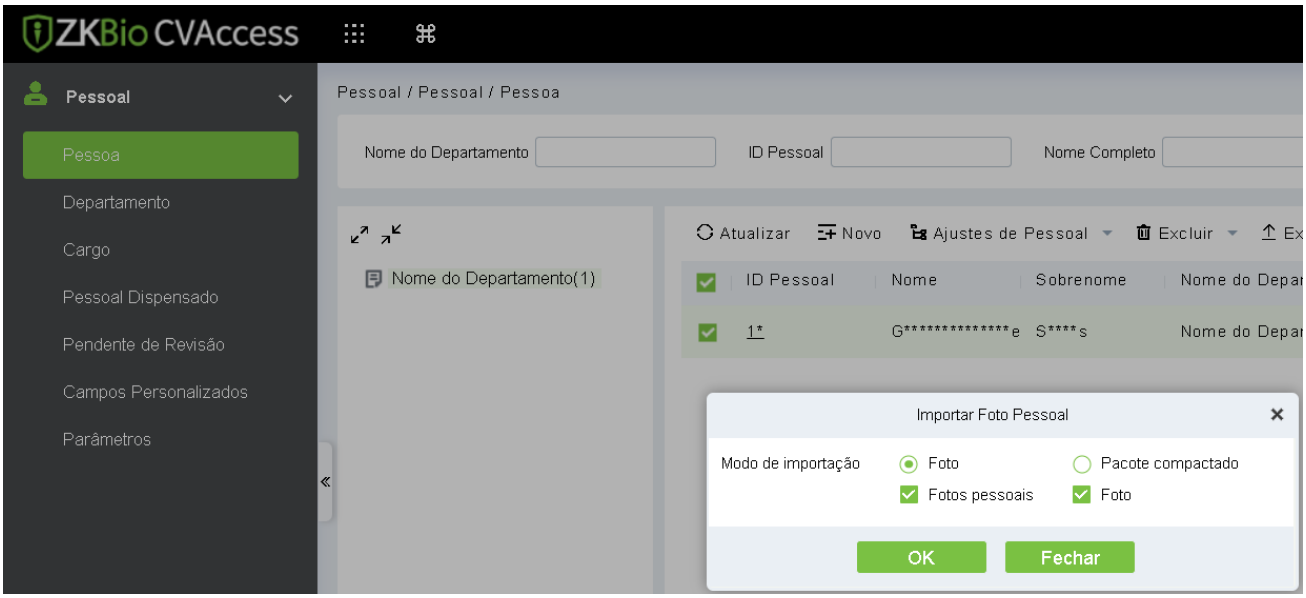
Importar Pessoal: Selecione "**Sim**" para [**Atualizar o ID de Pessoal existente no sistema**], os dados originais serão sobrescritos quando o ID de pessoal for repetido; selecione "**Não**" para o oposto.



Importar Template Biométrico.



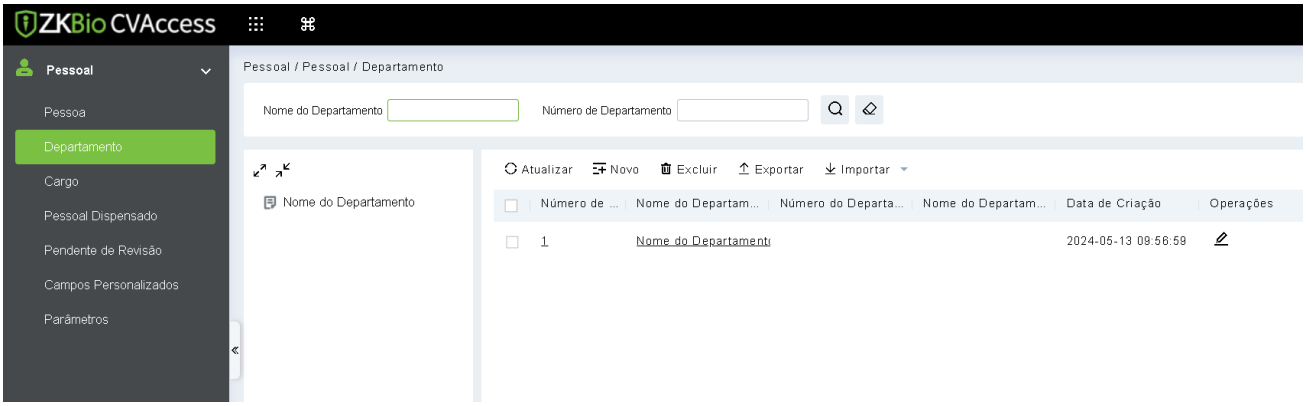
Importar Foto do Pessoal: A foto do pessoal precisa ser nomeada pelo ID do pessoal, suportando formatos de imagem comuns, como jpg, jpeg, png, gif, etc.



3.1.2 Departamento

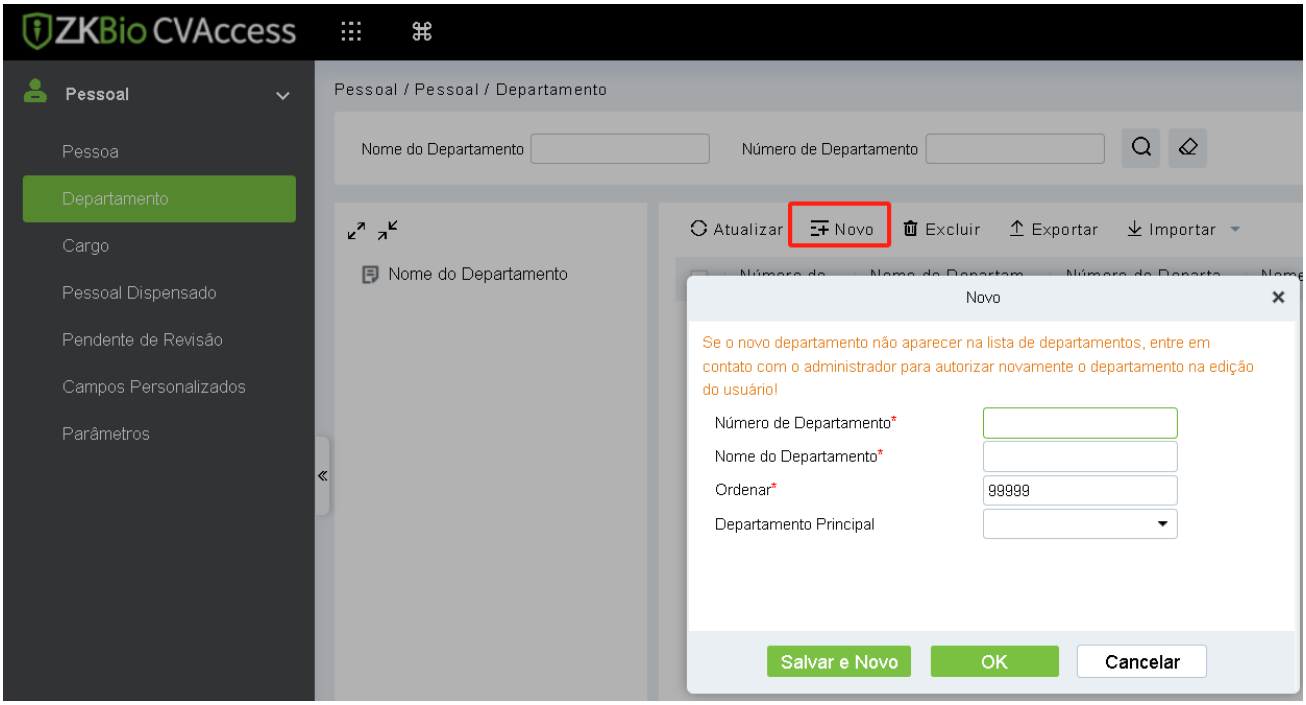
Antes de gerenciar o pessoal da empresa, é necessário configurar um organograma departamental da empresa. Ao usar o sistema pela primeira vez, por padrão, ele possui um departamento principal chamado **[Geral]** e numerado **[1].** Este departamento pode ser modificado, mas não pode ser excluído.

As principais funções do Gerenciamento de Departamento incluem Adicionar, Editar, Excluir, Exportar e Importar Departamento.



3.1.2.1 Adicionar um Departamento

Clique em **[Pessoal]** > **[Gerenciamento de Pessoal]** > **[Departamento]** > **[Novo].**



Os campos são os seguintes:

- **Número do Departamento:** Letras e números estão disponíveis. Não pode ser idêntico ao número de outros departamentos. O número não deve exceder 30 dígitos.
- **Nome do Departamento:** Combinação de caracteres de até 100. Em caso de diferentes níveis, os nomes dos departamentos podem se repetir.
- **Classificação:** Usada para definir a prioridade (nível) de um departamento dentro de um departamento pai. Quanto menor for o número de classificação do departamento, maior será o ranking desse departamento. Você pode definir qualquer número de 1 a 999999.

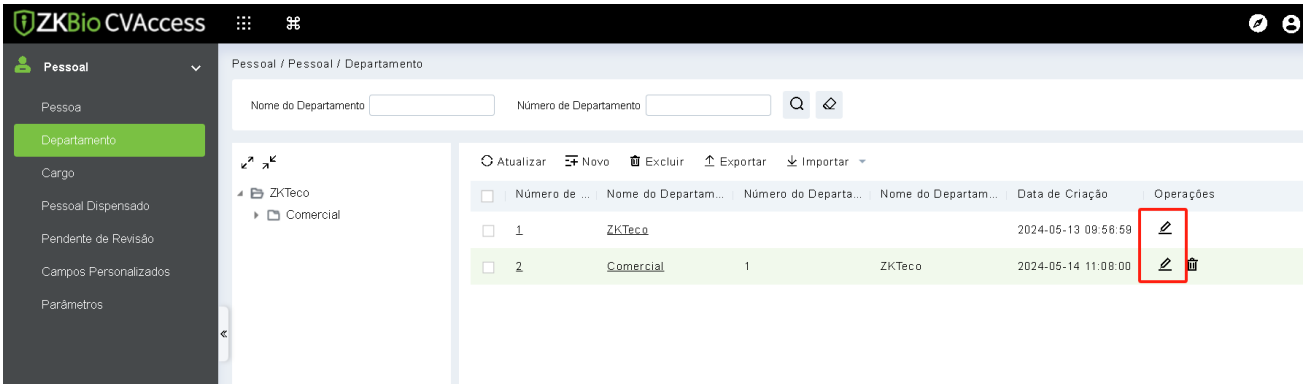
- **Departamento Pai:** Selecione um departamento pai na lista suspensa. O departamento pai é um parâmetro importante para determinar o organograma da empresa. À esquerda da interface, o organograma da empresa será mostrado na forma de uma árvore de departamentos.

Depois de preencher os detalhes, você pode clicar em **[OK]** para concluir a adição; ou clicar em **[Cancelar]** para cancelar ou clicar em **[Salvar e Novo]** para salvar e continuar adicionando um novo departamento.

Para adicionar um departamento, você também pode escolher **[Importar]** para importar informações de departamento de outro software ou de outros documentos para este sistema. Para detalhes, consulte Operações Comuns.

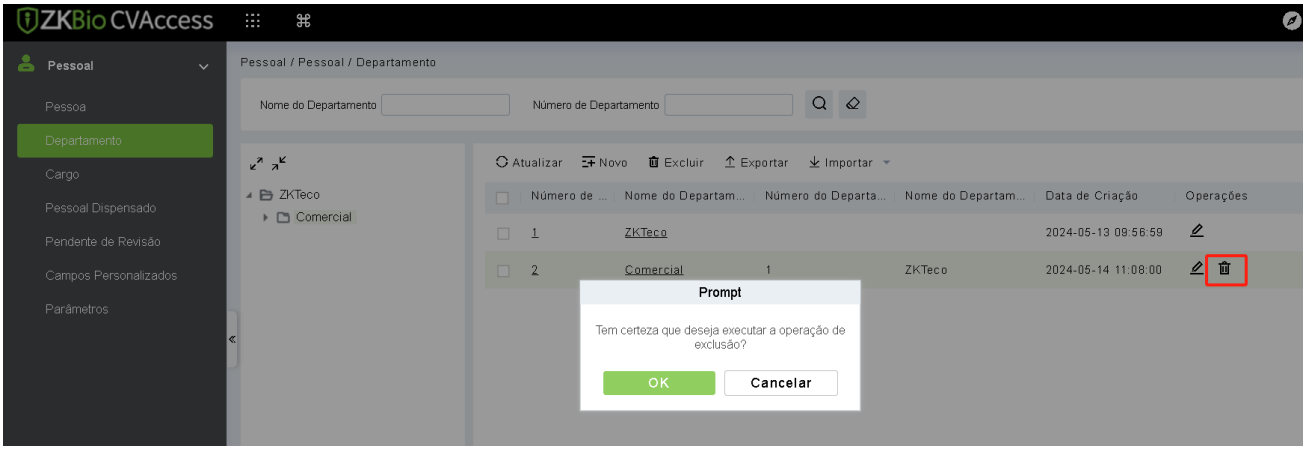
3.1.2.2 Editar um Departamento

Clique em **[Pessoal]** > **[Pessoal]** > **[Departamento]**, selecione um departamento e clique 



3.1.2.3 Excluir um Departamento

Clique em **[Pessoal]** > **[Pessoal]** > **[Departamento],** selecione um departamento e clique 

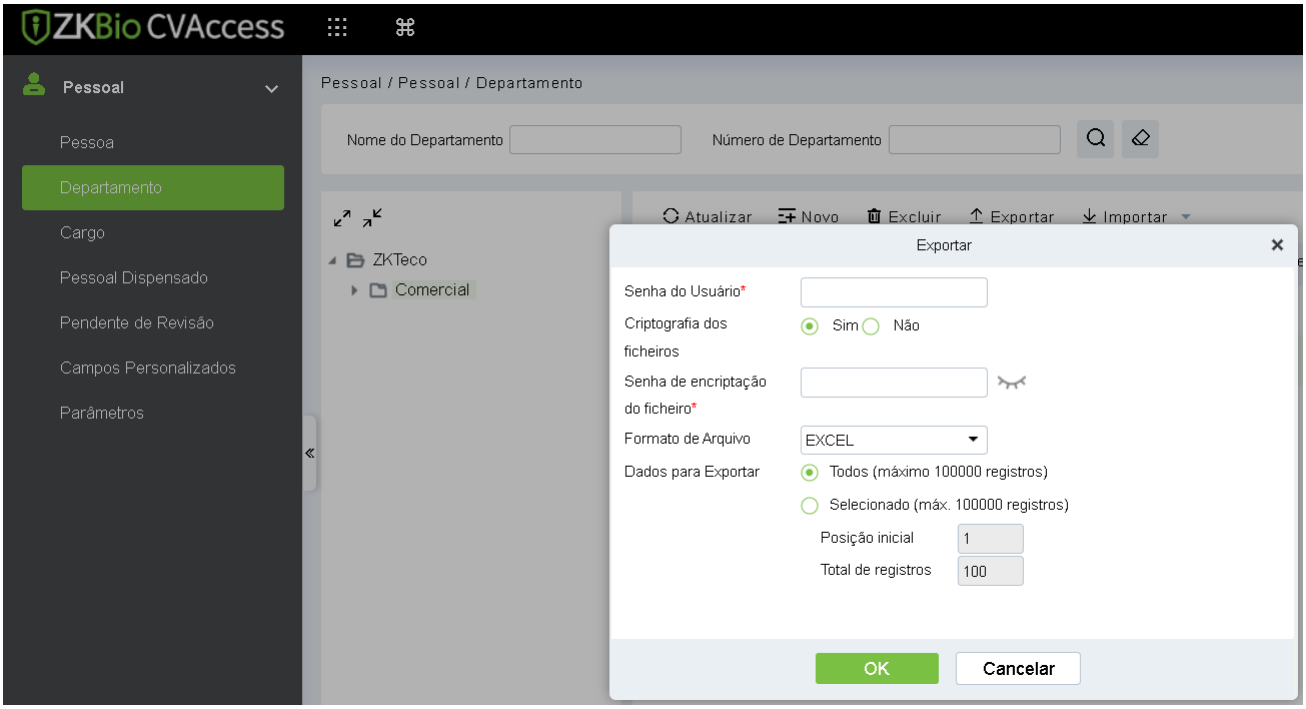


Clique em [OK] para excluir.

Nota: Se o departamento tiver subdepartamentos ou pessoal, o departamento não poderá ser excluído.

3.1.2.4 Exportar

Clique em [Pessoal] > [Departamento] > [Exportar], a interface de importação é a seguinte.



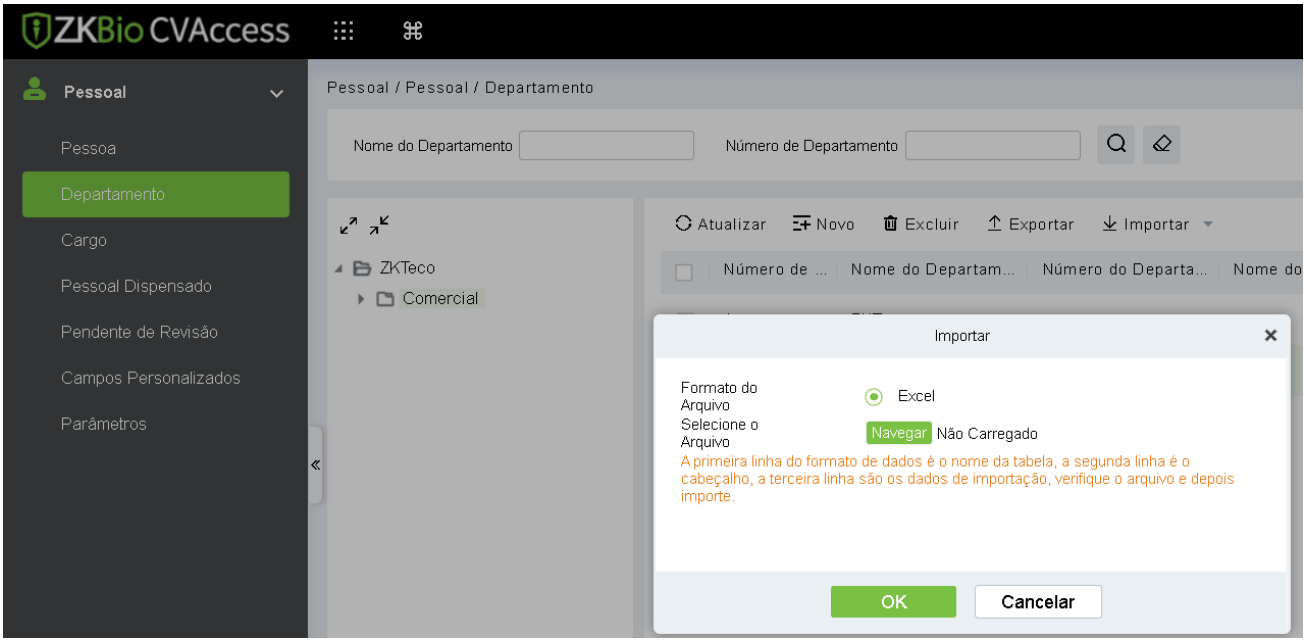
Pode ser exportado nos formatos de arquivo EXCEL, PDF e CSV.

Department

Department Name	Department Number	Parent Department Number	Parent Department Name	Created Date
ZKTeco	1			2018-12-21 14:10:08
Marketing Department	2	1	ZKTeco	2018-12-21 14:10:08
Development Department	3	1	ZKTeco	2018-12-21 14:10:08
Financial Department	4	1	ZKTeco	2018-12-21 14:10:08

3.1.2.5 Importar

Clique em **[Pessoal] > [Departamento] > [Importar],** a interface de importação é a seguinte:

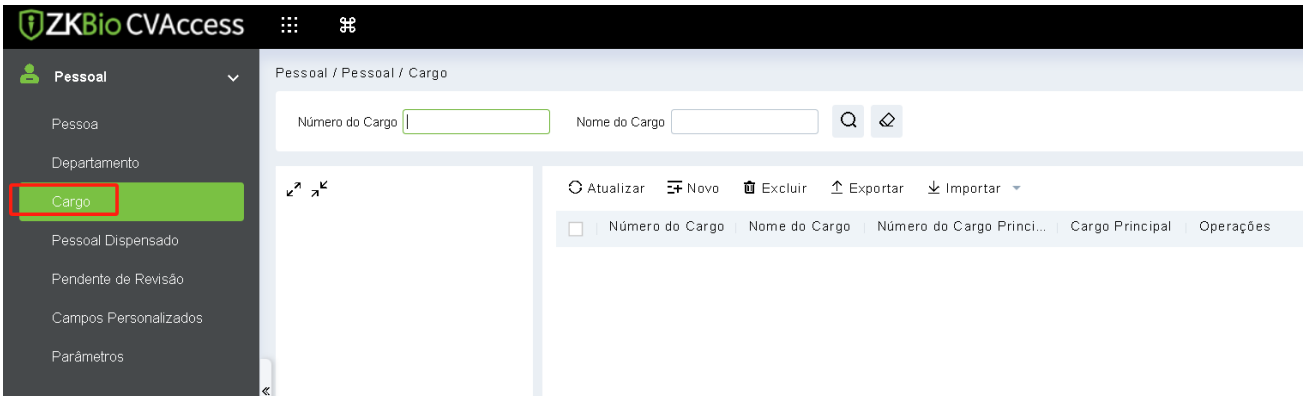


Importar informações do departamento: pode importar arquivos nos formatos EXCEL, CSV.

Após importar o arquivo, o sistema fará a correspondência automática entre o campo do relatório importado e o campo de segmento de dados.

3.1.3 Cargo

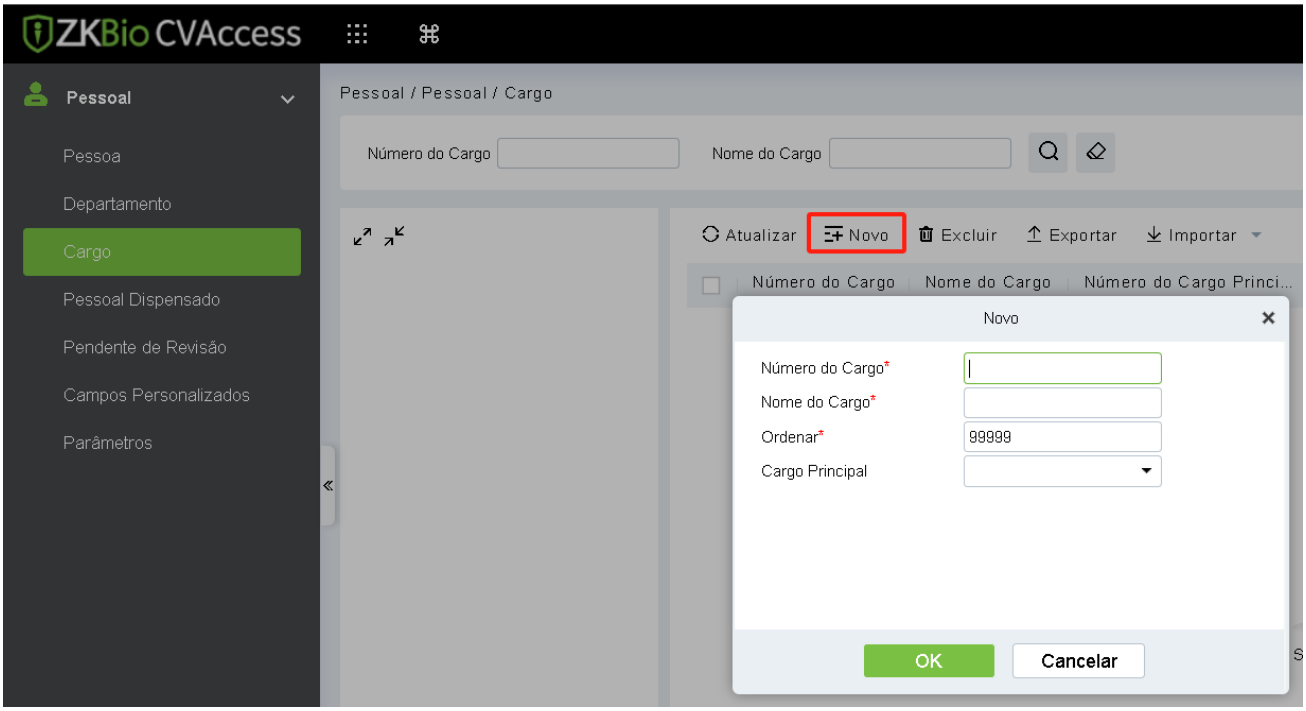
Introduz os passos de configuração para adicionar manualmente um cargo no ZKBioCVSecurity, e adicionar um cargo é usado para definir as informações do cargo de uma pessoa.



3.1.3.1 Adicionar Cargo

Clique em **[Pessoal] > [Gerenciamento de Pessoal] > [Posição] > [Novo].**

Na interface de novo cargo, preencha os parâmetros correspondentes de acordo com os requisitos de adição.

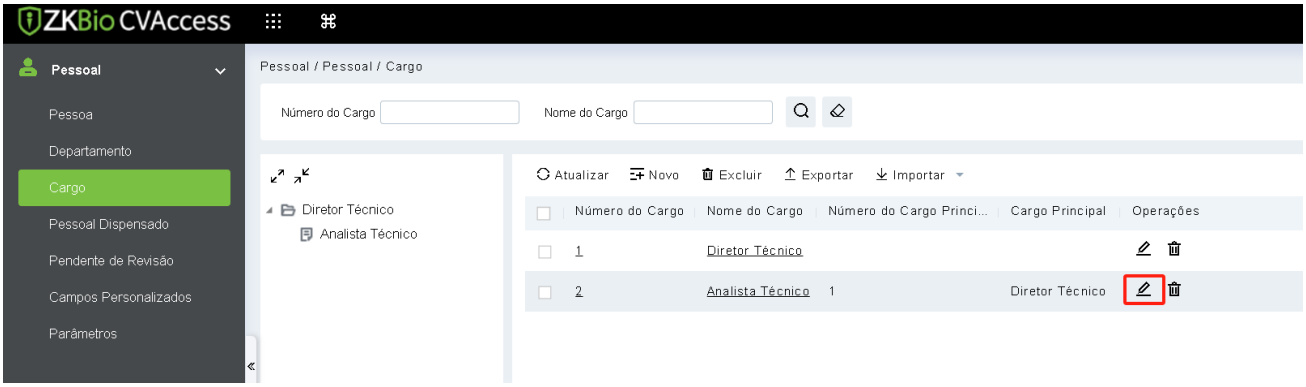


Os campos são os seguintes:

- **Número do Cargo:** Personalize o número do cargo para fácil memorização.
- **Título do Cargo:** Personalize o título do cargo.
- **Classificação:** Classifique as listagens de cargos, apenas números são suportados.
- **Cargo Pai:** Selecione o cargo pai correspondente na caixa de seleção suspensa. Se precisar cancelar, clique novamente em Selecionado.

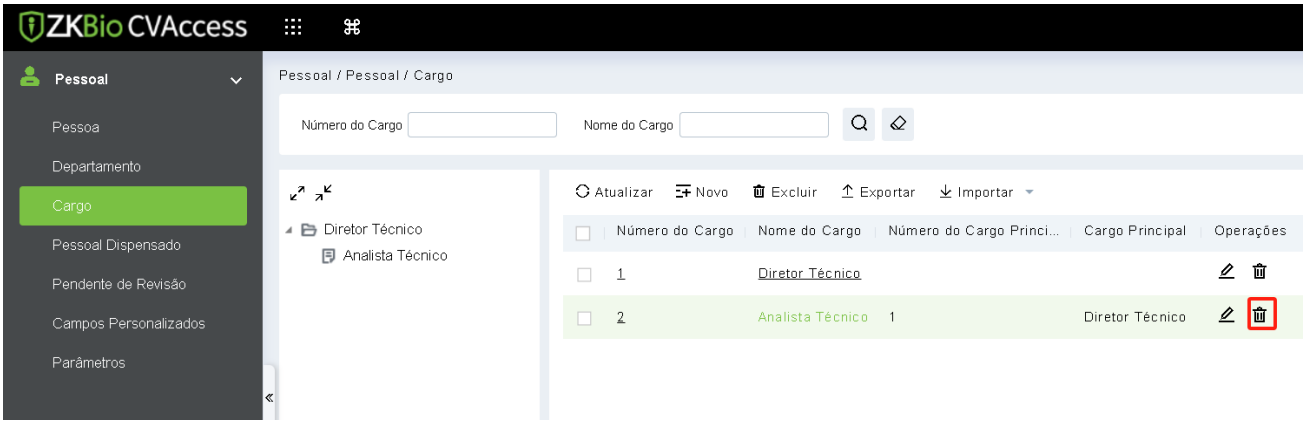
3.1.3.2 Editar

Clique em **[Pessoal]** > **[Gerenciamento de Pessoal]** > **[Posição],** selecione uma posição e clique...



3.1.3.3 Excluir

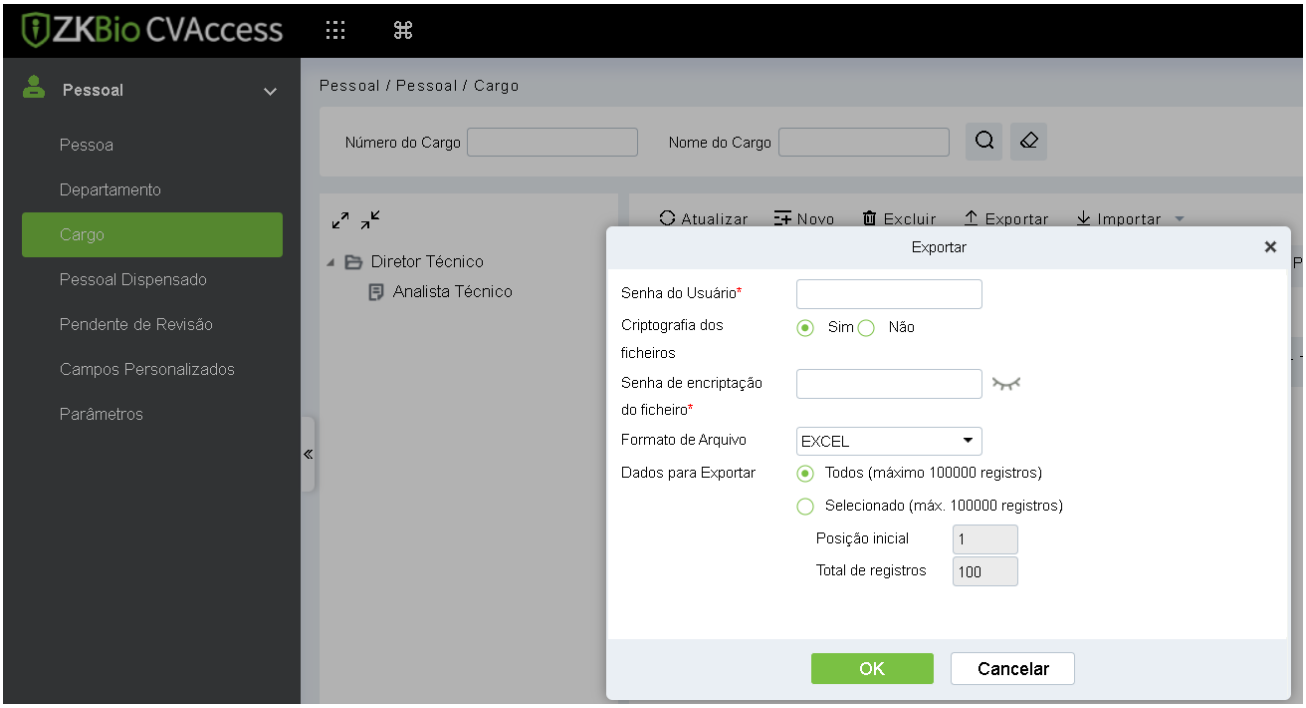
Clique em **[Gerenciamento de Pessoal]** > **[Pessoal]** > **[Posição],** selecione uma posição e clique...



Clique em **[OK]** para excluir.

3.1.3.4 Exportar

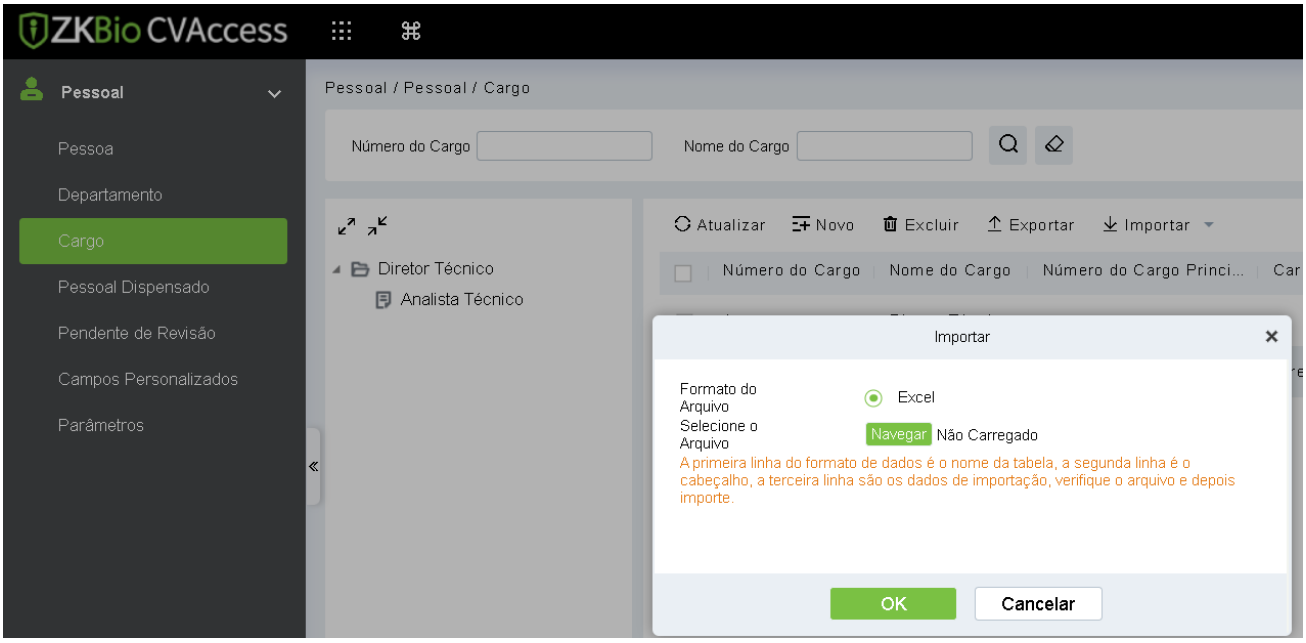
Clique em **[Gerenciamento de Pessoal] > [Departamento] > [Posição],** a interface de importação é a seguinte.



Pode ser exportado nos formatos de arquivo EXCEL, PDF e CSV.

3.1.3.5 Importar

1. Clique em **[Gerenciamento de Pessoal] > [Departamento] > [Importar],** a interface de importação é a seguinte:

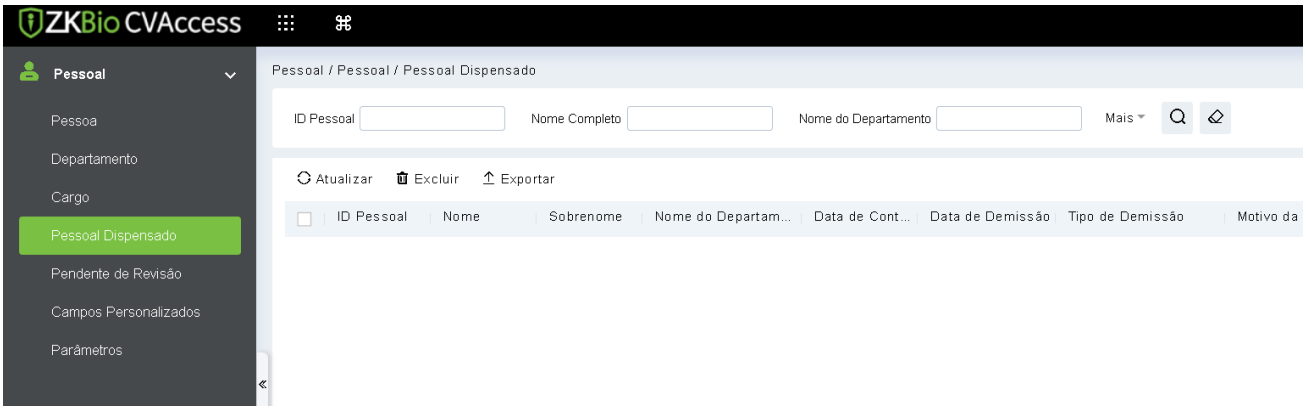


2. Importar informações do departamento: pode importar arquivos no formato EXCEL, CSV.
3. Após a importação do arquivo, o sistema irá combinar automaticamente o campo do relatório importado com o campo de segmento de dados.

3.1.4 Pessoal Desligado

Este parâmetro exibirá o pessoal que não está mais trabalhando na empresa. Uma vez que a pessoa seja desligada, ela será listada.

Clique em **[Pessoal] > [Gestão de Pessoal] > [Pessoal Desligado].**



3.1.4.1 Excluir

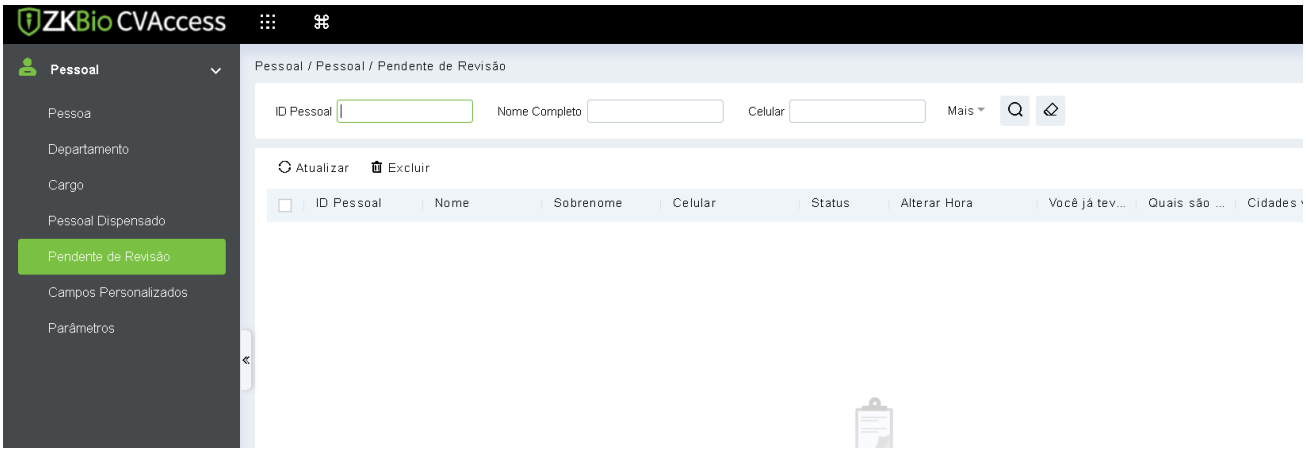
1. Clique em **[Pessoal] > [Gestão de Pessoal] > [Pessoal Desligado]**, selecione um funcionário e clique
2. Clique em **[OK]** para excluir.

3.1.4.2 Exportar

Clique em **[Pessoal] > [Gestão de Pessoal] > [Pessoal Desligado]**, pode ser exportado nos formatos de arquivo EXCEL, PDF e CSV.

3.1.5 Aguardando Revisão

Clique em **[Pessoal] > [Gestão de Pessoal] > [Aguardando Revisão].**

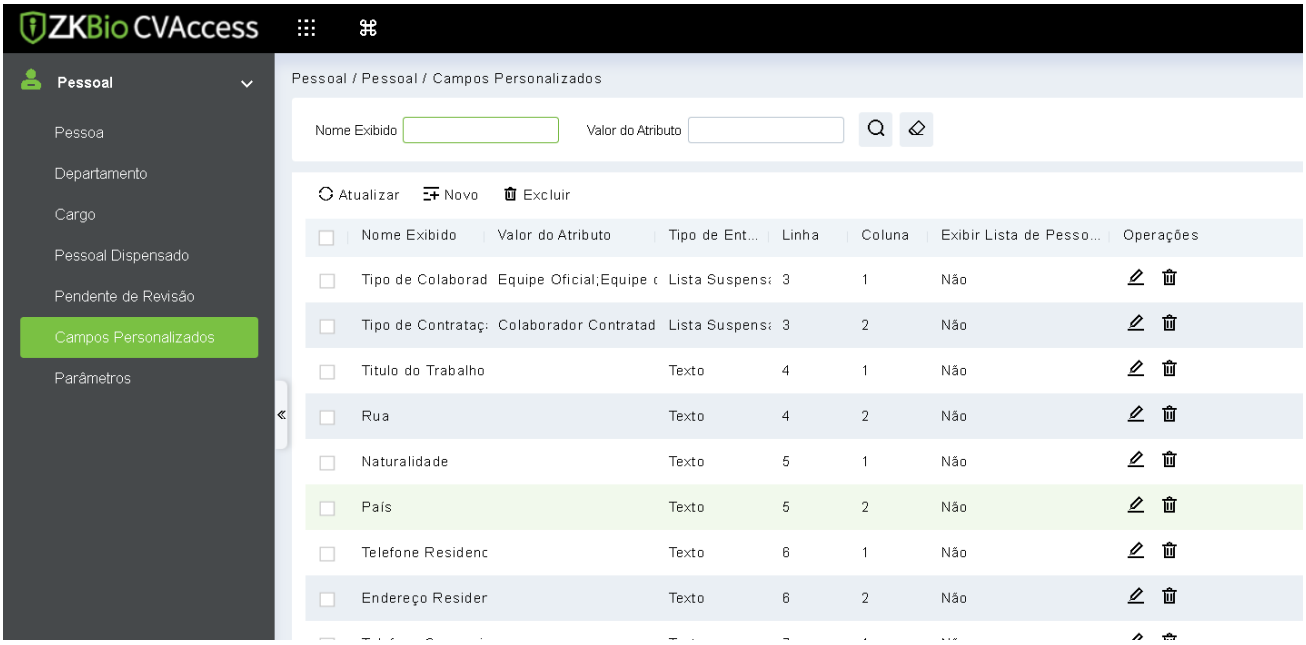


3.1.5.1 Excluir

1. Clique em **[Pessoal] > [Gestão de Pessoal] > [Aguardando Revisão],** selecione uma revisão e clique
2. Clique em **[OK]** para excluir.

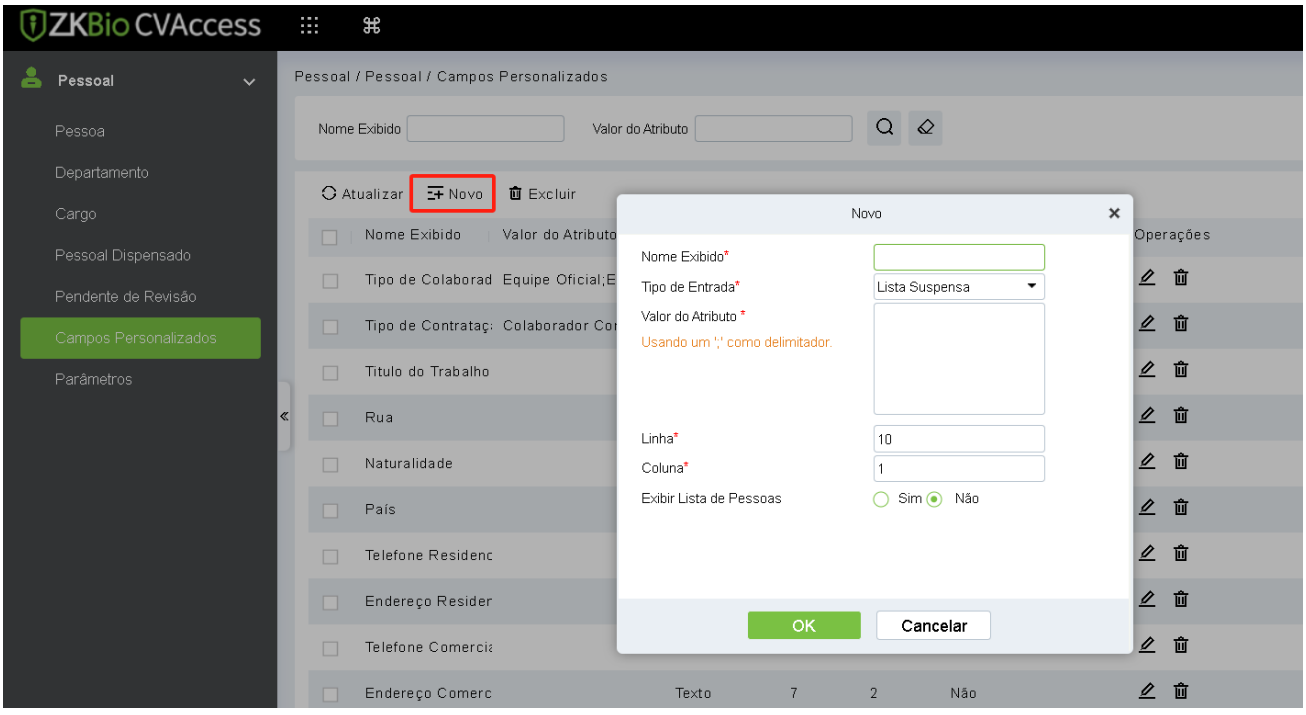
3.1.6 Atributos Personalizados

Alguns atributos pessoais podem ser personalizados ou excluídos para atender aos requisitos de diferentes clientes. Quando o sistema é utilizado pela primeira vez, o sistema inicializará alguns atributos pessoais por padrão. Atributos pessoais personalizados podem ser configurados para diferentes projetos de acordo com os requisitos.



3.1.6.1 Criar um Atributo Personalizado

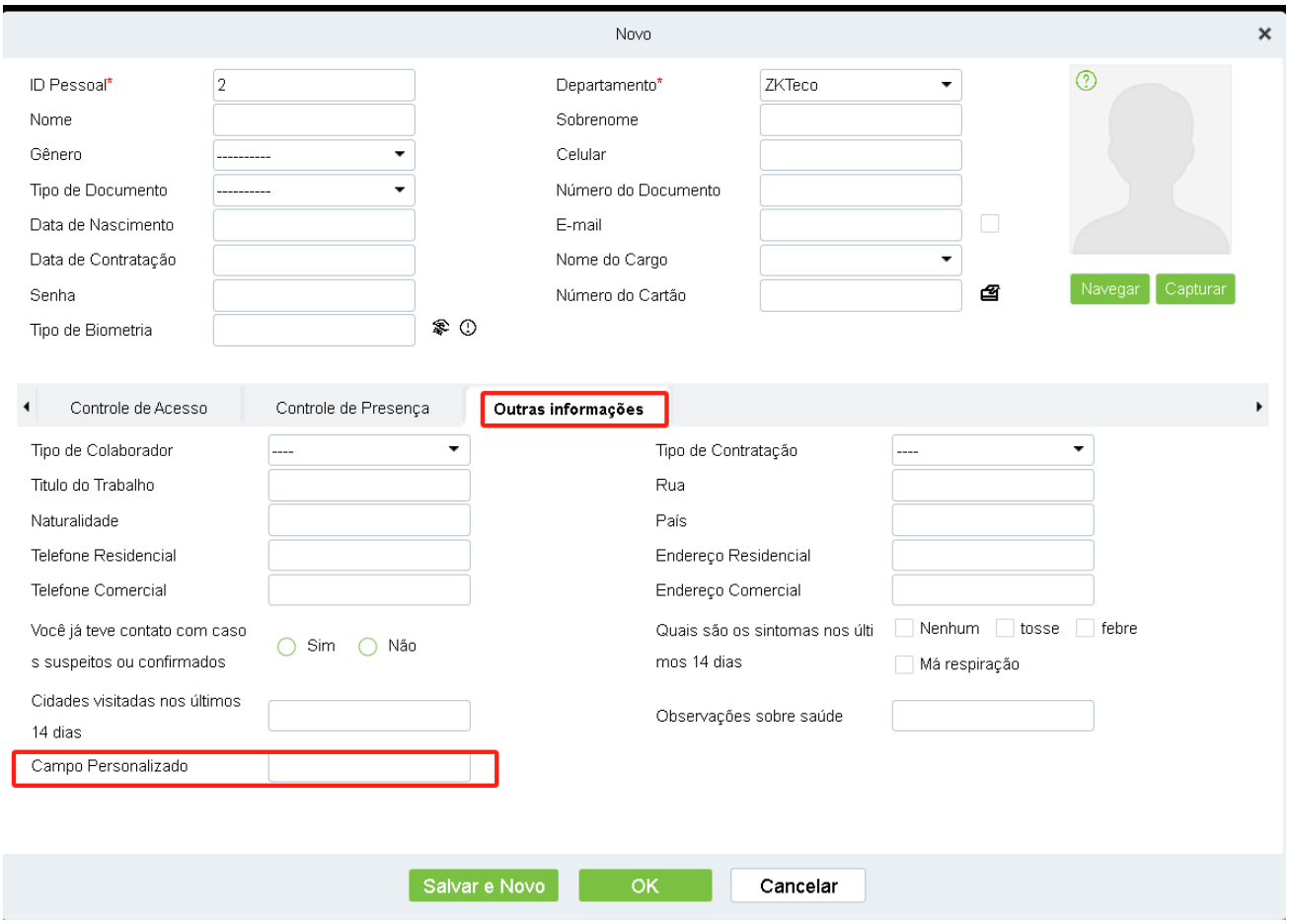
Clique em **[Pessoal]** > **[Gestão de Pessoal]** > **[Atributos Personalizados]** > **[Novo]**, depois edite os parâmetros e clique em **[OK]** para salvar e sair.



Os campos são os seguintes:

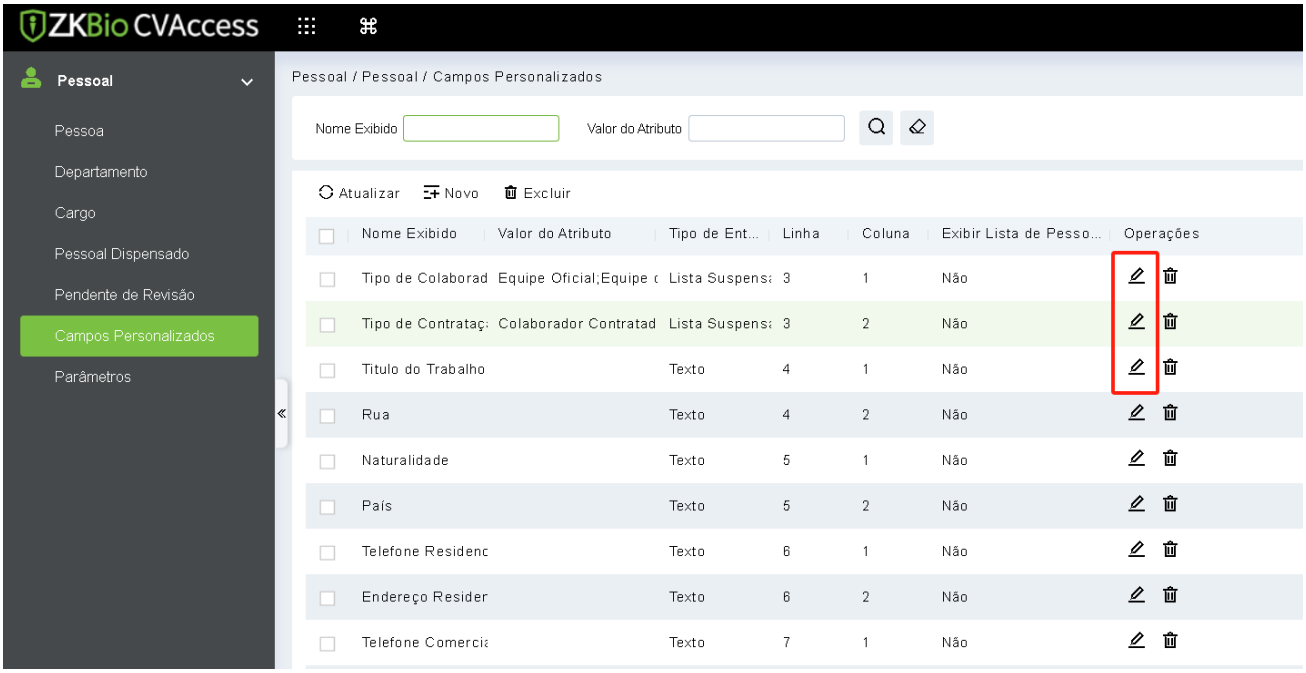
- **Nome de Exibição:** Deve ser preenchido e não deve ser repetido. O comprimento máximo é de 30 caracteres.

- **Tipo de Entrada:** Selecione o tipo de exibição entre "Lista Suspensa", "Escolha Múltipla", "Escolha Única" e "Texto".
- **Valor do Atributo:** Adequado para listas exibidas como 'Lista Suspensa', 'Escolha Múltipla' e 'Escolha Única'. Use ";" para distinguir os valores múltiplos. Se o tipo de entrada for "Texto", o valor do atributo não será adequado.
- **Linha/Coluna:** A coluna e a linha de um campo são usadas juntas para controlar a posição de exibição do campo. Números são suportados. O número da coluna pode ser 1 ou 2, e o número da linha pode ser apenas de 3 a 20. A combinação de coluna e linha não deve ser duplicada. Como mostrado na figura a seguir, o Tipo de Funcionário está na primeira coluna e na primeira linha, e o Tipo de Contratação está na primeira coluna e na segunda linha.



3.1.6.2 Editando um Atributo Personalizado

Clique em para modificar os atributos correspondentes.



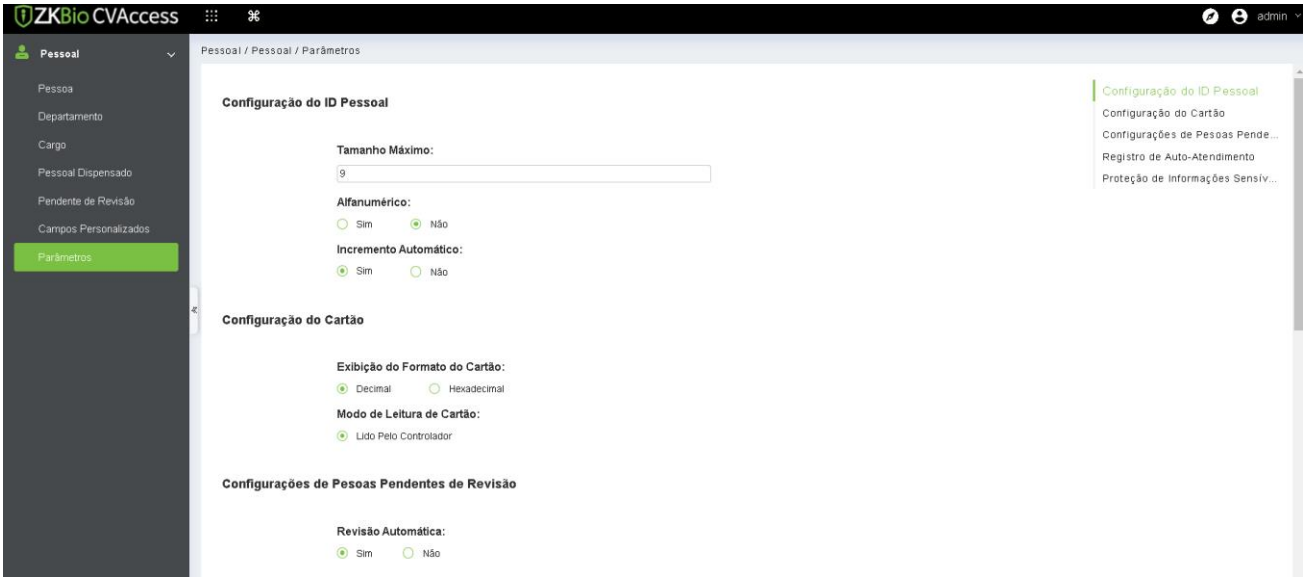
3.1.6.3 Excluindo um Atributo Personalizado

Clique em **[Excluir]** para excluir um atributo não utilizado. Se o atributo estiver em uso, o sistema exibirá uma confirmação antes de confirmar a exclusão.

Nota: O atributo personalizado não poderá ser recuperado uma vez excluído.

3.1.7 Parâmetros

1. Clique em **[Pessoal] > [Gestão de Pessoal] > [Parâmetros].**



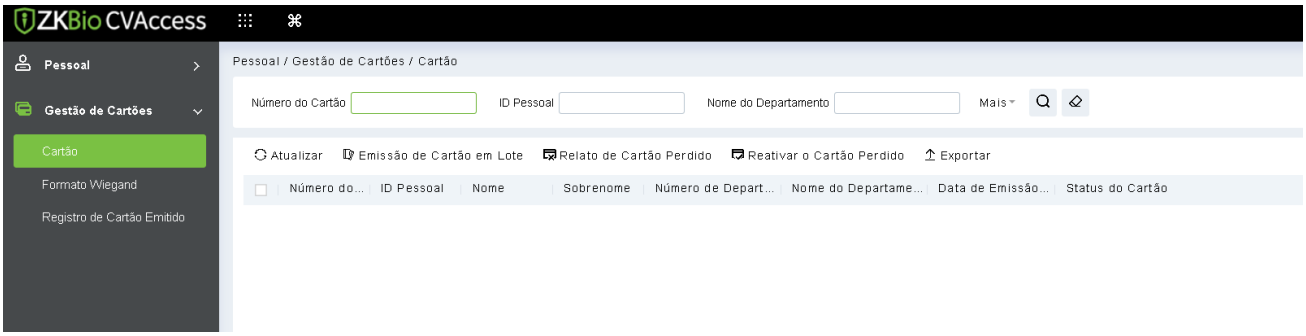
2. Você pode definir o comprimento máximo para um ID de Pessoal e se ele suportará letras ou não. Se a incrementação automática do ID de Pessoal for selecionada como Sim, então ao adicionar pessoal, o ID no campo será atualizado automaticamente para o próximo novo número sucessor.
3. Defina o comprimento máximo (número binário) do número do cartão que o sistema atual suportará.
4. Defina o formato do cartão atualmente usado no sistema. O formato do cartão não pode ser alterado após ser configurado.
5. Clique em [OK] para salvar as configurações e sair.

3.2 Gestão de Cartões

Existem três módulos na gestão de cartões: Cartão, Formato Wiegand e Registro de Emissão de Cartão.

3.2.1 Cartão

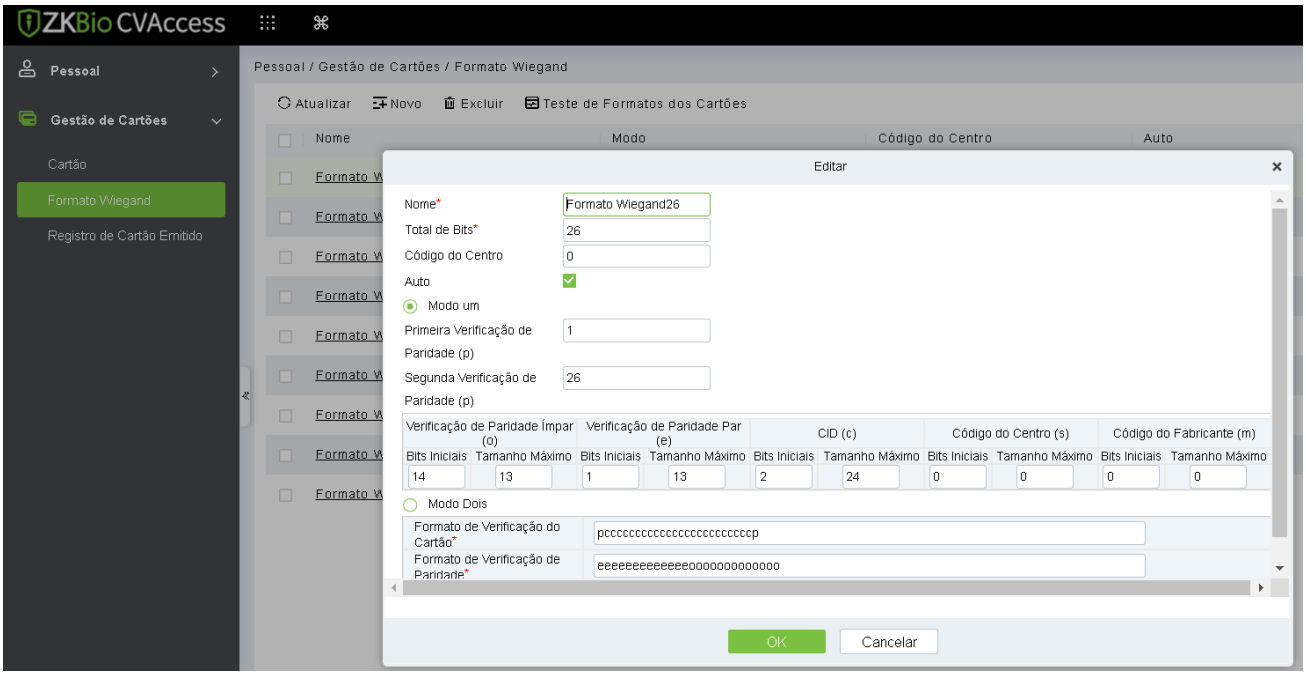
Mostra os cartões emitidos no sistema com seus status.



3.2.2 Formato Wiegand

O Formato Wiegand é o formato de cartão que pode ser identificado pelo leitor Wiegand. O software está incorporado com 9 formatos Wiegand. Você pode configurar o formato do cartão Wiegand conforme necessário.

Este software suporta dois modos para adicionar Formato Wiegand, se o modo 1 não atender aos requisitos de configuração, você pode alterá-lo para o modo 2. Tomando o Formato Wiegand 37 como exemplo:



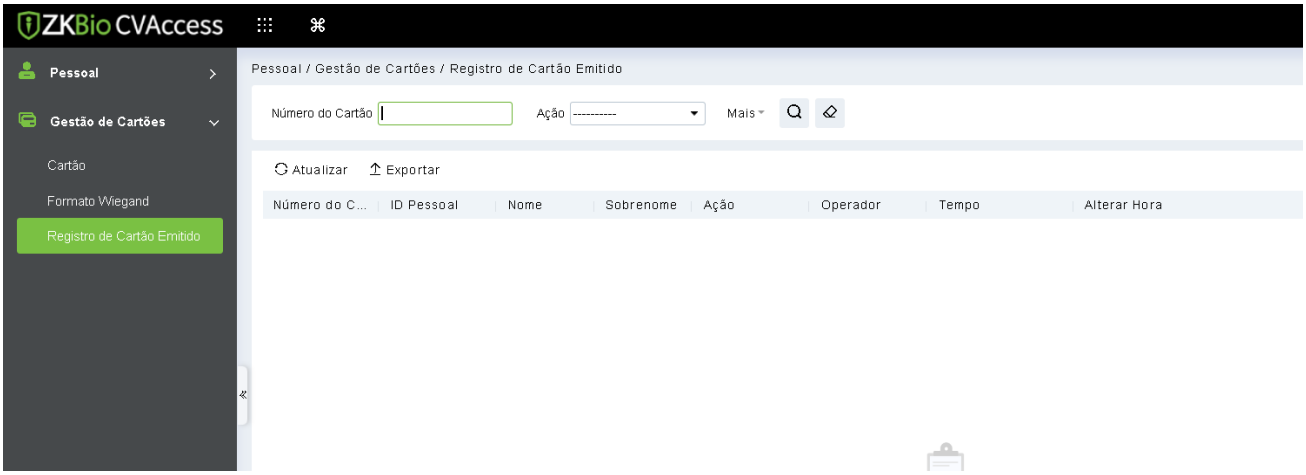
Especificação de Formato:

"P" indica Posição de Paridade; "s" indica Código de Site; "c" indica ID do Titular do Cartão; "m" indica Código do Fabricante; "e" indica Paridade Par; "O" indica Paridade Ímpar; "b" indica verificação tanto par como ímpar; "x" indica bits de paridade sem verificação.

O Formato Wiegand 37 anterior: os primeiros bits de paridade (p) verificam "eeeeeeeeeeeeeeeeee"; os segundos bits de paridade verificam "ooooooooooooooooooo". O Formato de Verificação de Cartão só pode ser configurado como "p, x, m, c, s"; O Formato de Verificação de Paridade só pode ser configurado como "x, b, o, e".

3.2.3 Registro de Emissão de Cartão

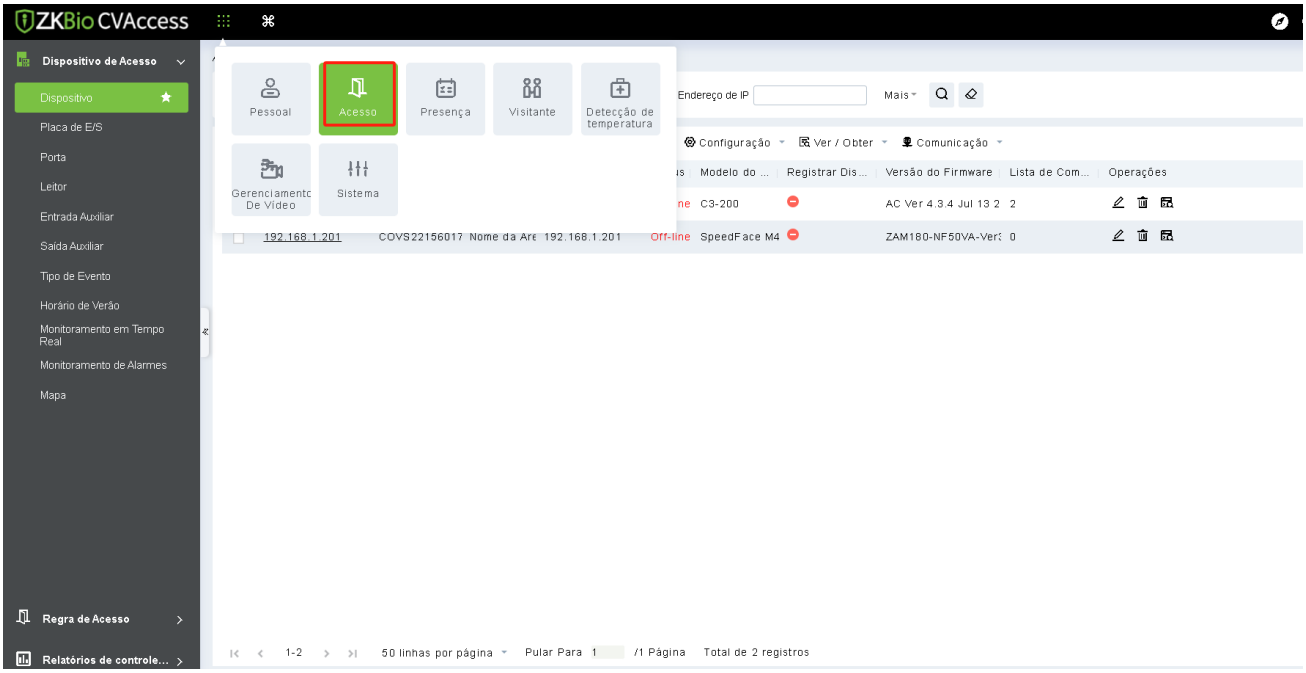
Registra o ciclo de vida de um cartão e exibirá as operações realizadas no cartão.



Nota: Os cartões e registros de emissão de cartão de um funcionário serão excluídos completamente quando a conta do funcionário for excluída.

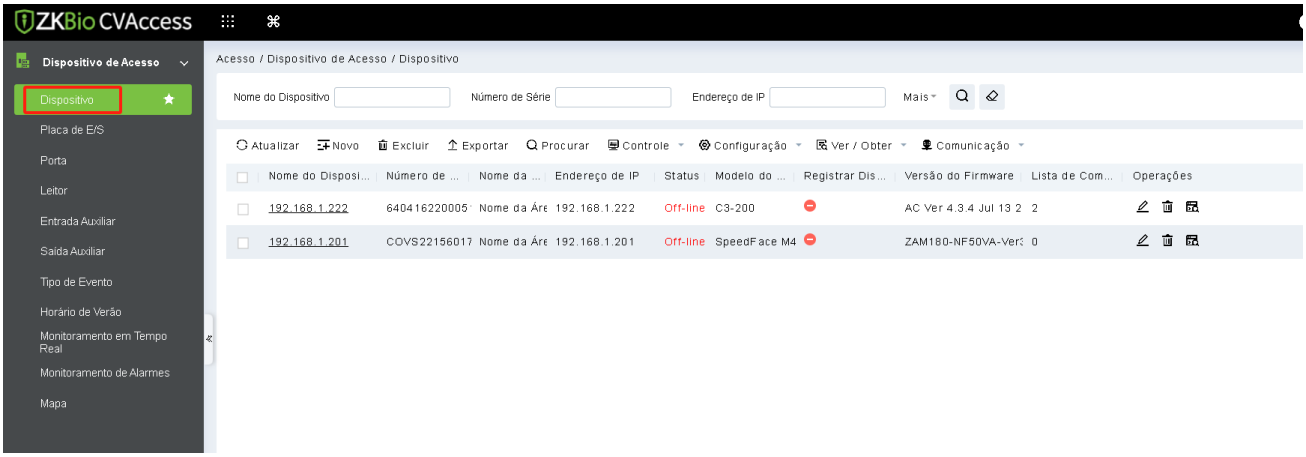
4 Acesso

O sistema precisa estar conectado a um controlador de acesso para fornecer funções de controle de acesso. Para usar essas funções, os usuários devem instalar dispositivos e conectá-los à rede primeiro, em seguida, configurar os parâmetros correspondentes, para que possam gerenciar dispositivos, fazer upload de dados de controle de acesso, baixar informações de configuração, gerar relatórios e alcançar o gerenciamento digital da empresa.



4.1 Dispositivo

Adicione um dispositivo de acesso, em seguida, defina os parâmetros de comunicação dos dispositivos conectados, incluindo configurações do sistema e configurações do dispositivo. Quando a comunicação é bem-sucedida, você pode visualizar aqui as informações dos dispositivos conectados e realizar monitoramento remoto, upload e download, etc.



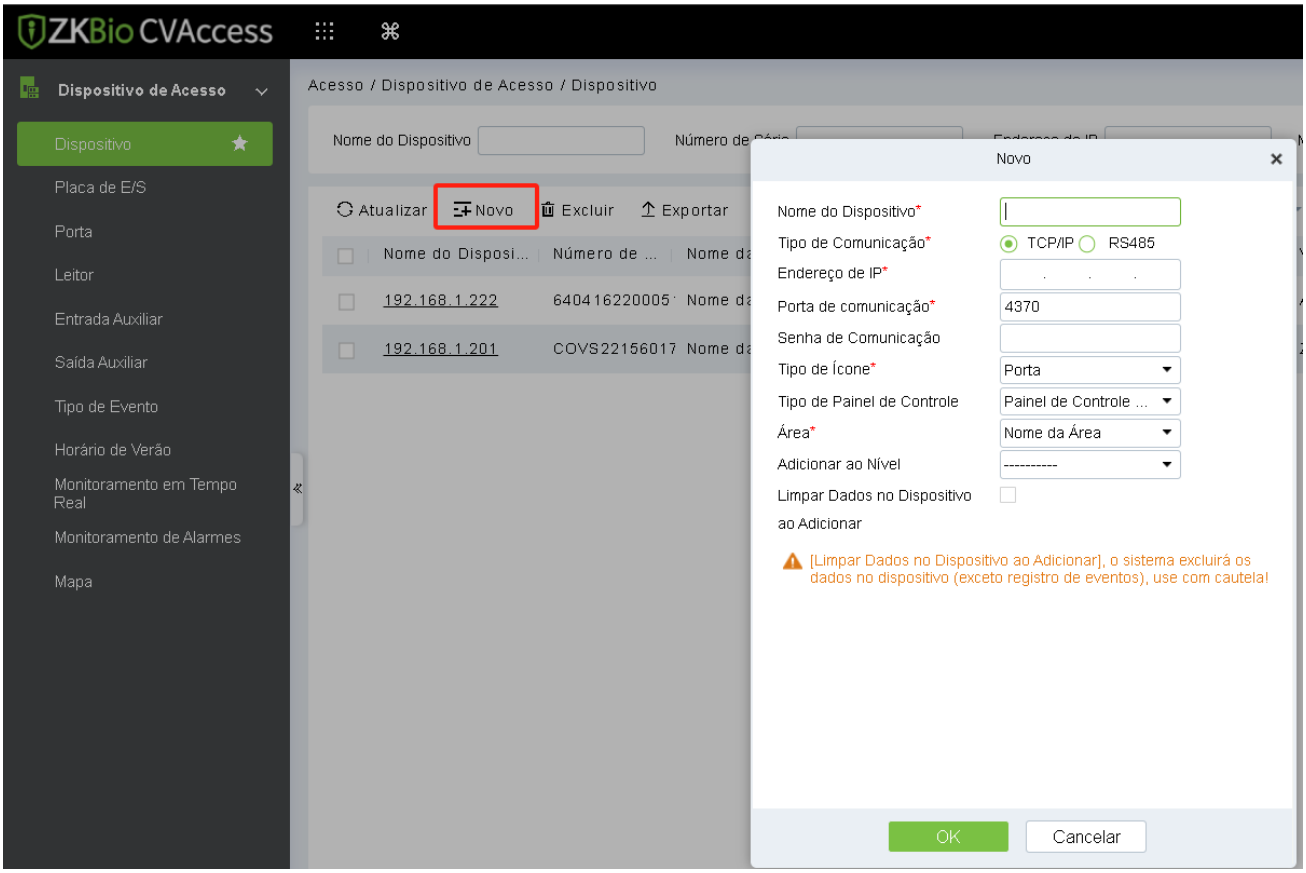
4.1.1 Dispositivo

4.1.1.1 Adicionar Dispositivo

Existem duas maneiras de adicionar Dispositivos de Acesso.

Adicionar Dispositivo Manualmente

Clique em **[Acesso] > [Dispositivo] > [Novo]** no Menu de Ações, a seguinte interface será exibida:



Os campos são os seguintes:

- **Nome do Dispositivo:** Qualquer caractere, até uma combinação de 20 caracteres.
- **Endereço IP:** Insira o Endereço IP do dispositivo.
- **Porta de Comunicação:** O valor padrão é 4370.
- **Senha de Comunicação:** A senha deve ser uma combinação de números e letras de 6 dígitos.

Notas:

(1) Você não precisa inserir este campo se for um dispositivo de fábrica novo ou acabou de ser inicializado.

(2) Quando a senha de comunicação para o dispositivo autônomo é definida como "0", significa que não há senha. No entanto, no caso do painel de controle de acesso, significa que a senha é 0.

(3) Você precisa reiniciar o dispositivo após configurar o sensor de porta do dispositivo autônomo.

- **Tipo de Ícone:** Ele definirá a representação do dispositivo. Você pode escolher de acordo com o tipo de dispositivo; Porta e Barreira de Giro.
- **Tipo de Painel de Controle:** Painel de controle de acesso de uma porta, painel de controle de acesso de duas portas, painel de controle de acesso de quatro portas, Dispositivo Autônomo.
- **Área:** Selecione áreas específicas de dispositivos. Após configurar as áreas, os dispositivos (portas) podem ser filtrados por áreas durante o Monitoramento em Tempo Real.

- **Adicionar ao Nível:** Adicione automaticamente o dispositivo ao nível selecionado. O dispositivo não pode ser adicionado automaticamente ao nível selecionado se o número de pessoal exceder 5000. Você pode adicionar pessoal após o dispositivo ser adicionado com sucesso.
- **Limpar Dados no Dispositivo ao Adicionar:** Se esta opção estiver marcada, o sistema limpará todos os dados no dispositivo (exceto os logs de eventos). Se você estiver adicionando o dispositivo apenas para demonstração ou teste, não é necessário selecioná-lo.

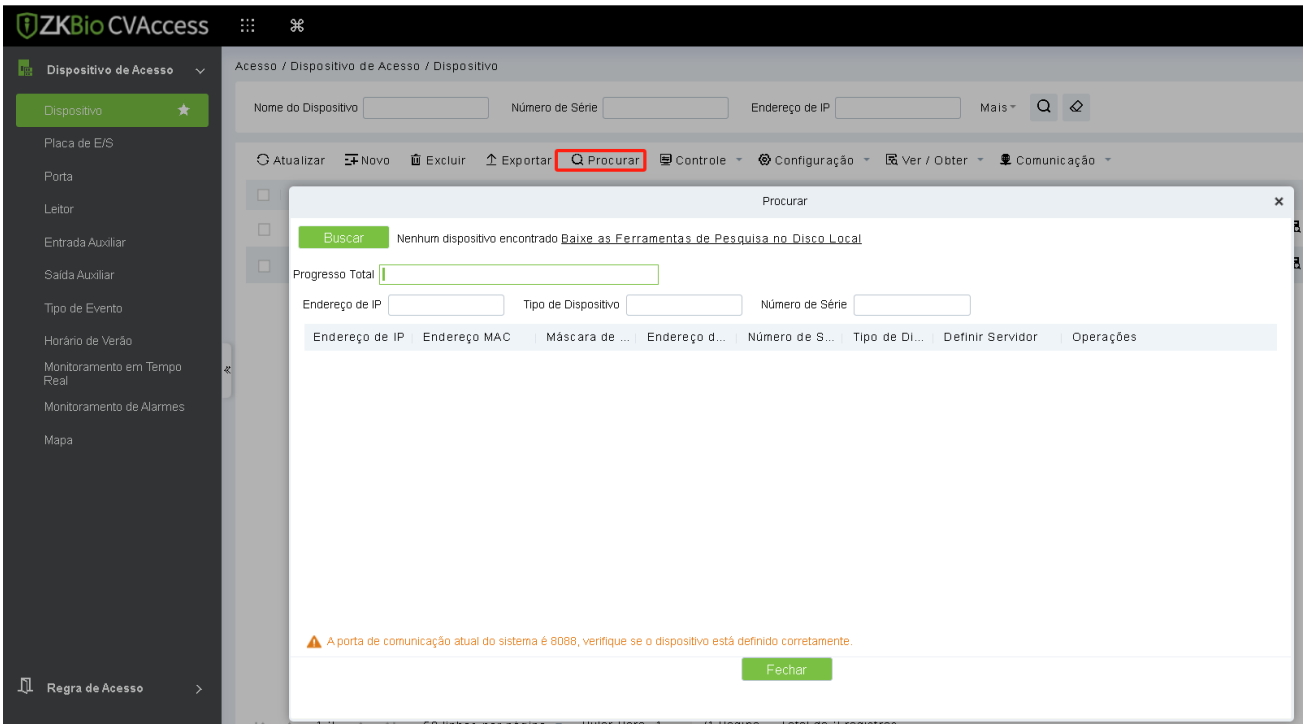
Após editar, clique em [OK], e o sistema tentará conectar o dispositivo atual.

Se a conexão for bem-sucedida, ele lerá os parâmetros estendidos correspondentes do dispositivo.

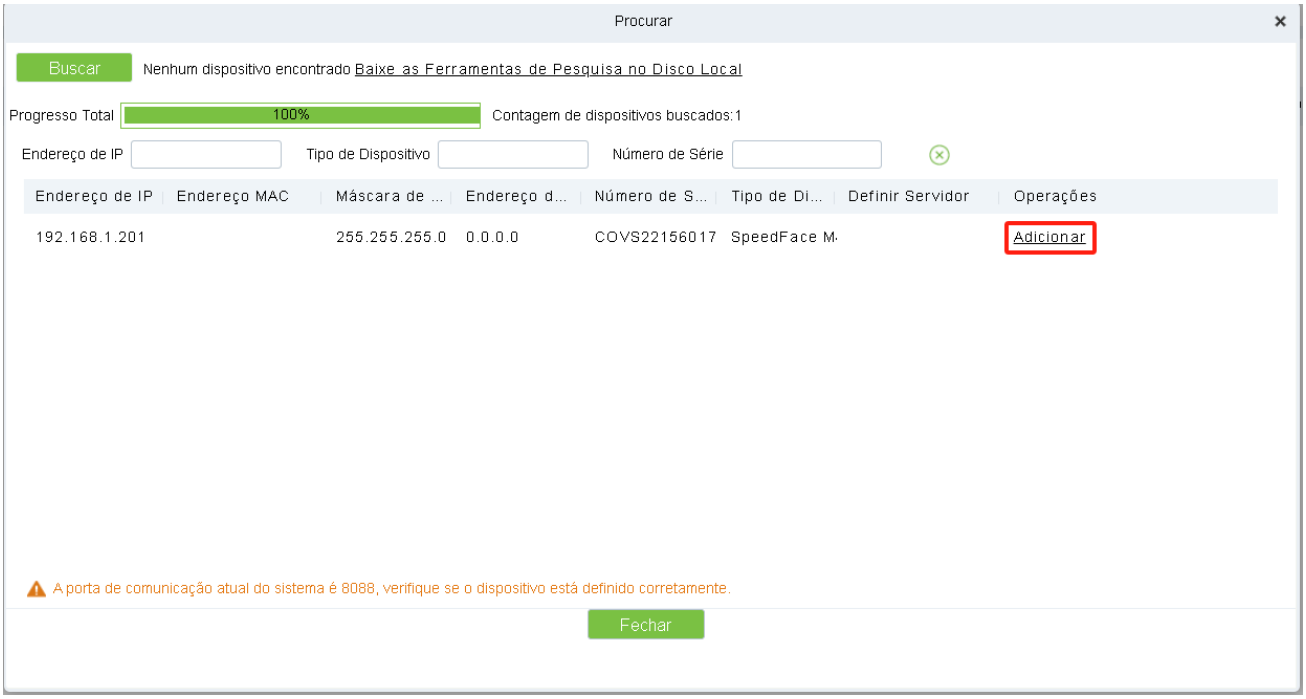
Nota: Ao excluir um dispositivo novo, o software limpará todas as informações do usuário, fusos horários, feriados e configurações de níveis de controle de acesso (incluindo níveis de acesso, anti-pass back, configurações de intertravamento, configurações de ligação, etc.) do dispositivo, exceto os registros de eventos (a menos que as informações no dispositivo sejam inutilizáveis, ou seja recomendável não excluir o dispositivo usado para evitar perda de informações).

Adicionar Dispositivo por Busca de Controladores de Acesso

1. Clique em [Acesso] > [Dispositivo] > [Buscar], para abrir a interface de Busca.



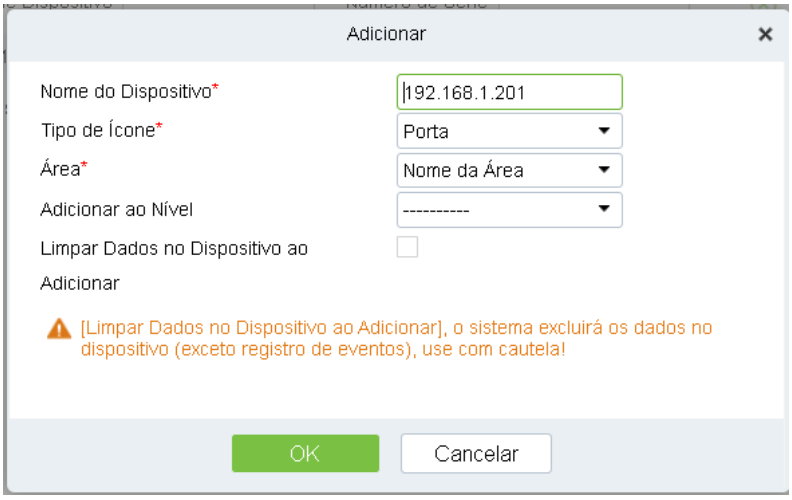
2. Clique em **[Buscar],** e ele mostrará "Buscando...".
3. Após a busca ser concluída, a lista e o número total de controladores de acesso serão exibidos.



Nota: O modo de transmissão UDP broadcast será usado para buscar dispositivos de acesso. Este modo não pode realizar uma função de cruzamento de roteador. O endereço IP pode fornecer segmentos de rede cruzados, mas deve estar na mesma sub-rede e precisará configurar o gateway e o endereço IP no mesmo segmento de rede.

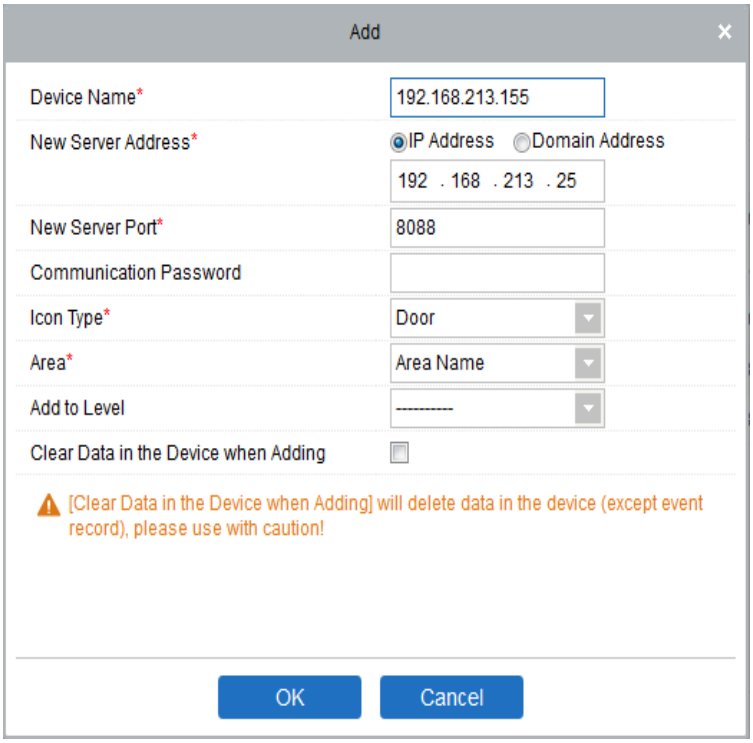
Clique em [Adicionar] na lista de busca.

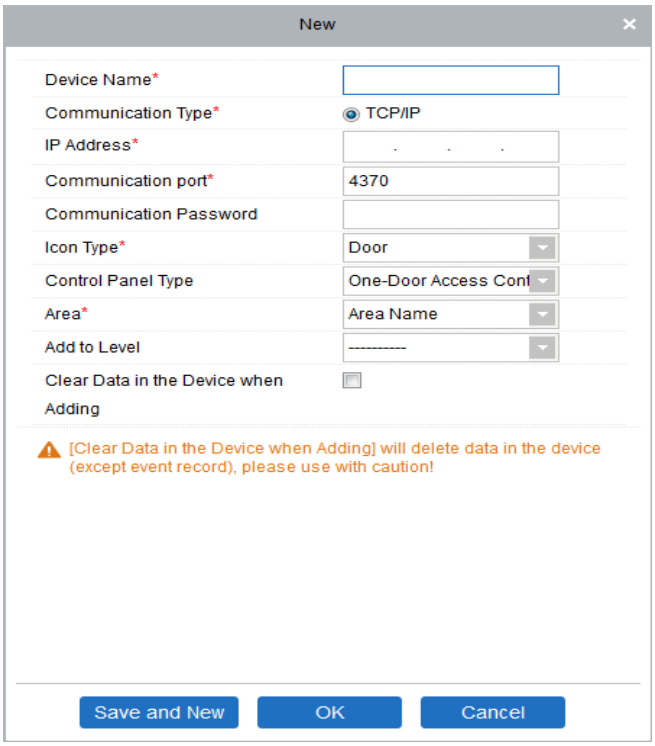
Se o dispositivo for um dispositivo de tração, você pode inserir um nome de dispositivo e clicar em [OK] para concluir a adição do dispositivo.



- **Limpar Dados no dispositivo ao Adicionar:** Se esta opção for selecionada, após adicionar o dispositivo, o sistema limpará todos os dados no dispositivo (exceto os logs de eventos).

Se o dispositivo for um dispositivo com firmware de push, a seguinte janela aparecerá após clicar em [Adicionar]. Se o Endereço IP em [Novo Endereço do Servidor] for selecionado, então configure o endereço IP e o número da porta. Se o Endereço do Domínio na opção [Novo Endereço do Servidor] for selecionado, então configure o endereço do domínio, número da porta e DNS. O dispositivo será adicionado ao software automaticamente.





- **Novo Endereço do Servidor:** Para adicionar um dispositivo pelo endereço IP ou endereço de domínio, os dispositivos podem ser adicionados ao software inserindo o endereço de domínio.
- **Nova Porta do Servidor:** Define o ponto de acesso do sistema.
- **DNS:** Configura um endereço DNS do servidor.
- **Limpar Dados no Dispositivo ao Adicionar:** Se esta opção for selecionada, então após adicionar o dispositivo, o sistema limpará todos os dados no dispositivo (exceto os logs de eventos). Se você adicionar o dispositivo apenas para demonstração ou teste, não é necessário selecioná-lo.

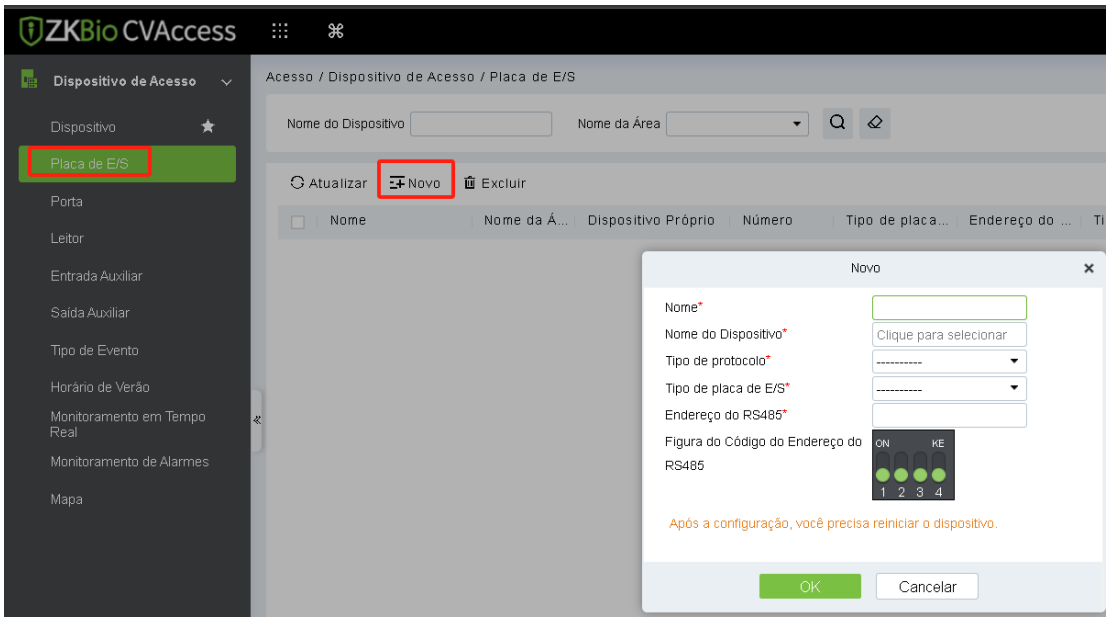
Nota: Ao usar qualquer um dos três métodos de adição de dispositivo acima, se houver dados residuais no dispositivo original, sincronize os dados originais nele após adicionar um novo dispositivo ao software clicando em [Dispositivo] > [Sincronizar Todos os Dados nos Dispositivos], caso contrário, esses dados originais podem entrar em conflito com o uso normal.

(1) O endereço IP padrão do dispositivo de acesso pode entrar em conflito com o IP de um dispositivo na rede local. Você pode modificar seu endereço IP: clique em [Modificar Endereço IP] ao lado de [Adicionar] e uma caixa de diálogo será exibida na interface. Insira o novo endereço IP e outros parâmetros (Nota: Configure o gateway e o endereço IP no mesmo segmento de rede).

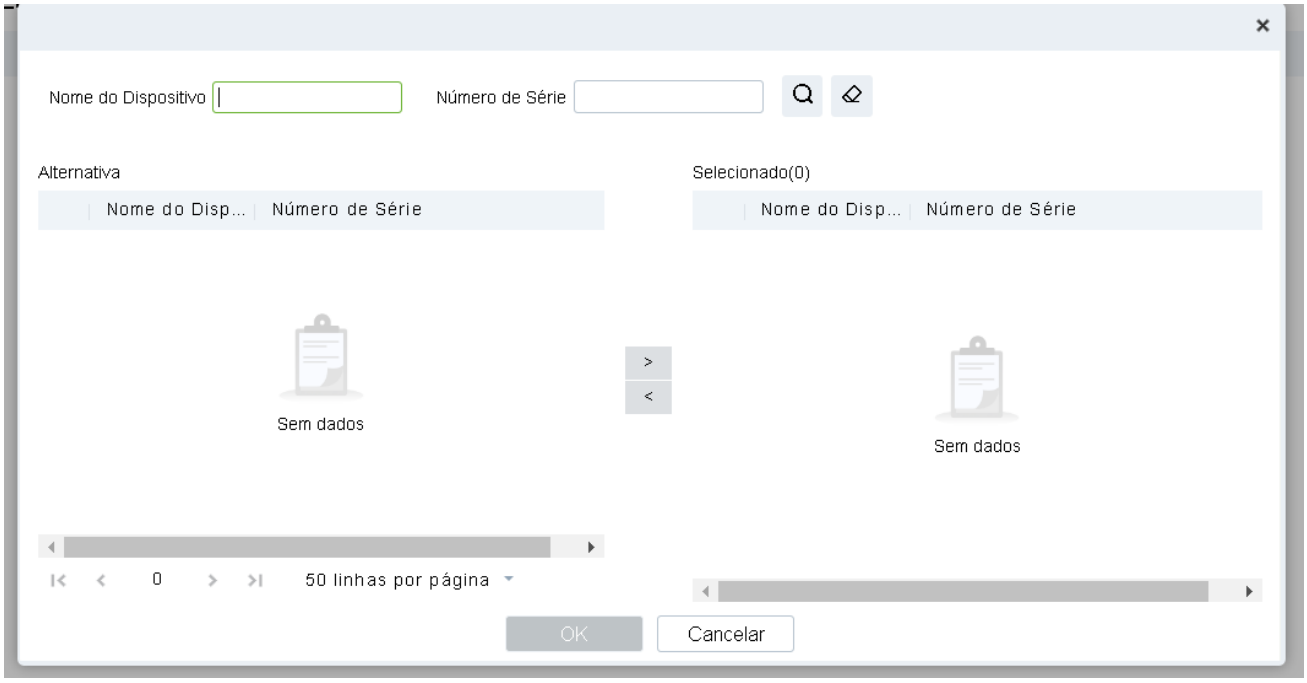
Nota: Alguns dispositivos PUSH suportam SSL. Para usar essa função, selecione a porta HTTPS durante a instalação do software e certifique-se de que o firmware do dispositivo suporte SSL.

4.1.2 Placa de Entrada/Saída

No módulo de dispositivo, clique em [Dispositivo]> [Placa de Entrada/Saída]> [Novo] para adicionar o dispositivo de Placa de Entrada/Saída ao software.



Digite o nome da Placa de Entrada/Saída. Selecione o Dispositivo clicando no campo Nome do Dispositivo. A lista de dispositivos aparece conforme mostrado abaixo:



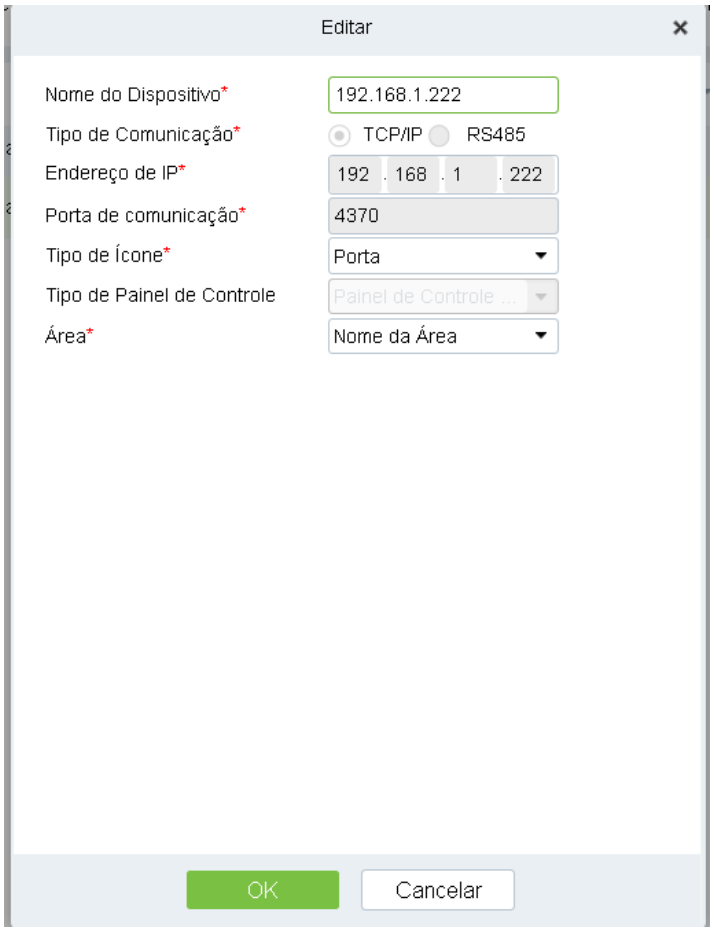
Selecione o dispositivo e clique em OK. Selecione o Tipo de Placa de Entrada/Saída. Configure o Endereço do Código RS485 alterando o botão correspondente. Clique em OK para salvar os detalhes. Você pode visualizar todas as entradas auxiliares na interface [Entrada Auxiliar].

4.1.3 Operação do Dispositivo

Para a comunicação entre o sistema e o dispositivo; upload de dados, download de configuração, parâmetros do dispositivo e sistema devem ser configurados. Os usuários podem editar controladores de acesso dentro dos níveis relevantes no sistema atual; os usuários só podem adicionar ou excluir dispositivos na Gestão de Dispositivos, se necessário.

4.1.3.1 Editar ou Excluir um Dispositivo

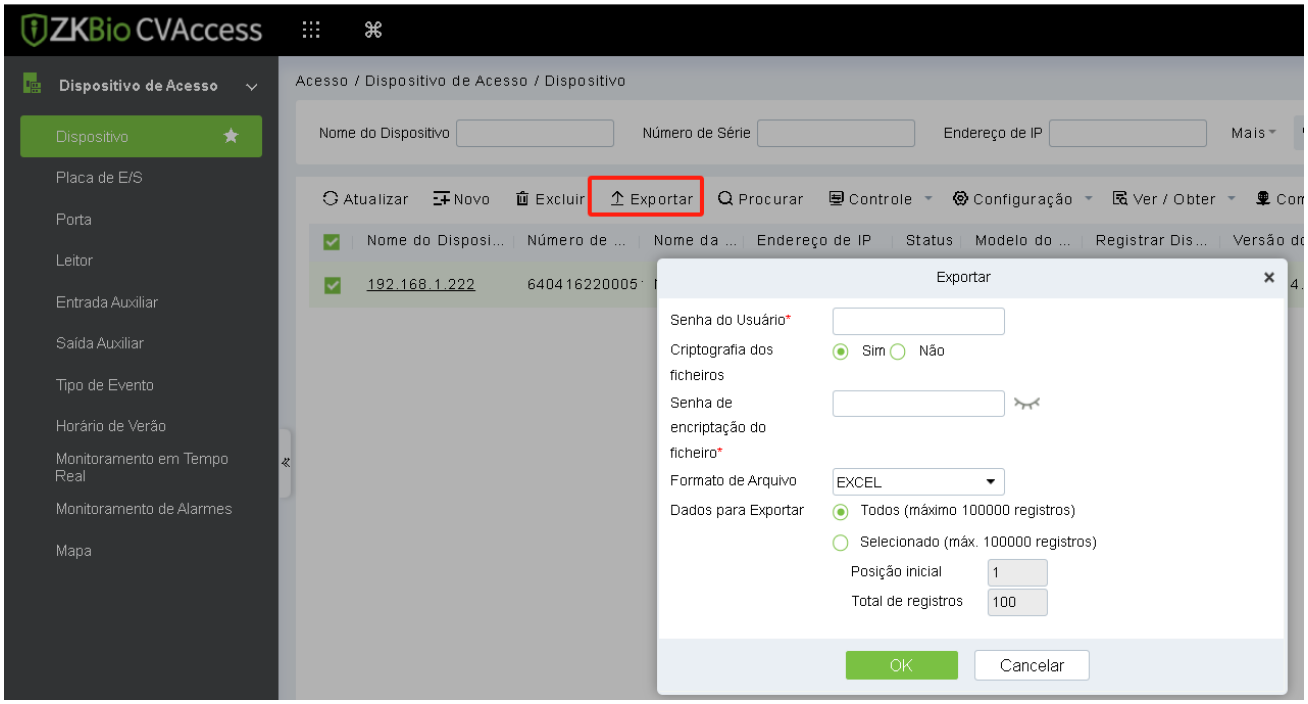
- **Editar:** Clique no Nome do Dispositivo ou clique em [Editar] para acessar a interface de edição.
- **Excluir:** Selecione o dispositivo, clique em [Excluir] e clique em [OK] para excluir o dispositivo.



Para os detalhes e configurações dos parâmetros acima, consulte o Dispositivo. Alguns detalhes não podem ser editados. O Nome do Dispositivo deve ser único e não pode ser idêntico a outro dispositivo. O Tipo de Painel de Controle não pode ser modificado. Se o tipo estiver errado, os usuários precisam excluir manualmente o dispositivo e adicioná-lo novamente.

4.1.3.2 Exportar

As informações do dispositivo podem ser exportadas nos formatos de arquivo EXCEL, PDF e CSV.

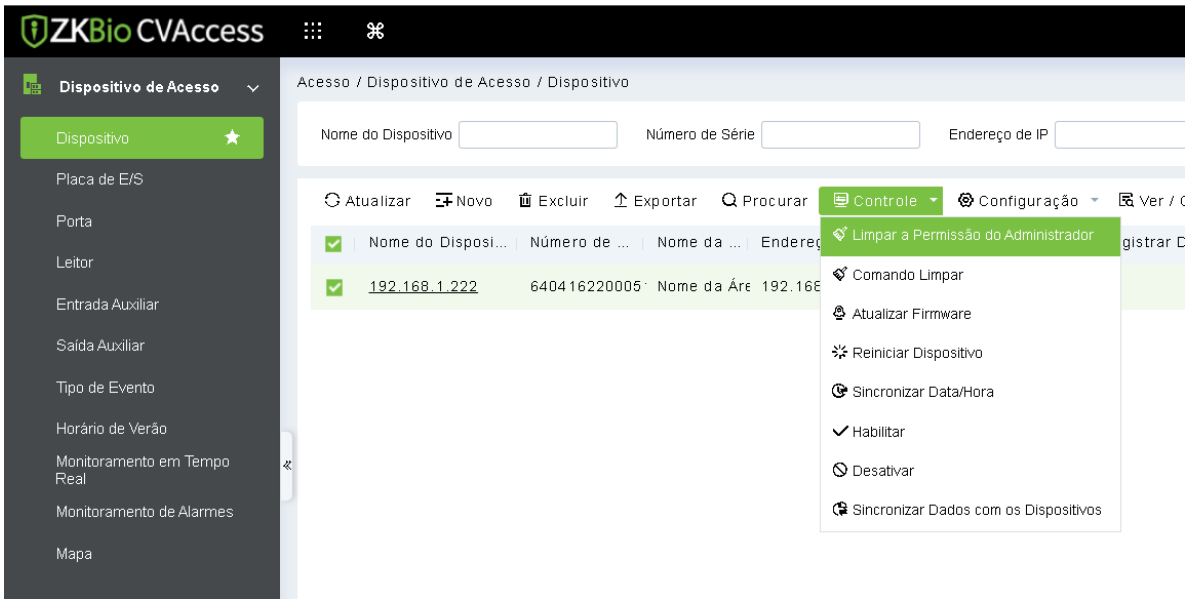


Device

Device Name	Serial Number	Area Name	Communication Type	Network Connection Mode	IP Address	RS485 Parameter	Status	Device Model	Register Device	Firmware Version
SpeedFace-V5	CGFE184760043	Area Name	HTTP	Wired	192.168.213.67		Offline	SpeedFace-V5	Yes	1.0.55

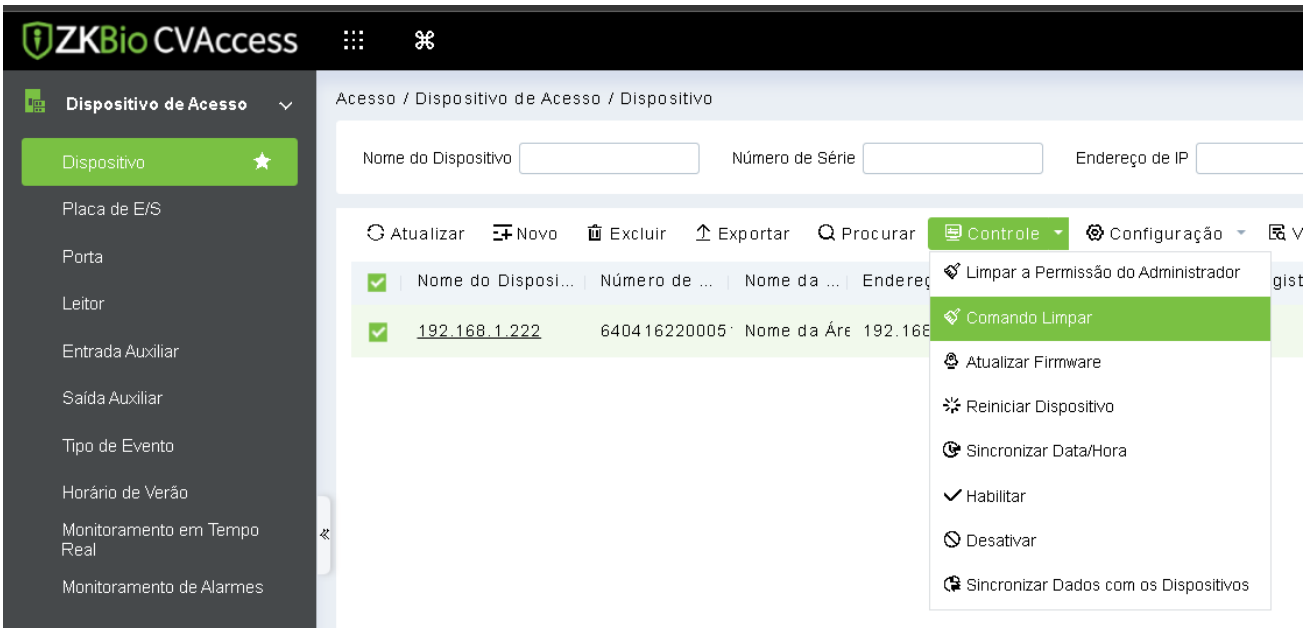
4.1.3.3 Limpar Permissão do Administrador

Selecione o dispositivo necessário, clique em [Limpar Permissão do Administrador] para limpar as permissões do administrador do dispositivo e clique em **[OK]** para concluir.



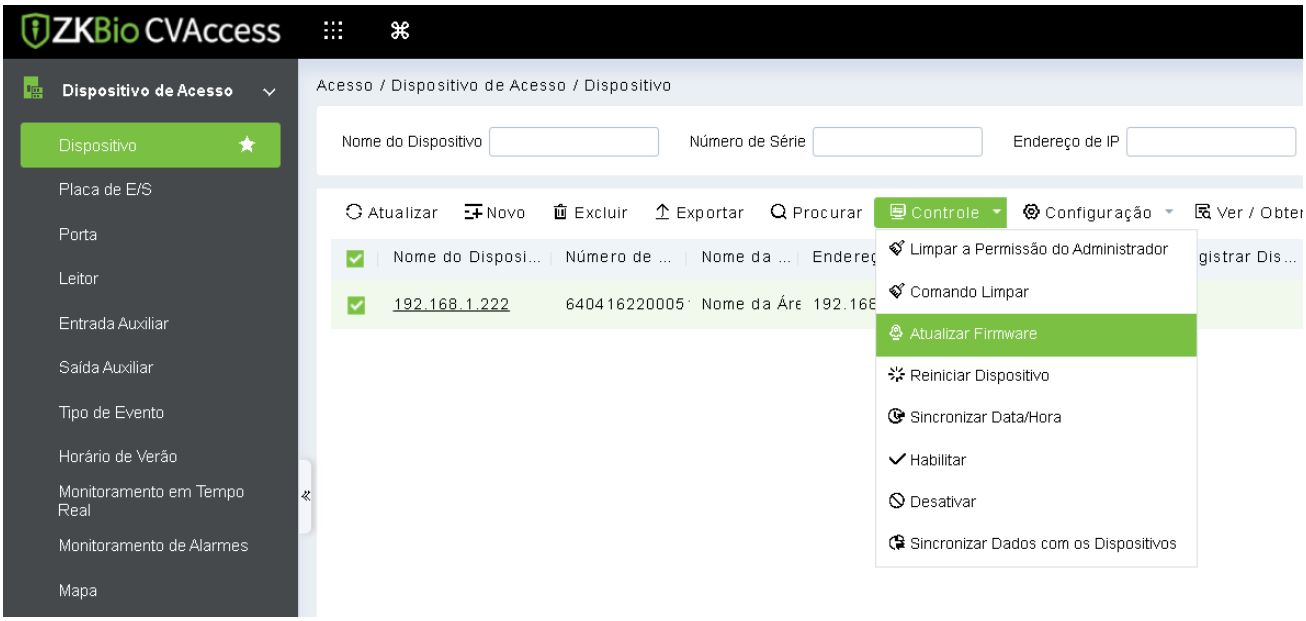
4.1.3.4 Comando de Limpeza

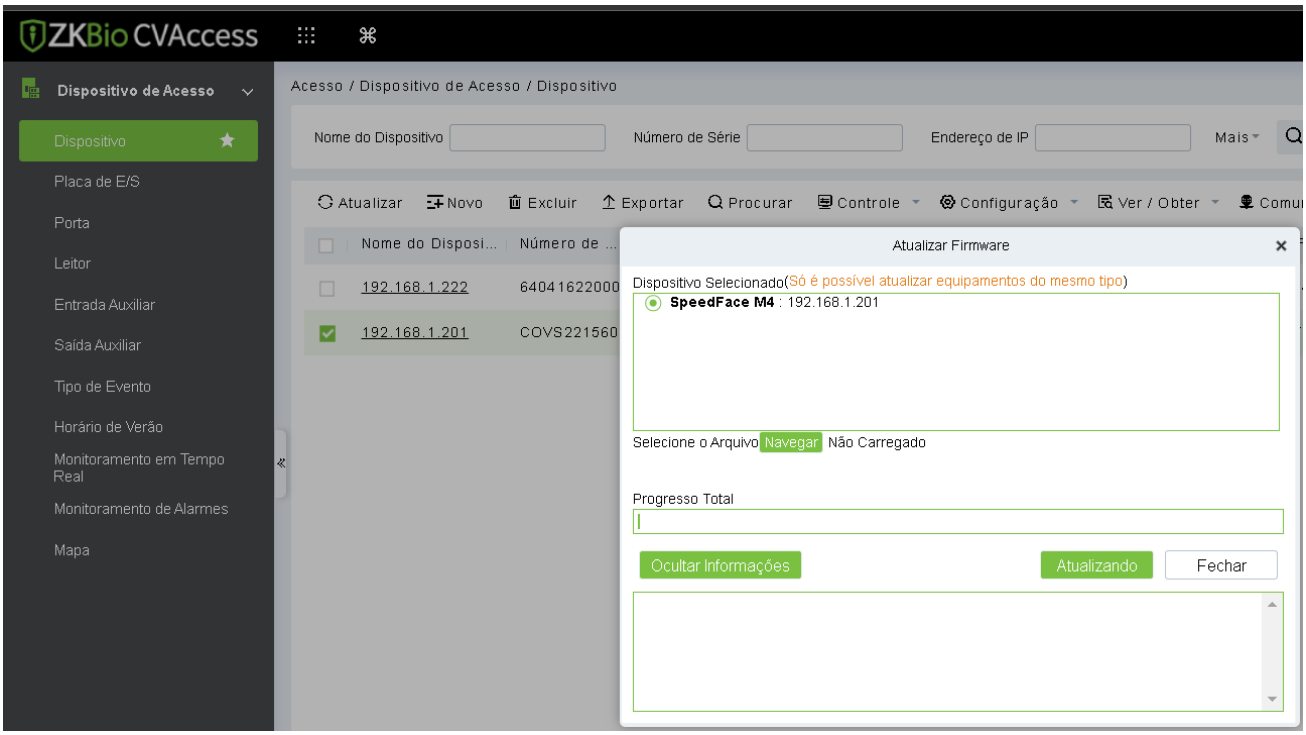
Selecione o dispositivo necessário, clique em **[Limpar Comando]** para limpar o comando sendo sincronizado com o dispositivo, e clique em **[OK]** para concluir.



4.1.3.5 Atualização de Firmware

Selecione o dispositivo necessário que precisa ser atualizado, clique em **[Atualizar firmware]** para entrar na interface de edição, em seguida, clique em **[Escolher Arquivo]** para selecionar o arquivo de atualização de firmware (nomeado emfw.cfg) fornecido pelo software de acesso, e clique em **[OK]** para iniciar a atualização.

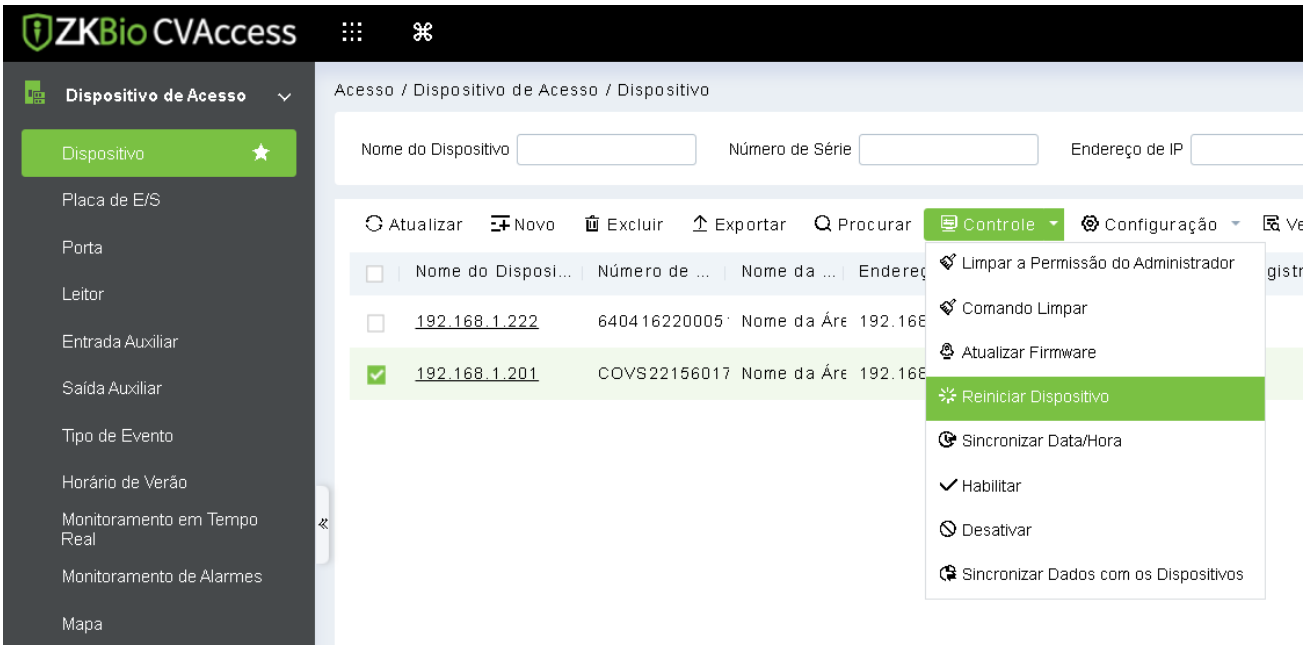




Nota: O usuário não deve atualizar o firmware sem autorização. Entre em contato com o distribuidor antes de atualizar o firmware ou atualize-o seguindo as instruções do distribuidor. A atualização não autorizada pode afetar as operações normais.

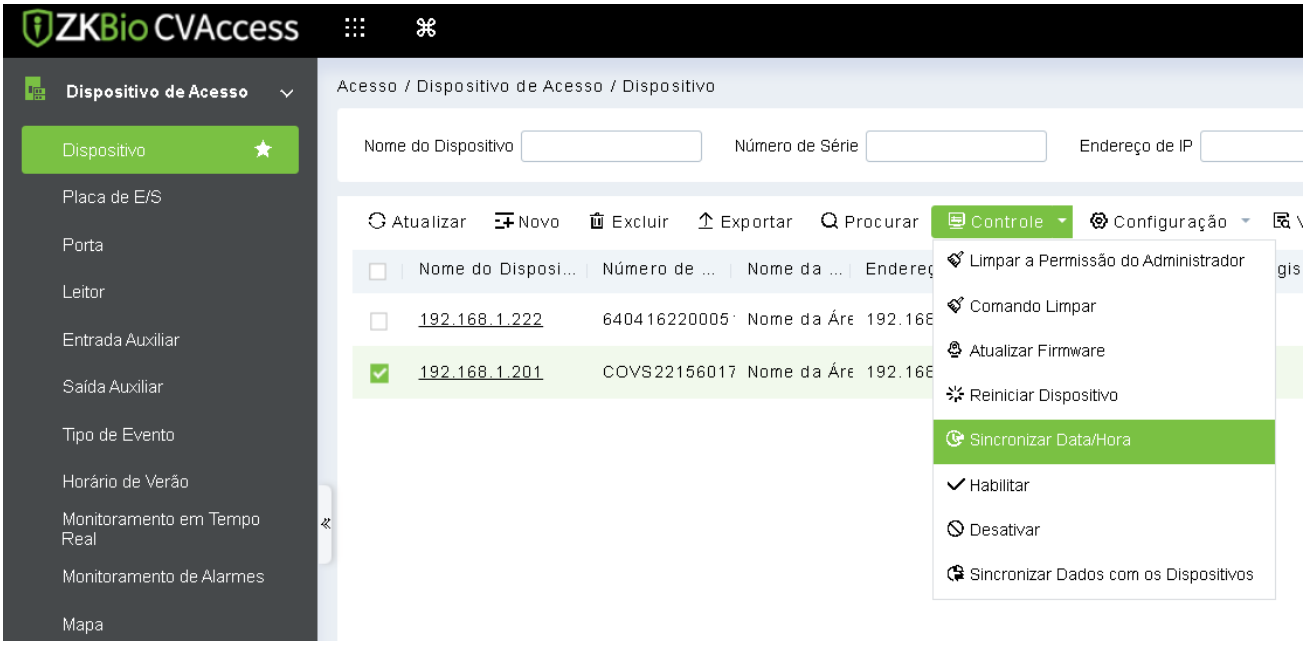
4.1.3.6 Reiniciar Dispositivo

Ele reiniciará o dispositivo selecionado.



4.1.3.7 Sincronizar Hora

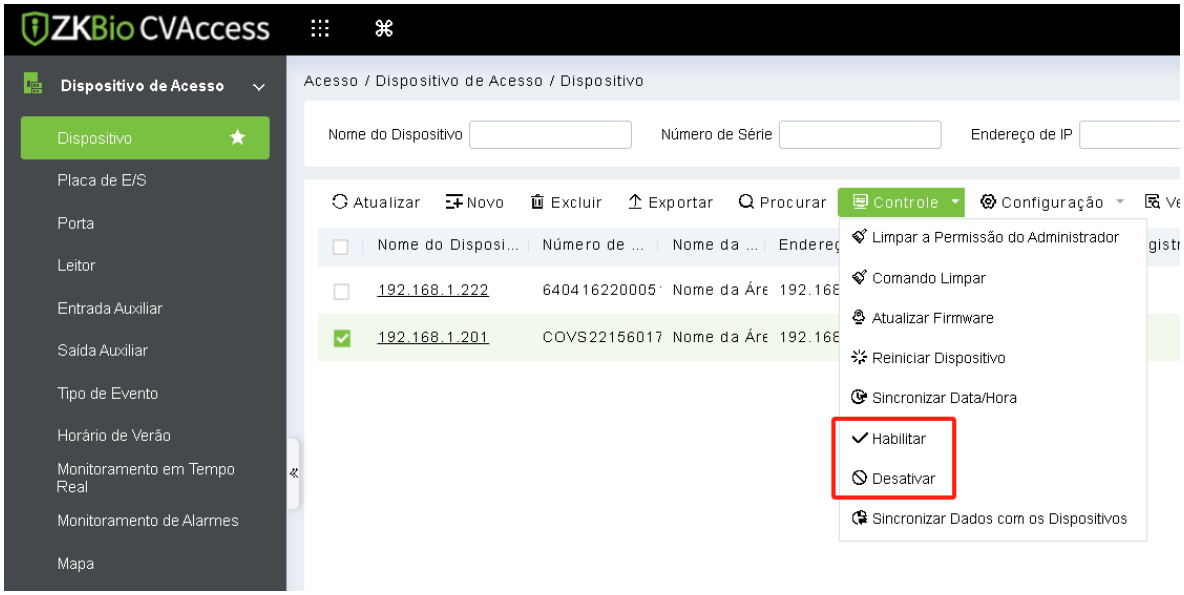
Ele sincronizará a hora do dispositivo com a hora atual do servidor.



4.1.3.8 Habilitar/Desativar

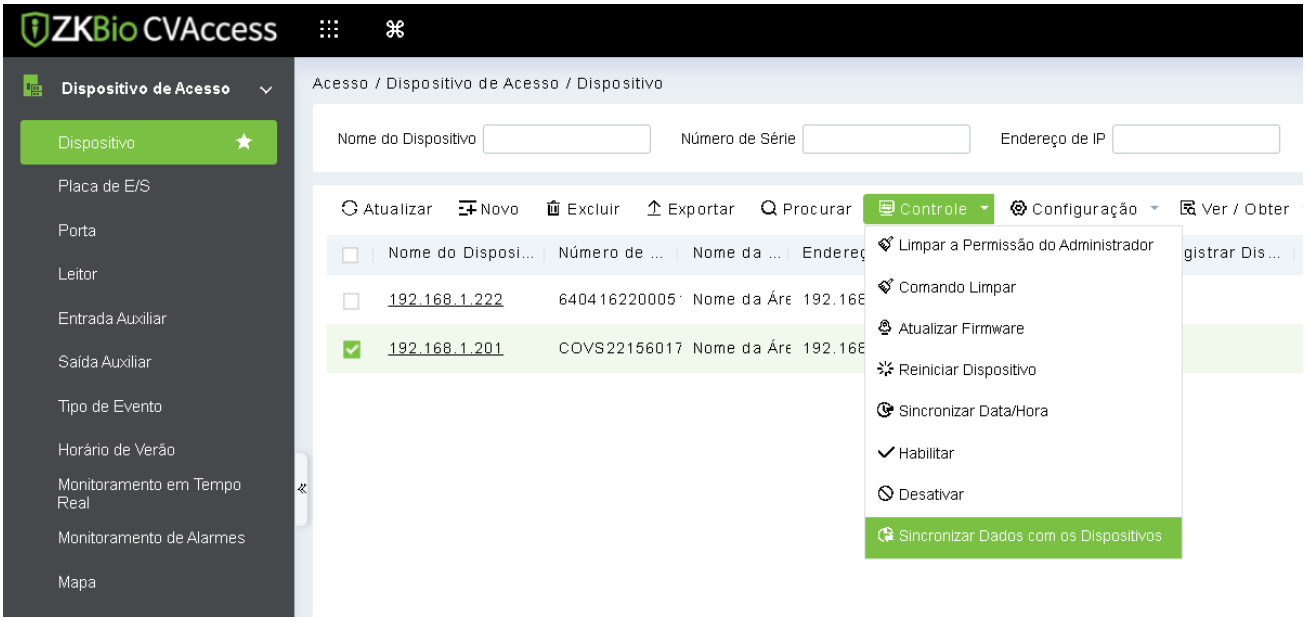
Selecione o dispositivo, clique em **[Desativar/Ativar]** para parar/iniciar o uso do dispositivo. Quando a comunicação entre o dispositivo e o sistema for interrompida ou o dispositivo falhar, o dispositivo pode

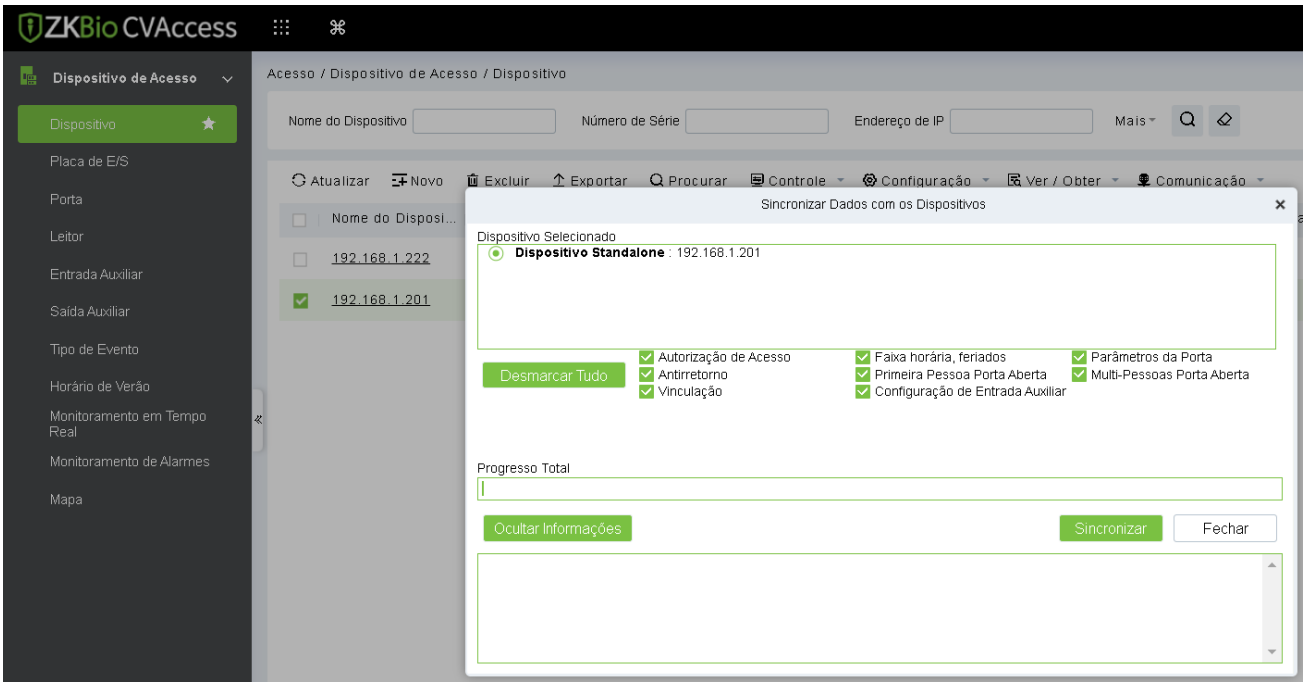
aparecer automaticamente no status desativado. Após ajustar a rede local ou o dispositivo, clique em [Ativar] para reconectar o dispositivo e restaurar a comunicação do dispositivo.



4.1.3.9 Sincronizar Todos os Dados nos Dispositivos

Sincronize os dados do sistema no dispositivo. Selecione o dispositivo, clique em **[Sincronizar Todos os Dados nos Dispositivos]** e clique em **[OK]** para completar a sincronização.

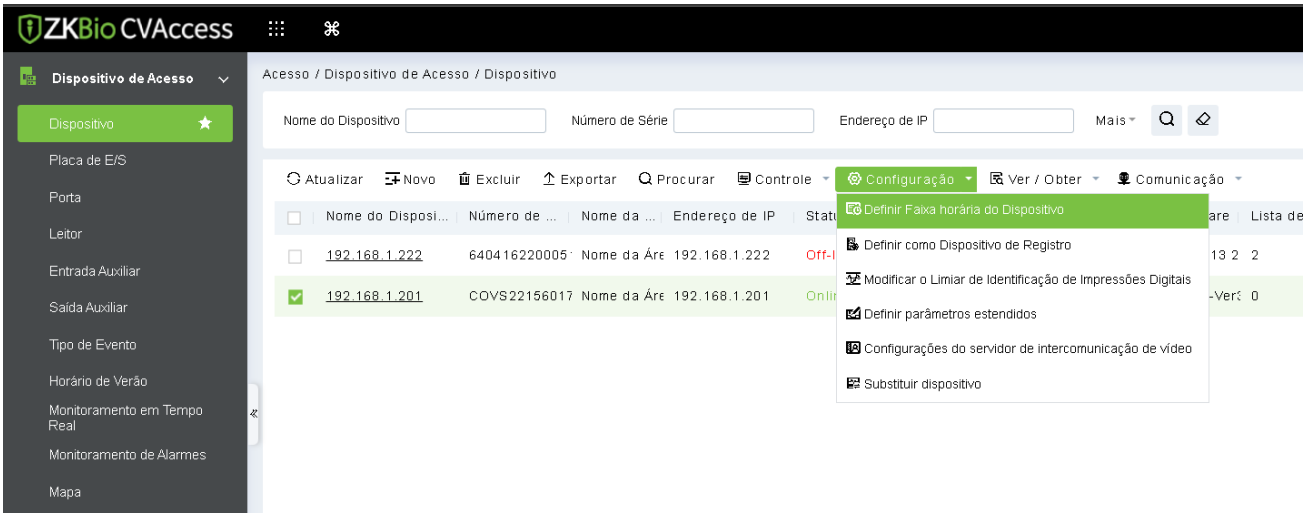




Nota: [Sincronizar Todos os Dados nos Dispositivos] irá apagar todos os dados no dispositivo primeiro (exceto transações), e então baixar todas as configurações novamente. Mantenha a conexão com a internet estável e evite situações de desligamento de energia. Se o dispositivo estiver funcionando normalmente, use essa função com cautela. Execute-a raramente para evitar impacto no uso normal do dispositivo.

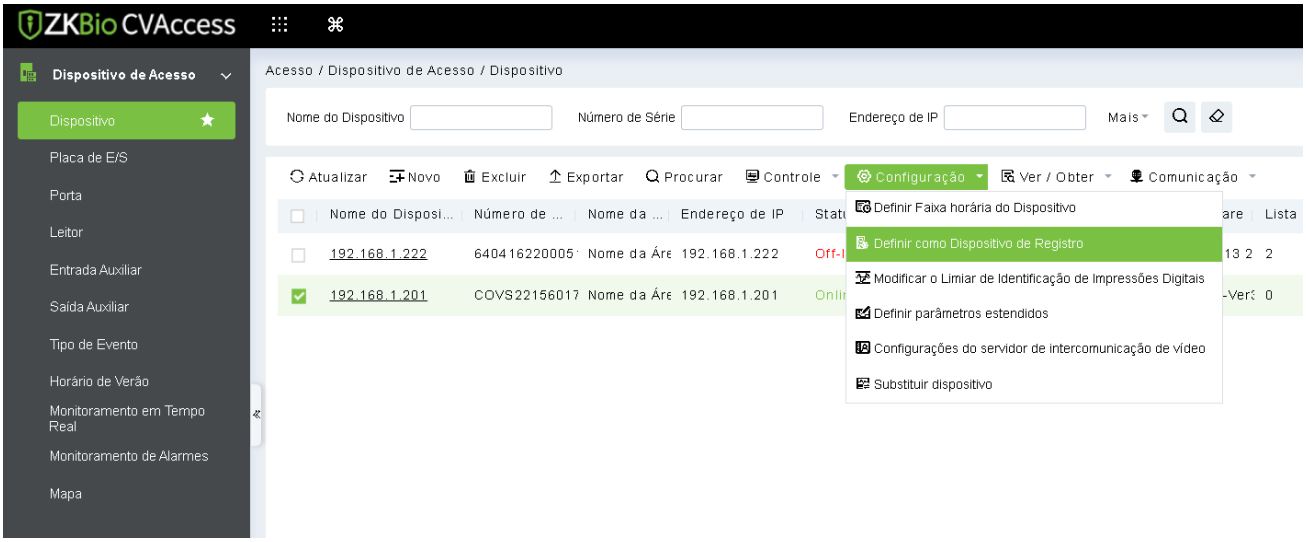
4.1.3.10 Configurar Fuso Horário do Dispositivo

Se o dispositivo suportar as configurações de fuso horário e não estiver no mesmo fuso horário do servidor, você precisa configurar o fuso horário do dispositivo. Após configurar o fuso horário, o dispositivo irá automaticamente sincronizar o horário de acordo com o fuso horário e horário do servidor.



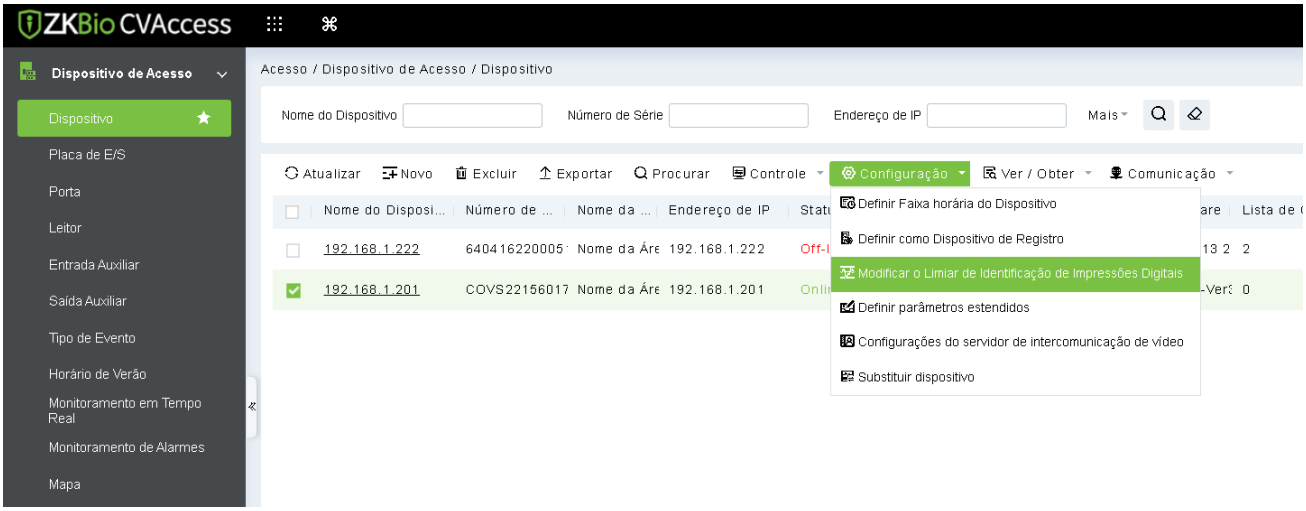
4.1.3.11 Definir como Dispositivo de Registro

Defina o dispositivo de registro apenas quando os dados do dispositivo autônomo, como pessoal, puderem ser carregados automaticamente.



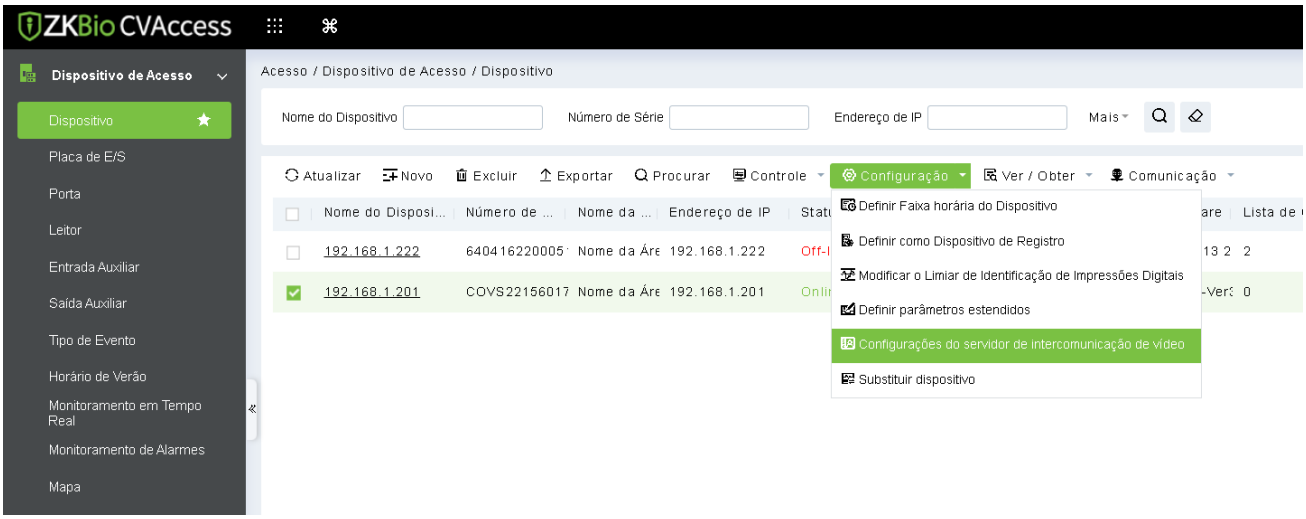
4.1.3.12 Modificar o Limiar de Identificação de Impressão Digital

Nota: Certifique-se de que o controlador de acesso suporta a função de impressão digital.



4.1.3.13 Configurar Servidor de Intercomunicação por Vídeo

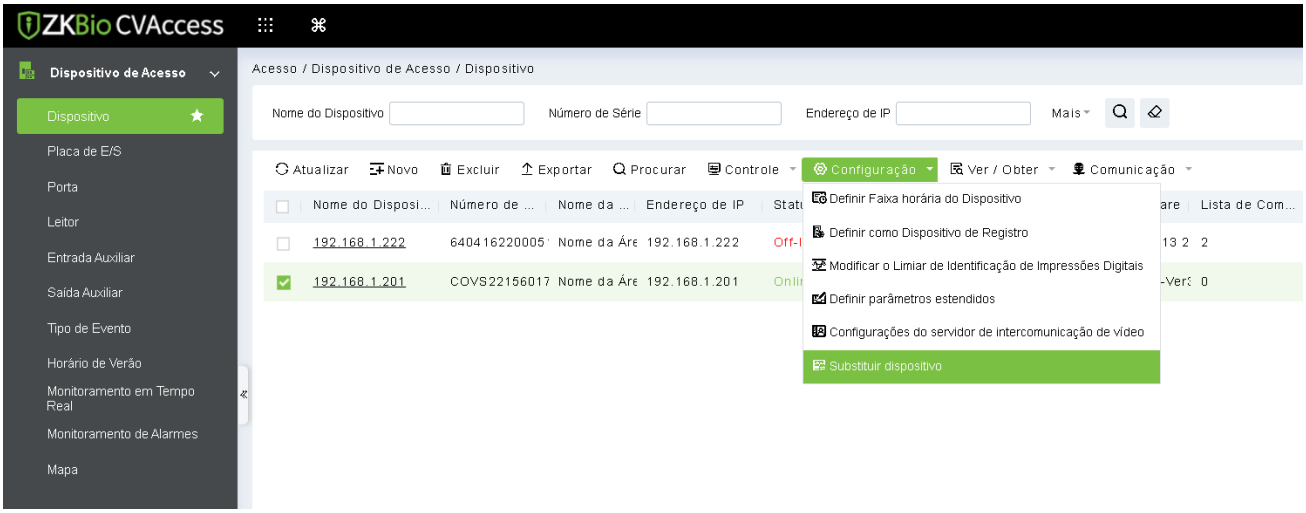
Configure o endereço do servidor de intercomunicação por vídeo para o dispositivo de luz visível.



4.1.3.14 Substituir Dispositivo

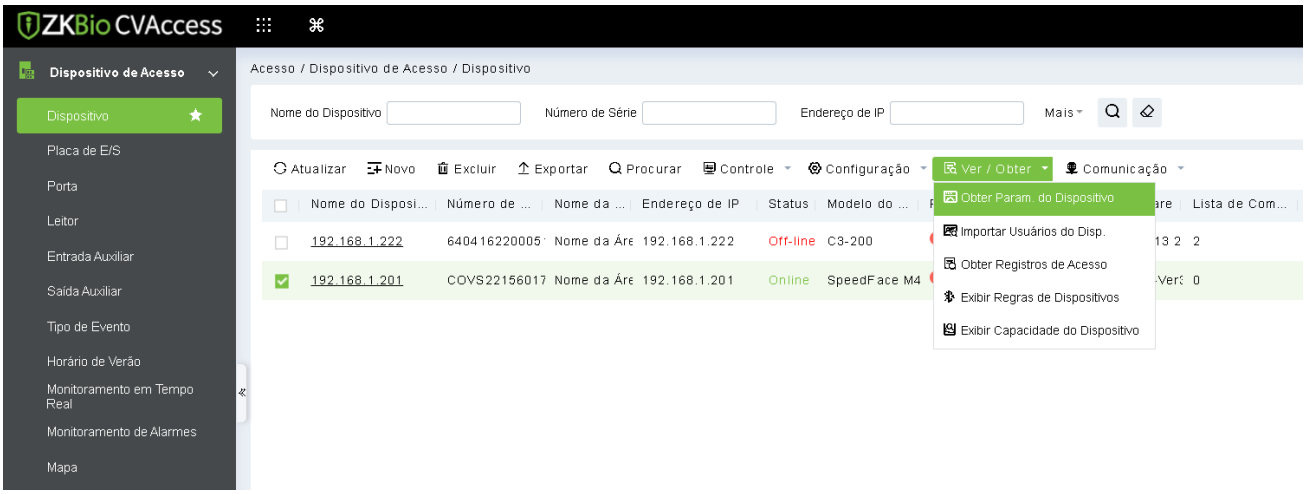
Função rápida de substituição de dispositivo. Quando o dispositivo estiver danificado, basta inserir o número de série do novo dispositivo para copiar rapidamente os dados do dispositivo antigo para o novo dispositivo.

Nota: Apenas dispositivos do mesmo tipo podem ser substituídos, como dispositivos de luz visível podem ser substituídos apenas por dispositivos de luz visível, e controladores podem ser substituídos apenas por novos controladores.



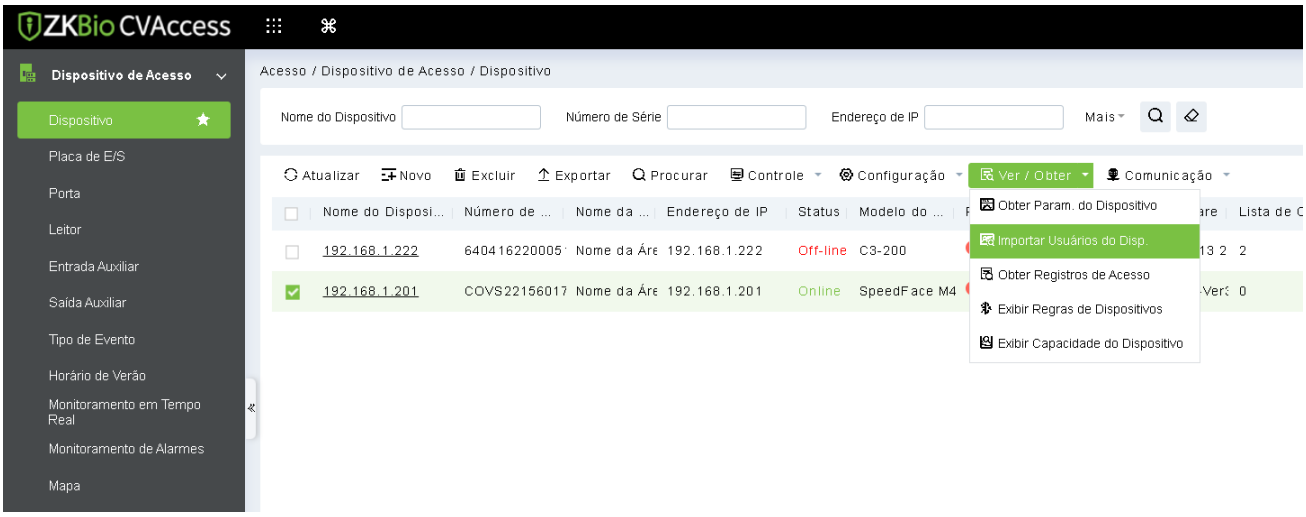
4.1.3.15 Obter Opção do Dispositivo

Obtém os parâmetros comuns do dispositivo. Por exemplo, obtenha a versão do firmware após a atualização do dispositivo.



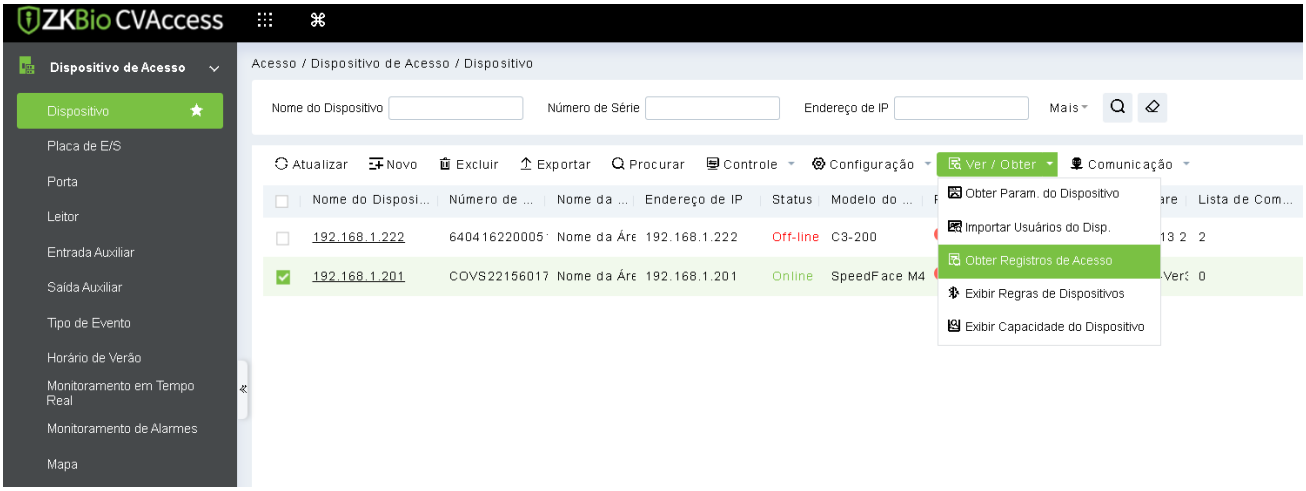
4.1.3.16 Obter Informações do Pessoal

Atualize o número atual de pessoal, impressões digitais, veias dos dedos e modelos faciais no dispositivo. O valor final será exibido na lista de dispositivos.



4.1.3.17 Obter Transações

Obtenha as transações do dispositivo para o sistema. Duas opções são fornecidas para esta operação: Obter Novas Transações e Obter Todas as Transações.



- **Obter Novas Transações:** O sistema apenas obtém novas transações desde a última transação coletada e registrada. Transações repetidas não serão reescritas.
- **Obter Todas as Transações:** O sistema obterá novamente as transações. Entradas repetidas não serão mostradas duas vezes.

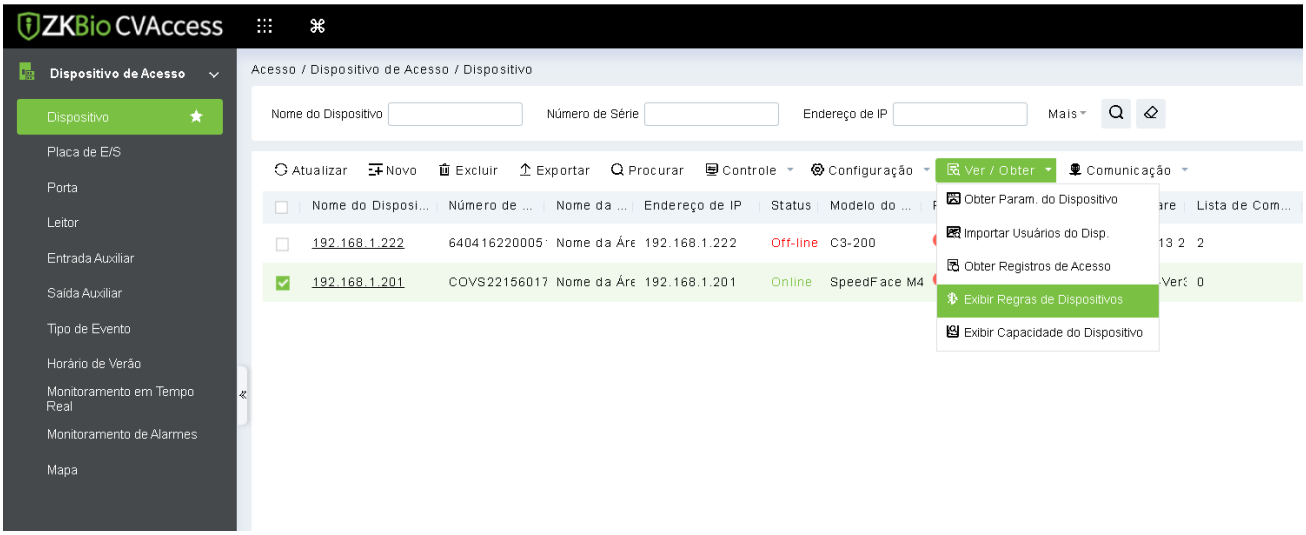
Quando o status da rede estiver saudável e a comunicação entre o sistema e o dispositivo estiver normal, o sistema adquirirá transações do dispositivo em tempo real e as salvará no banco de dados do sistema. No entanto, quando a rede for interrompida ou a comunicação for interrompida por qualquer motivo, e as transações do dispositivo não tiverem sido enviadas para o sistema em tempo real, [Obter Transações]

pode ser usado para adquirir manualmente as transações do dispositivo. Além disso, o sistema, por padrão, adquirirá automaticamente as transações do dispositivo à 00:00 de cada dia.

Nota: O controlador de acesso pode armazenar até 100 mil transações. Quando as transações excederem esse número, o dispositivo excluirá automaticamente as transações mais antigas armazenadas (exclui 10 mil transações).

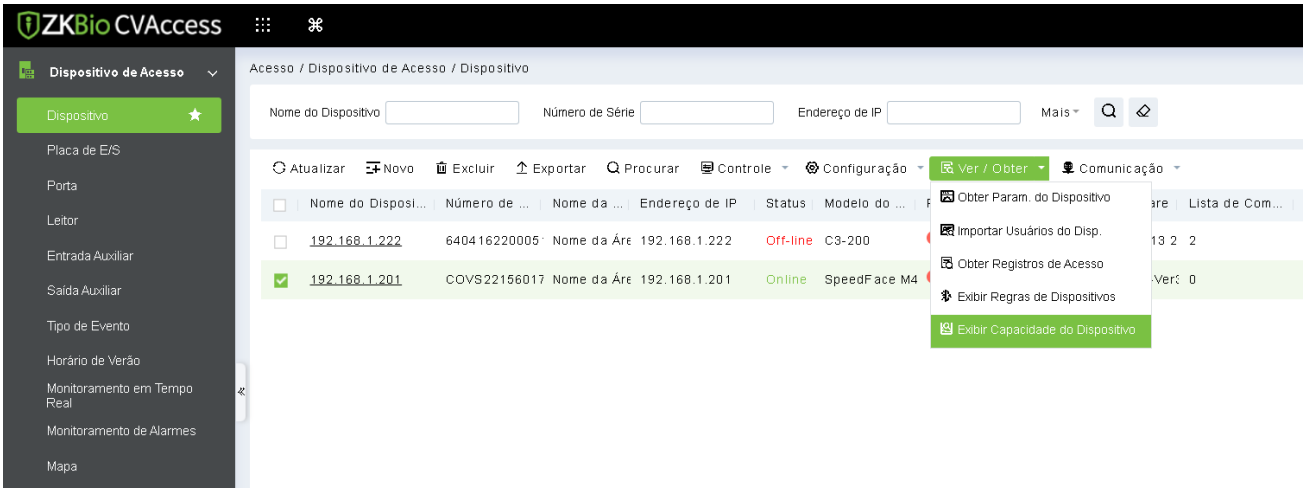
4.1.3.18 Visualizar Regras dos Dispositivos

Mostra as regras de acesso no dispositivo.



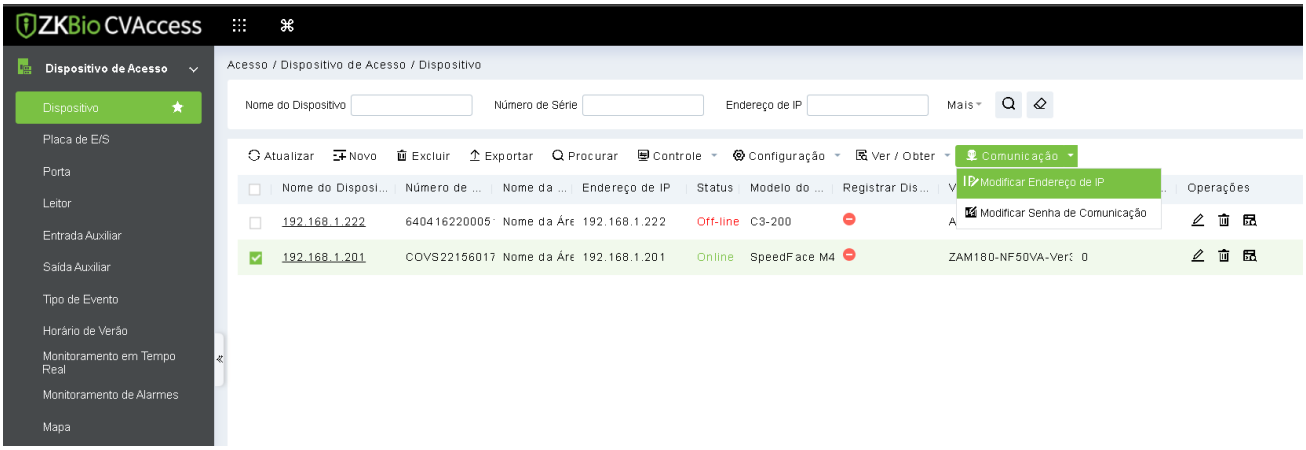
4.1.3.19 Visualizar Capacidade do Dispositivo

Verifica a capacidade dos detalhes biométricos do pessoal no dispositivo.



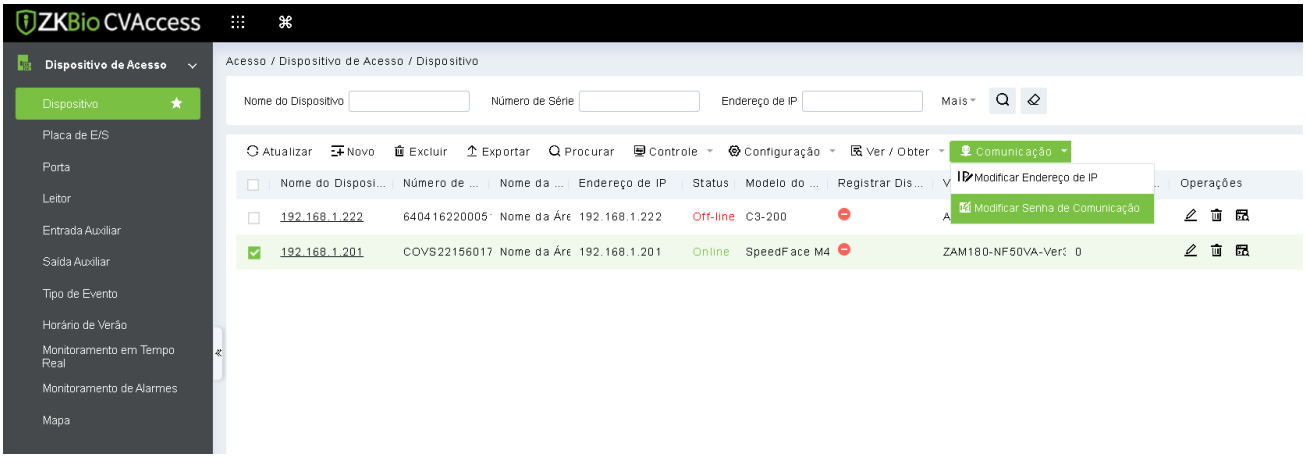
4.1.3.20 Modificar Endereço IP

Selecione um dispositivo e clique em **[Modificar endereço IP]** para abrir a interface de modificação. Ele obterá um gateway de rede e uma máscara de sub-rede em tempo real do dispositivo (falha ao fazer isso, você não poderá modificar o endereço IP). Em seguida, insira um novo endereço IP, gateway e máscara de sub-rede. Clique em **[OK]** para salvar e sair. Esta função é semelhante à **[Função de Modificar Endereço IP]** no Dispositivo.



4.1.3.21 Modificar Senha de Comunicação

O sistema solicitará a senha antiga de comunicação antes de modificá-la. Após a verificação, insira a nova senha duas vezes e clique em **[OK]** para modificar a senha de comunicação.

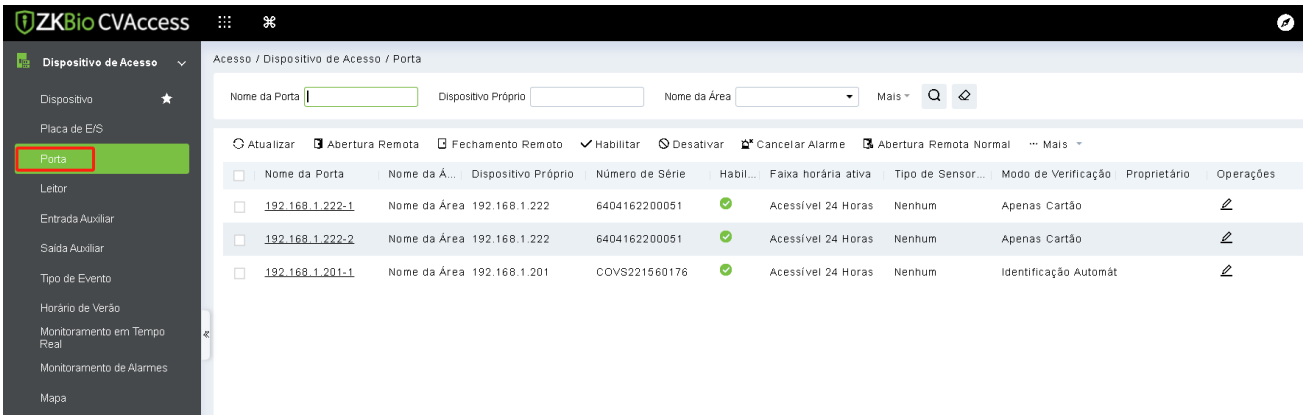


Nota: A senha deve ser uma combinação de números e letras de 6 dígitos.

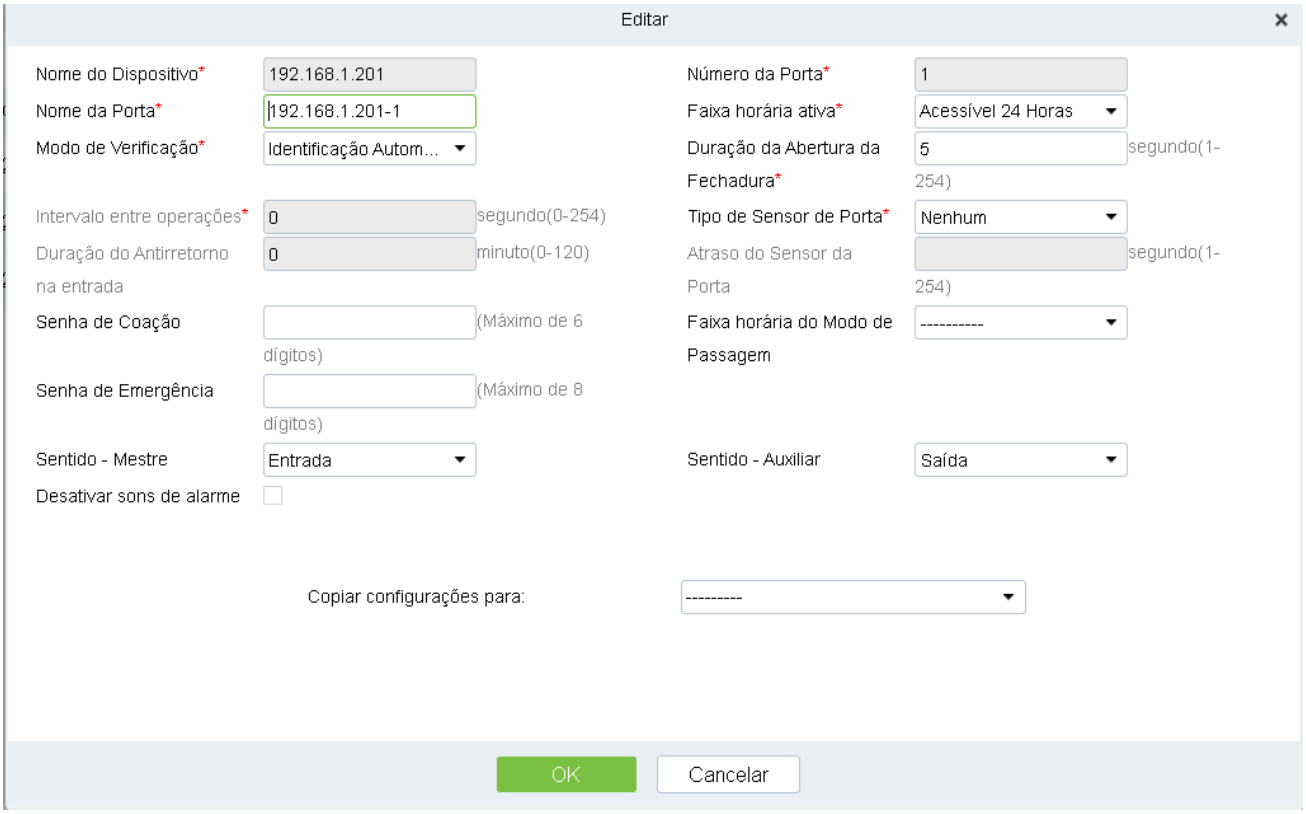
Os usuários podem modificar os limiares de identificação de impressão digital nos dispositivos; varia de 35 a 70 e é 55 por padrão. O sistema lerá os limiares do dispositivo. Os usuários podem visualizar a lista de dispositivos de limiares. Mais de um dispositivo pode ser alterado usando a função de operação em lote.

4.1.4 Portas

Clique **em [Acesso] > [Dispositivo] > [Porta]** para acessar a interface de Gerenciamento de Portas (clique em "Nome da Área" à esquerda, o sistema filtrará e exibirá automaticamente todos os dispositivos de acesso nesta área).



Selecione a porta a ser modificada e clique no nome da porta ou no botão abaixo da guia de operações para abrir a interface de Edição:



Os campos são os seguintes:

- **Nome do Dispositivo:** Não pode ser editado.
- **Número da Porta:** O sistema nomeará automaticamente de acordo com a quantidade de portas do dispositivo. Este número será consistente com o número da porta no dispositivo.

Nota: Por padrão, o número sufixo no Nome da Porta é consistente com o Número da Porta, mas 1/2/3/4 em Anti-Retorno e intertravamento referem-se ao Número da Porta, e não necessariamente ao número após o Nome da Porta, e eles não estão necessariamente relacionados.

- **Nome da Porta:** O padrão é "nome do dispositivo - número da porta". O nome pode ser modificado conforme necessário. São permitidos números, letras ou uma combinação de ambos com até 30 caracteres.
- **Fuso Horário Ativo:** Deve-se selecionar o Fuso Horário Ativo, para que a porta possa ser aberta e fechada normalmente. Um Fuso Horário de Passagem deve ser definido dentro do Fuso Horário Ativo.

Nota: Para uma porta, no estado Normal Aberto, uma pessoa que tenha permissão para ser verificada 5 vezes consecutivas (intervalo de verificação deve estar dentro de 5 segundos) pode liberar o status de Normal Aberto atual e fechar a porta. A próxima verificação será uma verificação normal. Esta função só é eficaz durante o Fuso Horário Ativo das portas especificadas. E no mesmo dia, outros intervalos de Normal Aberto definidos para a porta e configurações de Primeira Pessoa Normalmente Aberta não terão mais efeito.

- **Modo de Verificação:** Os modos de identificação incluem Identificação Automática, Apenas Impressão Digital, Apenas PIN, Apenas Senha, PIN e Impressão Digital, Impressão Digital e Senha, PIN e Senha e Impressão Digital, Face, Rosto e Dedo, Rosto e Dedo e Senha. O valor padrão é Cartão ou Impressão Digital. Quando ambos os modos de Cartão e Senha estão selecionados, certifique-se de que a porta esteja equipada com um leitor que tenha um teclado.
- **Duração de Abertura da Fechadura:** É o período de tempo em que a porta permanece destrancada após uma verificação bem-sucedida. A unidade é segundo (intervalo: 0 a 254 segundos), e o valor padrão é 5 segundos.
- **Intervalo de Operação:** É o intervalo de tempo entre duas verificações. A unidade é Segundos (intervalo: 0 a 254 segundos), e o valor padrão é 0 segundos.
- **Duração de Anti-Retorno de Entrada:** Apenas uma entrada é permitida com um leitor neste período. A unidade é minuto (intervalo: 0 a 120 minutos), e o valor padrão é 0 minutos.
- **Tipo de Sensor de Porta:** Nenhum (não detectará o sensor de porta), Normalmente Aberto, Normalmente Fechado. Se você tiver selecionado como Normalmente Aberto ou Normalmente Fechado, precisará definir o Atraso do Sensor de Porta e decidir se é necessário ou não Fechar e Reverter o bloqueio. Quando o tipo de sensor de porta é definido como Normalmente Aberto ou Normalmente Fechado, o atraso padrão do sensor de porta é de 15 segundos, e então o estado de fechamento e reversão é ativado.
- **Atraso do Sensor de Porta:** É a duração de atraso para a detecção do sensor de porta após a porta ser aberta. Quando a porta não estiver no período de Normalmente Aberta e a porta estiver aberta, o dispositivo iniciará a contagem. Ele acionará um alarme quando a duração do atraso expirar e interromperá o alarme quando você fechar a porta. O atraso padrão do sensor de porta é de 15s (intervalo: 1 a 254 segundos). O Atraso do Sensor de Porta deve ser maior que a Duração de Abertura da Fechadura.
- **Senha de Pressão, Senha de Emergência:** Pressão significa ameaças, violência, restrições ou outra ação usada para forçar alguém a fazer algo contra sua vontade. Nestas situações, insira a Senha de Pressão (com um cartão autorizado) para abrir a porta. Quando a porta é aberta com a Senha de Pressão, o alarme é disparado. Em caso de emergência, o usuário pode usar a Senha de Emergência (chamada de Super Senha) para abrir a porta. A Senha de Emergência permite a abertura normal e é eficaz em qualquer fuso horário e qualquer tipo de modo de verificação, geralmente usada para o administrador.
  1) **Abertura de Senha de Pressão (usada com um cartão autorizado):** A senha deve ser um número não superior a 6 dígitos. Quando o modo de verificação Somente Cartão é usado, você precisa pressionar [ESC] primeiro, e depois pressionar a senha mais o botão [OK], e finalmente inserir o cartão válido. A porta se abre e dispara o alarme. Quando o modo de verificação Cartão + Senha é usado, por favor, passe o cartão válido primeiro, em seguida, pressione a senha mais o botão [OK] (mesmo que a abertura normal no modo de verificação Cartão + Senha), a porta se abre e dispara o alarme.
  2) **Abertura de Senha de Emergência:** A senha deve ter 8 dígitos. A porta pode ser aberta apenas inserindo a senha. Por favor, pressione [ESC] cada vez antes de inserir a senha, e depois pressione [OK] para executar.

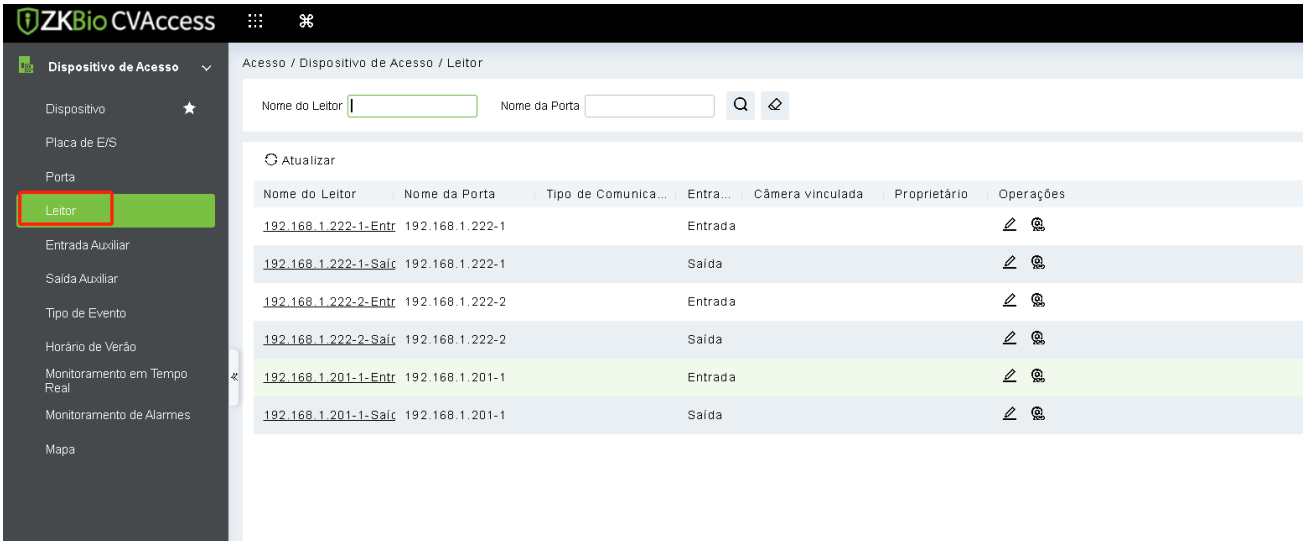
Ao usar a Senha de Pressão ou Senha de Emergência, o intervalo para inserir cada número não deve exceder 10 segundos, e ambas as senhas não devem ser iguais.

- **Desativar Alarme:** Selecione a caixa de seleção Desativar Alarme para desativar o som do alarme na página de monitoramento em tempo real.
  1) As Configurações acima são Copiadas para: Possui duas opções abaixo.
  2) Todas as portas no dispositivo atual: Clique para aplicar as configurações acima a todas as portas do dispositivo de acesso atual.
  3) Todas as portas em Todos os Dispositivos de Controle: Clique para aplicar as configurações acima a todas as portas de todos os dispositivos de acesso dentro do nível de usuário atual.

Após configurar o(s) parâmetro(s), clique em [OK] para salvar e sair.

4.1.5 Leitor

Clique em **[Dispositivo] > [Leitor]** no Menu e, em seguida, clique no nome do leitor ou no botão 

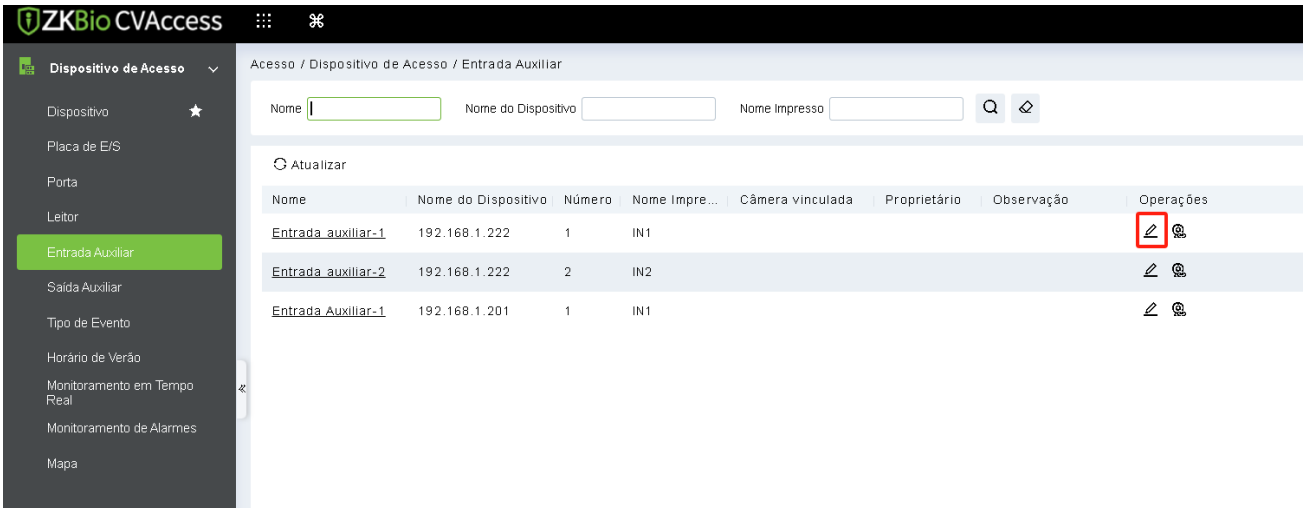


- **Nome:** Defina o nome do leitor exibido na página da lista.

4.1.6 Entrada Auxiliar

É principalmente usado para conectar dispositivos como sensores infravermelhos, sensores de fumaça, detectores de fumaça, etc.

1) Clique em [Dispositivo de Acesso] > [Entrada Auxiliar] no Menu de Ação, para acessar a interface mostrada abaixo:
2) Clique no Nome ou botão para modificar os parâmetros conforme mostrado abaixo:



Os campos são os seguintes:

- **Nome:** Você pode personalizar o nome de acordo com sua preferência.
- **Nome Impresso:** Será o nome impresso no hardware, como IN5.
- **Fuso Horário Ativo:** A entrada auxiliar estará disponível apenas no segmento de tempo especificado.

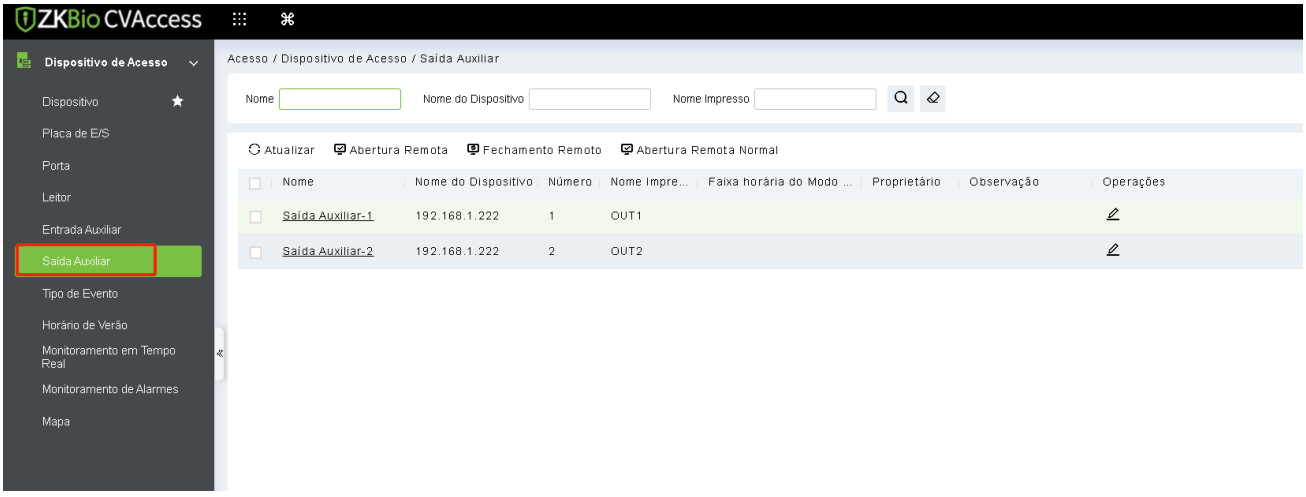
Nota: Apenas o Nome pode ser modificado.

3) Clique em **[OK]** para salvar o nome e sair.

4.1.7 Saída Auxiliar

É principalmente usado para saída de alarme e com função de ligação ativa.

1) Clique em **[Dispositivo de Acesso] > [Saída Auxiliar]** no Menu de Ação para acessar a seguinte interface:



2) Clique no botão para modificar os parâmetros:

Os campos são os seguintes:

- **Nome:** Você pode personalizar o nome de acordo com sua preferência.
- **Nome Impresso:** O nome impresso no hardware, por exemplo, OUT2.
- **Fuso Horário do Modo de Passagem:** A saída auxiliar estará normalmente aberta ou fechada no fuso horário selecionado.

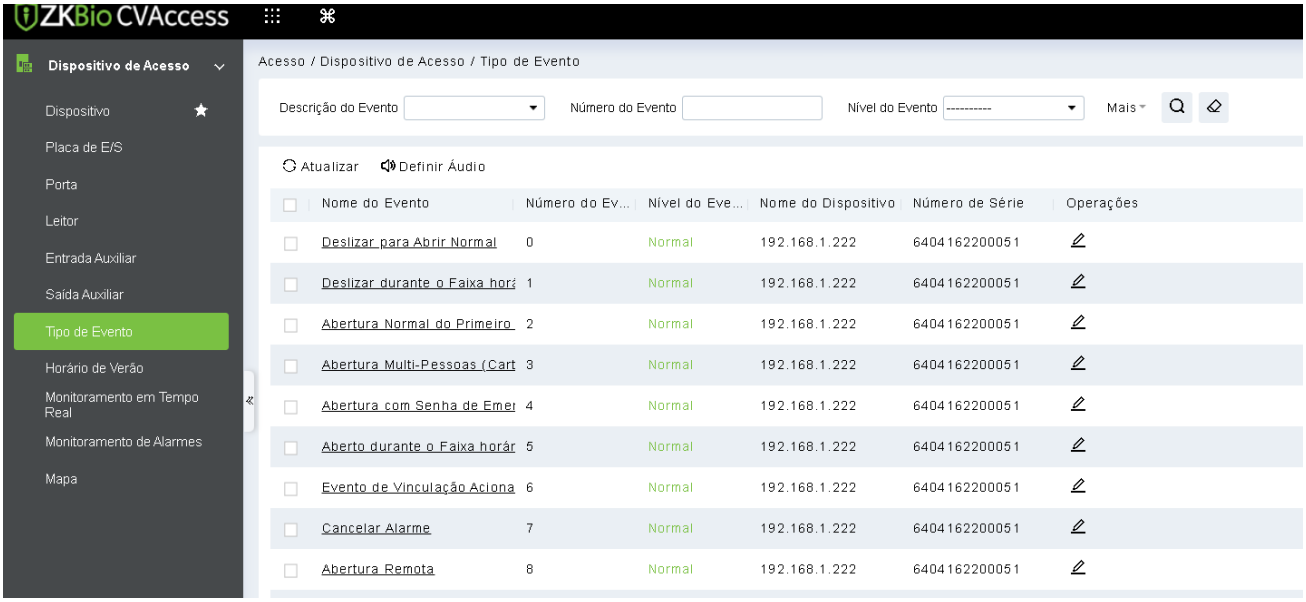
Nota: Apenas Nome, Fuso Horário do Modo de Passagem e Observações podem ser modificados.

3) Clique em **[OK]** para salvar o nome e a observação e sair.

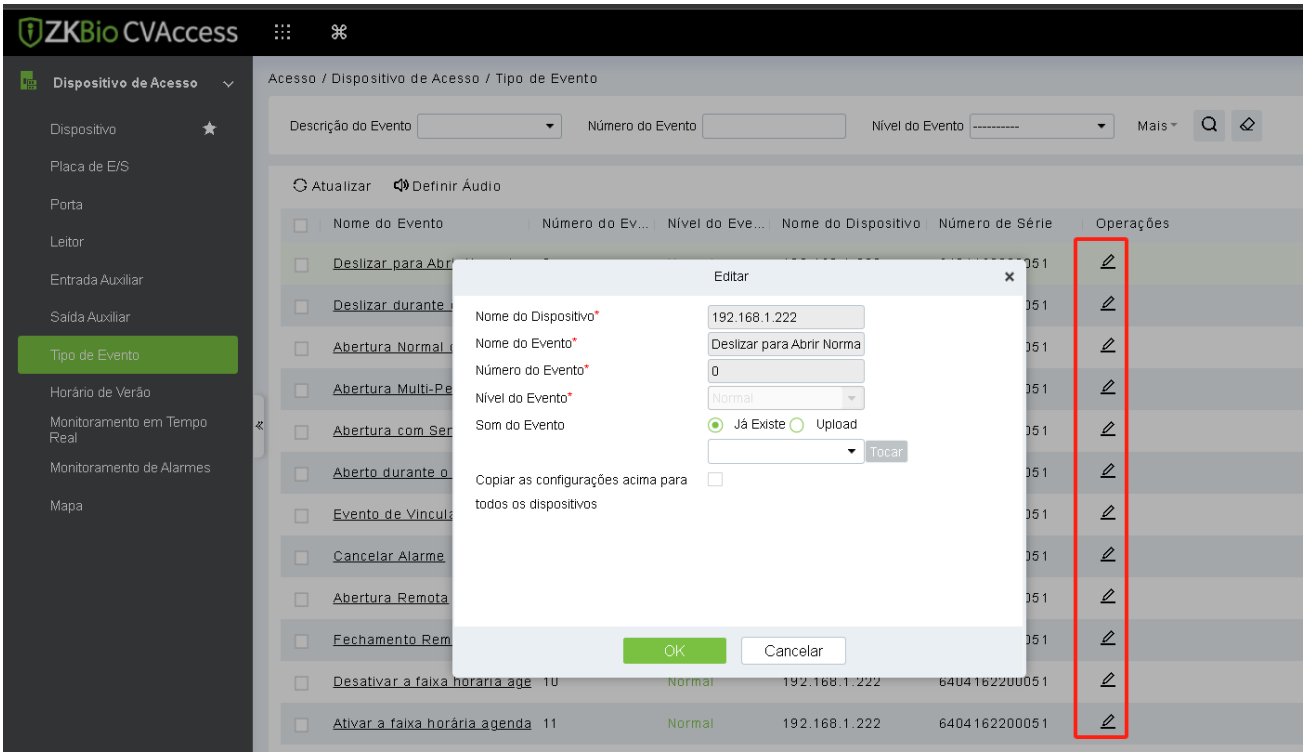
4.1.8 Tipo de Evento

Exibirá os tipos de eventos dos dispositivos de acesso.

1) Clique em **[Dispositivo]** > **[Evento]** para acessar a seguinte página:



2) Clique em **[Editar]** ou clique no nome do tipo de evento para editar:

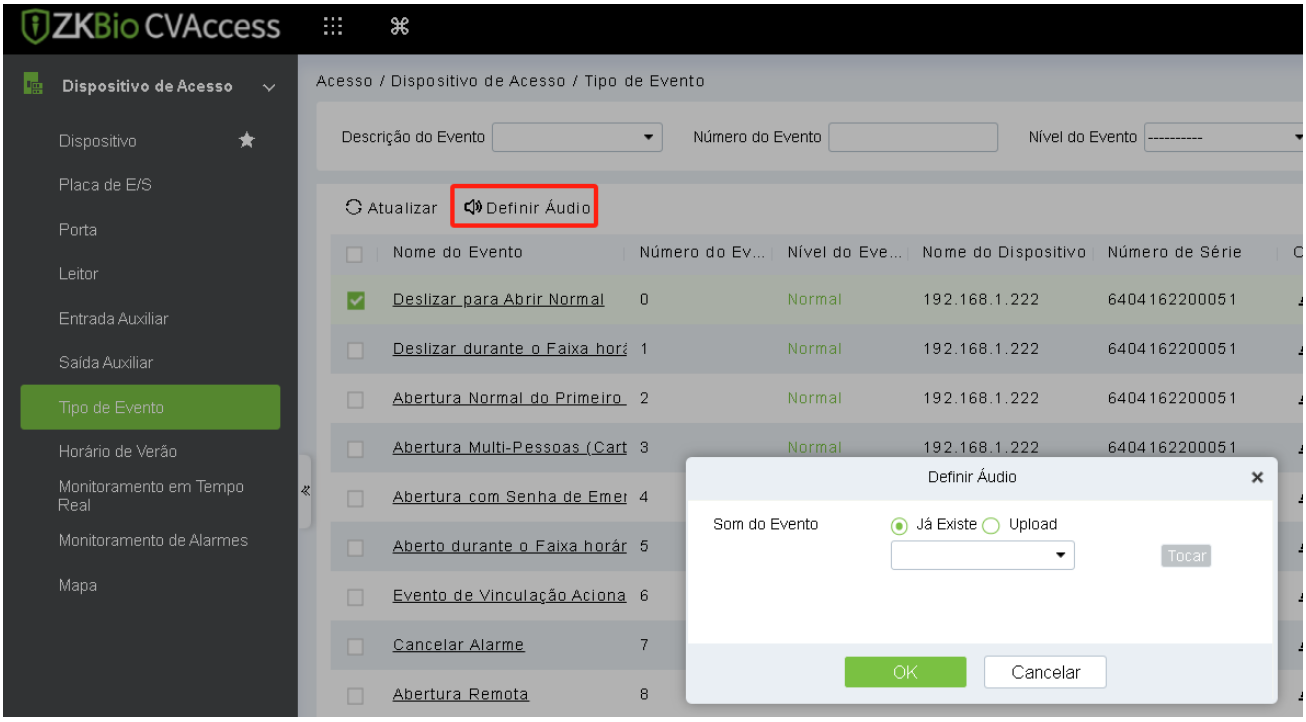


Os campos são os seguintes:

- **Nível do Evento:** Normal, Exceção e Alarme estão disponíveis.
- **Nome do Evento:** Não pode ser modificado.
- **Som do Evento:** Você pode definir um som personalizado a ser reproduzido quando o evento ocorrer na monitoração em tempo real.
- **Copiar as configurações acima para todos os dispositivos:** Este evento será aplicado a todos os dispositivos atuais dentro do escopo do mesmo número de evento do usuário.

Configurar Áudio

Igual ao som do evento. Clique em [Configurar Áudio]:

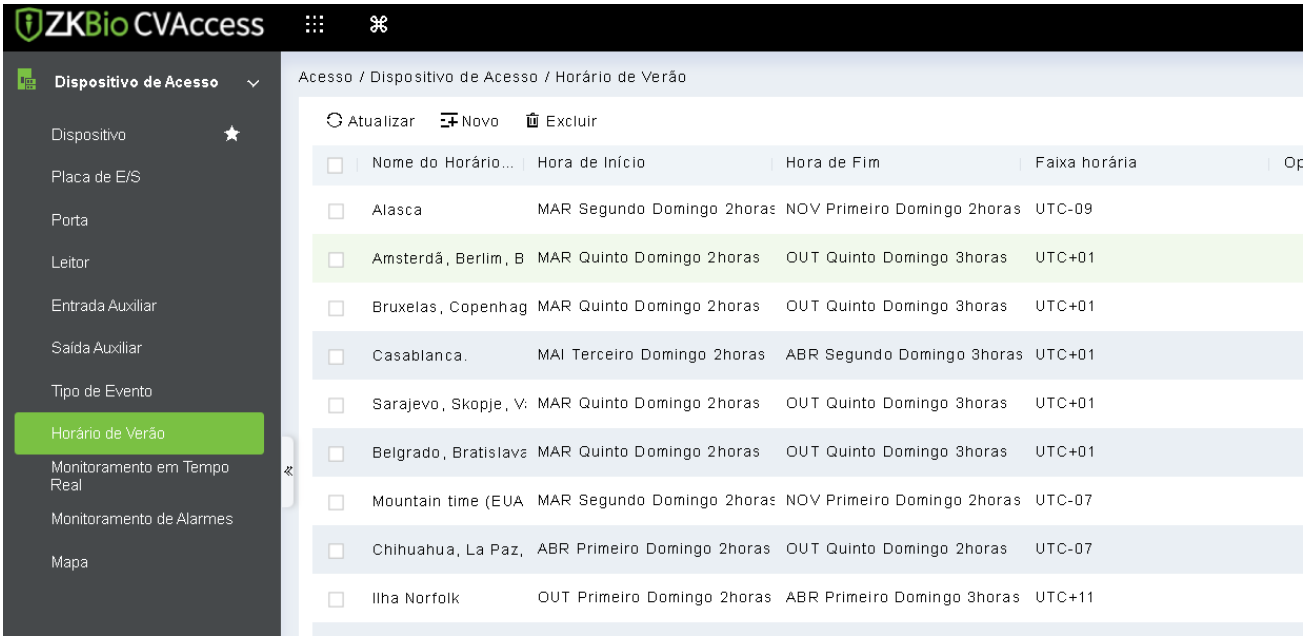


Você pode fazer upload de áudio do seu PC local. O arquivo deve estar no formato wav ou mp3, e não deve exceder 10MB. Para mais detalhes sobre Tipo de Evento, consulte Tipo de Evento de Acesso.

4.1.9 Horário de Verão

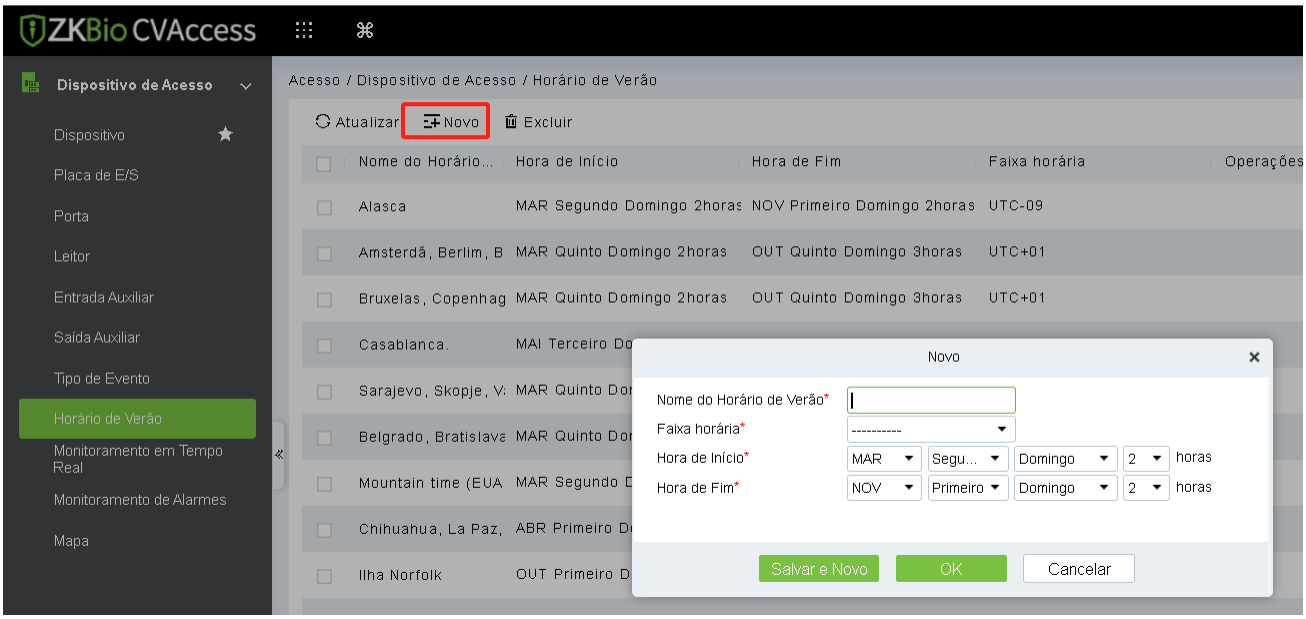
O Horário de Verão é uma função para ajustar o horário local oficialmente prescrito para economizar energia. O horário unificado adotado durante a implementação é conhecido como "DST". Tipicamente, regiões que utilizam o horário de verão ajustam os relógios adiante em uma hora para o horário padrão perto do início da primavera no verão para que as pessoas durmam mais cedo. Isso também pode ajudar a economizar energia. No outono, os relógios são ajustados para trás para levantar mais cedo. As regulamentações são diferentes em diferentes países. Atualmente, cerca de 70 países adotam o DST.

Para atender ao requisito de DST, uma função especial pode ser personalizada. Você pode ajustar o relógio uma hora adiante em (hora) (dia) (mês) e uma hora para trás em (hora) (dia) (mês) se necessário.



4.1.9.1 Adicionar DST

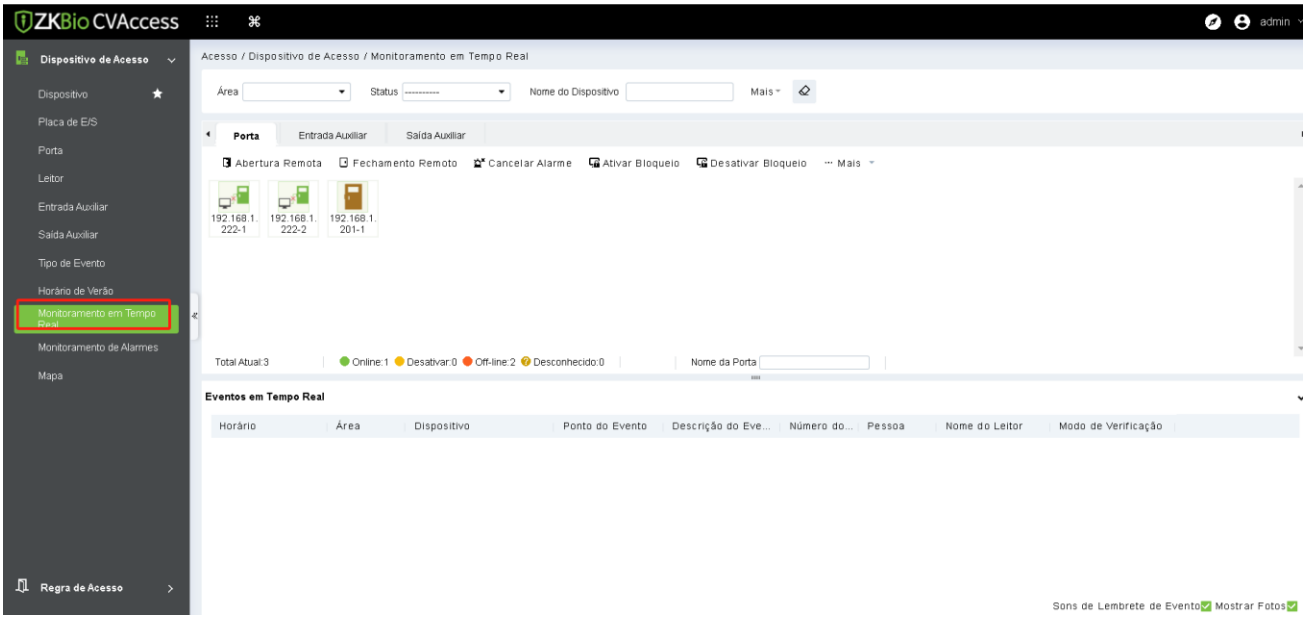
1) Clique em **[Acesso] > [Dispositivo] > [Horário de Verão] > [Novo]:**



Os campos de linha são em formato "Mês - Semana - Dia - Hora". Por exemplo, se o horário de início for definido como "Março - Segundo - Domingo - 2 horas", isso significa que o DST começará a partir do segundo domingo de março às 2h da manhã. O sistema avançará uma hora no horário de início. O sistema voltará para o horário original no final do tempo.

4.1.10 Monitoramento em Tempo Real

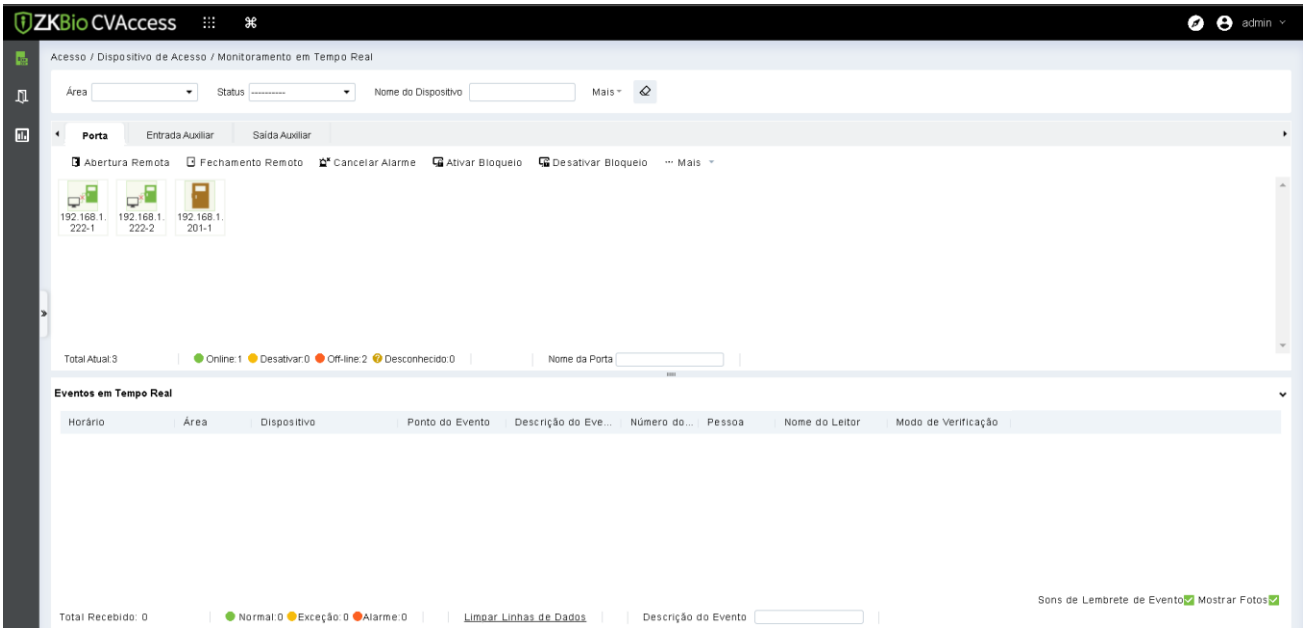
Clique em [Dispositivo de Acesso] > [Monitoramento em Tempo Real].



Ele monitorará o status e eventos em tempo real das portas sob os painéis de controle de acesso no sistema em tempo real, incluindo eventos normais e anormais (incluindo eventos de alarme).

A interface de Monitoramento em Tempo Real é mostrada da seguinte forma:

Sem status de relé, indica que o firmware atual não suporta ação no dispositivo. Diferentes ícones representam o status da seguinte forma:



4.1.10.1 Porta

- **Abertura/Fechamento Remoto:** Pode controlar uma porta ou todas as portas.

Para controlar uma única porta, clique com o botão direito sobre ela e clique em [Abertura/Fechamento Remoto] na caixa de diálogo que aparece. Para controlar todas as portas, clique diretamente em [Abertura/Fechamento Remoto] atrás de Todas Atuais.

Na abertura remota, o usuário pode definir a duração da abertura da porta (o padrão é 15 segundos). Você pode selecionar [Habilitar Fuso Horário de Modo de Passagem Intradiário] para habilitar os fusos horários de modo de passagem intradiário ou definir a porta como Normalmente Aberta, então a porta não estará limitada a nenhum fuso horário (pode ser aberta a qualquer momento).

Para fechar uma porta, selecione [Desabilitar Fuso Horário de Modo de Passagem Intradiário] primeiro, para evitar habilitar outros fusos horários normais para abrir a porta, e depois selecione [Fechamento Remoto].

Nota: Se [Abertura/Fechamento Remoto] falhar, verifique se os dispositivos estão desconectados ou não. Se desconectado, verifique a rede.

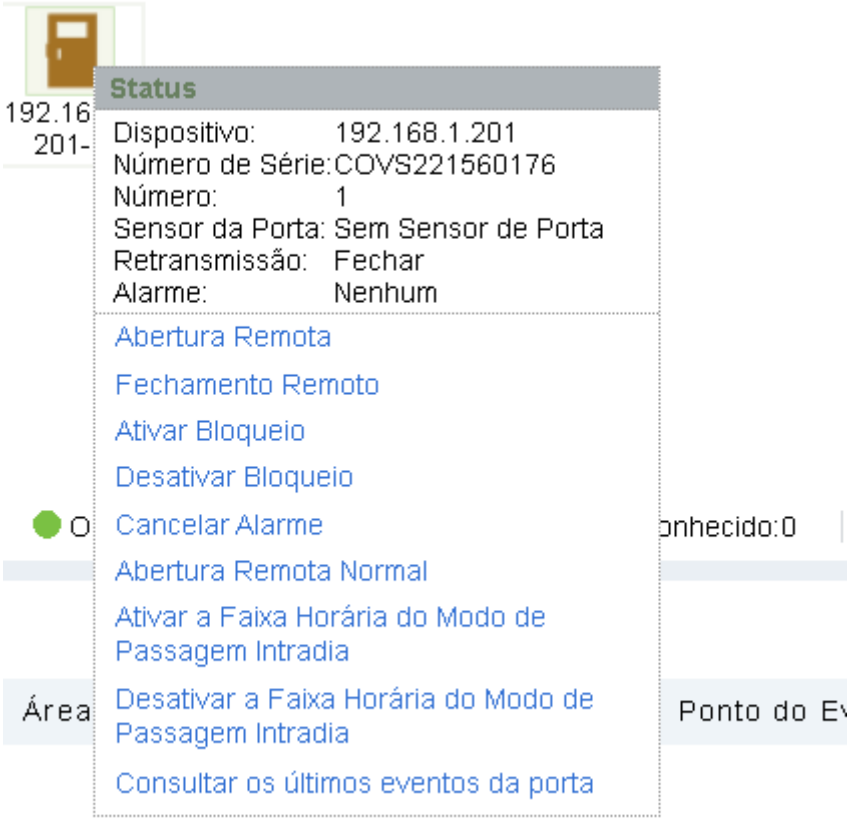
- **Cancelar o alarme:** Uma vez que uma porta alarmante aparece sobre a interface, o som do alarme será reproduzido. O cancelamento do alarme pode ser feito para uma porta única e todas as portas. Para controlar uma única porta, mova o cursor sobre o ícone da porta, um menu aparecerá, então clique em [Abertura/Fechamento Remoto] no menu. Para controlar todas as portas, clique diretamente em [Abertura/Fechamento Remoto] atrás de Todas Atuais.

Nota: Se [Cancelar o alarme] falhar, verifique se há dispositivos desconectados. Se encontrou desconexão, verifique a rede.

- **Normalmente Aberto Remoto:** Irá configurar o dispositivo como normalmente aberto remotamente.

Gerenciamento Rápido de Portas

Se você mover o cursor sobre o ícone de uma porta; você pode realizar as operações acima explicadas de forma rápida. Além disso, você pode consultar os eventos mais recentes da porta.



- **Consultar os eventos mais recentes da porta:** Clique para visualizar rapidamente os eventos atuais na porta.
- **Emitir cartão para pessoa:** Se você passar um cartão não registrado, um registro com um número de cartão aparecerá na interface de monitoramento em tempo real. Clique com o botão direito sobre esse número de cartão, e um menu aparecerá. Clique em "Emitir cartão para pessoa", para atribuir esse cartão a uma pessoa.

Seleção Múltipla

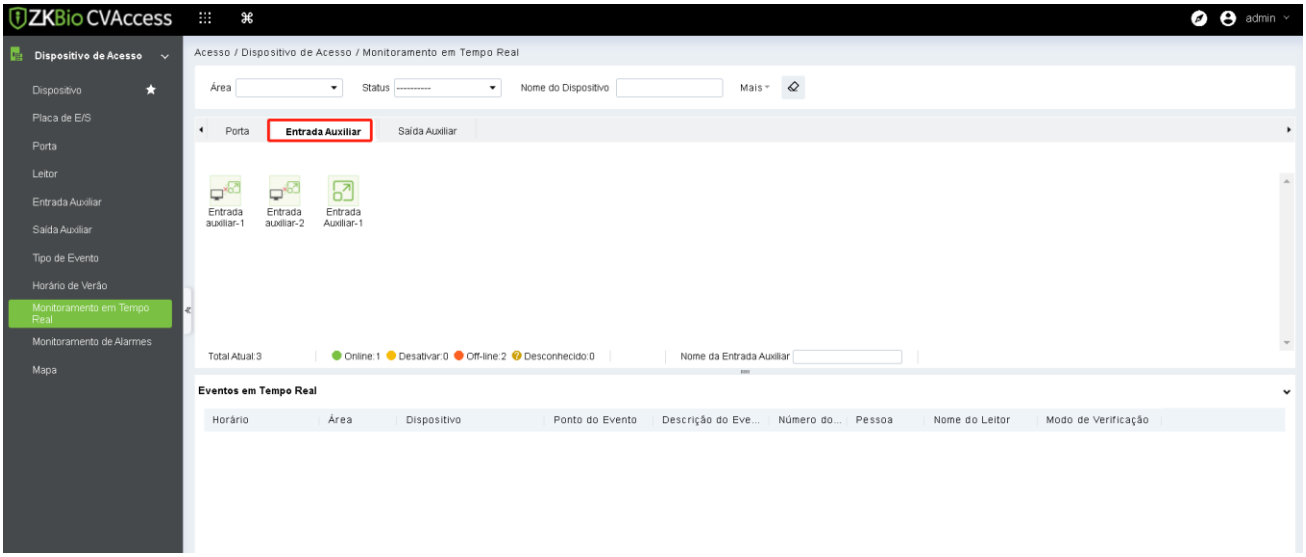
Você pode selecionar várias portas ao mesmo tempo para realizar operações como abertura remota, fechamento remoto, cancelamento de alarme, etc. Dê um clique duplo no ícone da porta para editar as propriedades da porta.

Monitoramento de Eventos

O sistema adquirirá automaticamente registros dos dispositivos sendo monitorados (por padrão, exibe 200 registros), incluindo eventos normais e anormais de controle de acesso (incluindo eventos de alarme). Eventos normais aparecerão em verde; eventos de alarme aparecerão em vermelho; outros eventos anormais aparecerão em laranja.

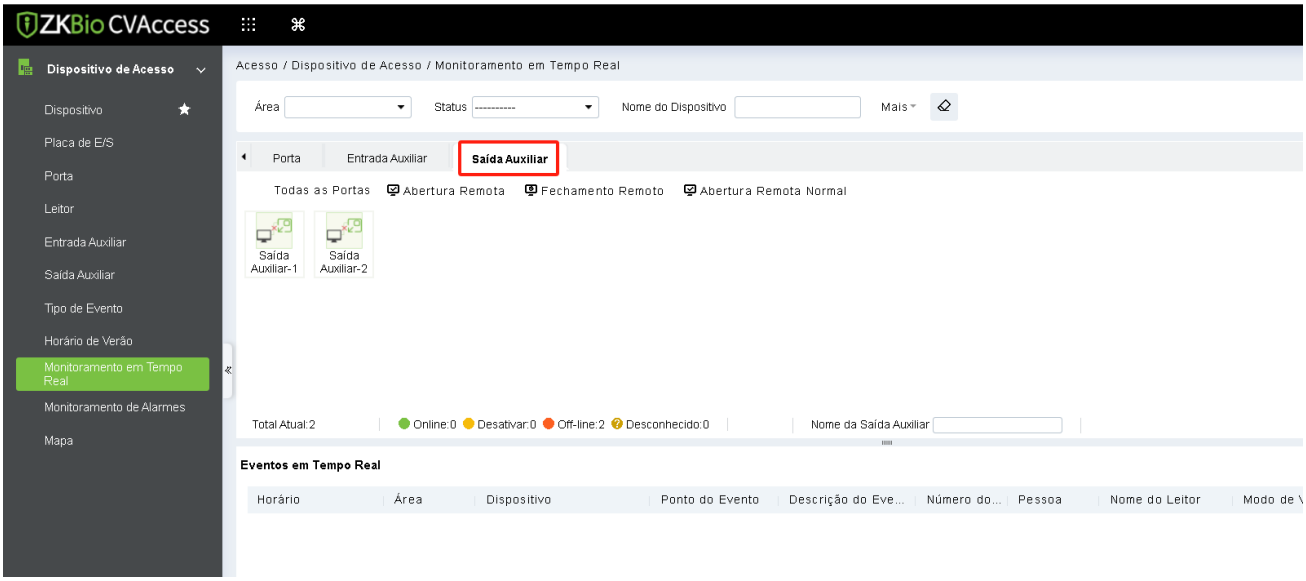
4.1.10.2 Entrada Auxiliar

Monitora eventos atuais de entrada auxiliar em tempo real.



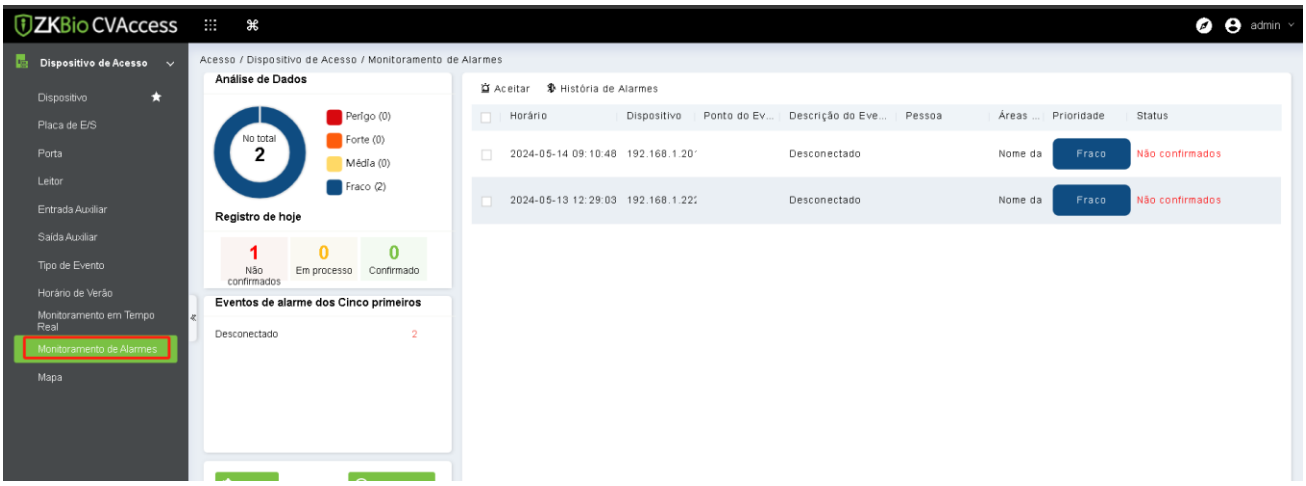
4.1.10.3 Saída Auxiliar

Aqui você pode realizar Abertura Remota, Fechamento Remoto, Normalmente Aberto Remoto.

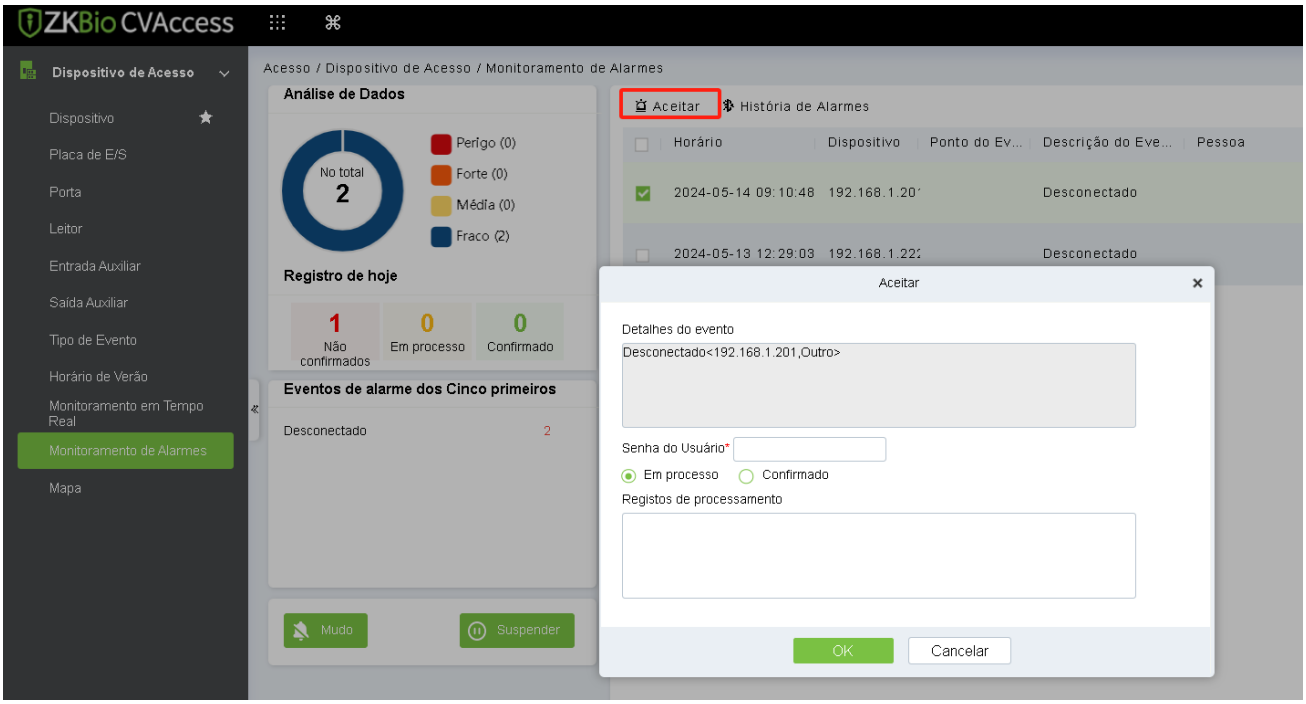


4.1.11 Monitoramento de Alarme

Ele monitora os eventos de alarme das portas. O alarme será ativado em caso de anormalidades como Violação, Retrocesso, etc. Os alarmes ativados pelas portas serão exibidos nesta página. Os detalhes do alarme consistem em Hora, Nome do Dispositivo, Ponto do Evento, Descrição do evento, Pessoa responsável pelo alarme e o nome do leitor correspondente.



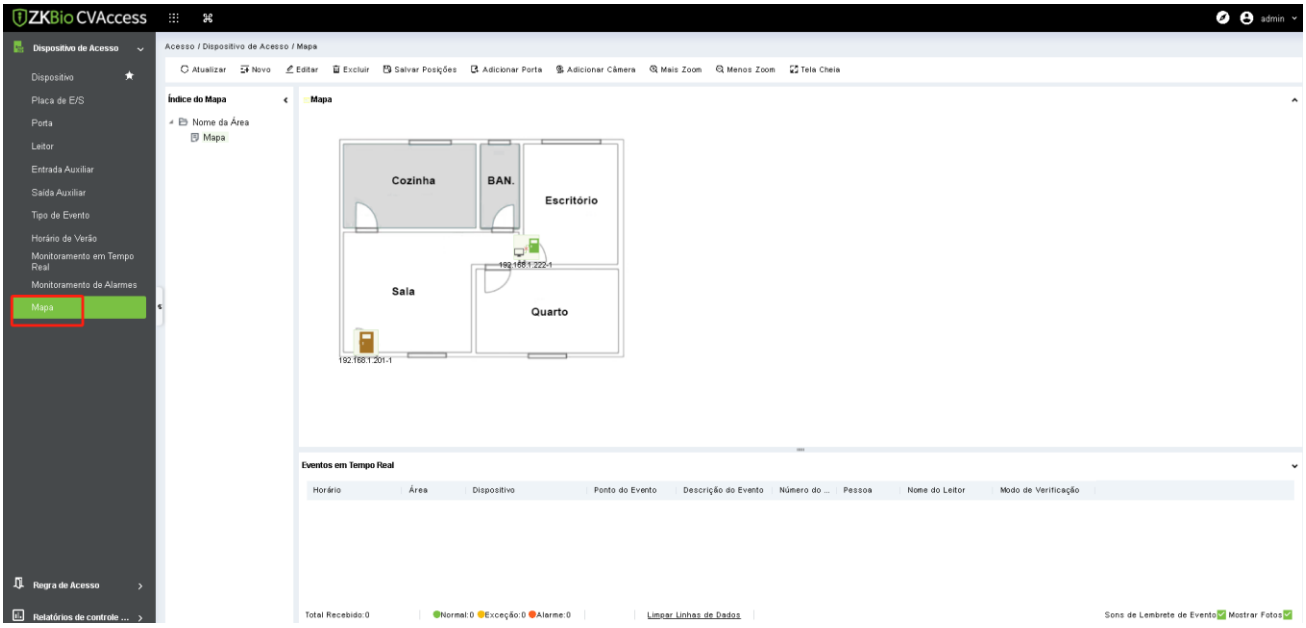
Nota: Se a versão do firmware do dispositivo suportar, a Descrição do Evento será exibida, caso contrário, apenas "Alarme" será exibido na Descrição do Evento sem detalhes. Selecione o Alarme e clique em [Reconhecer] para responder ao Alarme.



Nota: Quando uma porta tem múltiplos estados de alarme, será exibida apenas uma descrição de tipo de alarme na ordem de gravidade decrescente, a ordem é a seguinte: alarme de resistência a violação > alarme de coação (senha + impressão digital) > alarme de coação por senha ou impressão digital > alarme de abertura inesperada > alarme de tempo limite de abertura > alarme de desconexão do dispositivo.

4.1.12 Mapa

Clique em **[Dispositivo de Acesso] > [Mapa] > [Novo]** para adicionar um mapa.



Após adicionar, os usuários podem adicionar uma porta no mapa; realizar zoom-in, zoom-out, etc. Se os usuários relocarem algumas seções ou modificarem o mapa, clique em [Salvar Posições] para salvar. O usuário pode visualizar as novas configurações ao reabrir a interface do Mapa.

- **Adicionar / Excluir Mapa:** Os usuários podem adicionar ou excluir um mapa conforme necessário.
- **Editar Mapa:** Os usuários podem editar o nome do mapa, mudar o mapa ou a área a que pertence.
- **Ajustar mapa (inclui porta):** Os usuários podem adicionar uma porta no mapa ou excluir uma existente (clique com o botão direito no ícone da porta e selecione [Excluir Porta]), ou ajustar o mapa ou a posição da(s) porta(s) ou ícones de câmera (arrastando os ícones de porta ou câmera), ajustar o tamanho do mapa (clique em [Zoom in] ou [Zoom out] ou clique em [Tela Cheia]).
- **Operação de Porta:** Se você mover o cursor sobre um ícone de porta, o sistema filtrará automaticamente e exibirá a operação de acordo com o status da porta. Os usuários podem abrir/fechar portas remotamente, cancelar alarmes, etc.

Controle de Níveis:

1) Os usuários precisam selecionar a área relevante para o mapa ao adicionar níveis. A área será relevante para os níveis de acesso do usuário, os usuários só podem visualizar ou gerenciar o mapa dentro dos níveis. Se a área relevante de um mapa for modificada, todas as portas no mapa serão apagadas. Os usuários precisam adicionar as portas manualmente novamente.
2) Quando um administrador está adicionando um novo usuário, ele pode definir os direitos de operação do usuário nas configurações de função, como Salvar posições, Adicionar Porta, Adicionar Câmera, etc.

Notas:

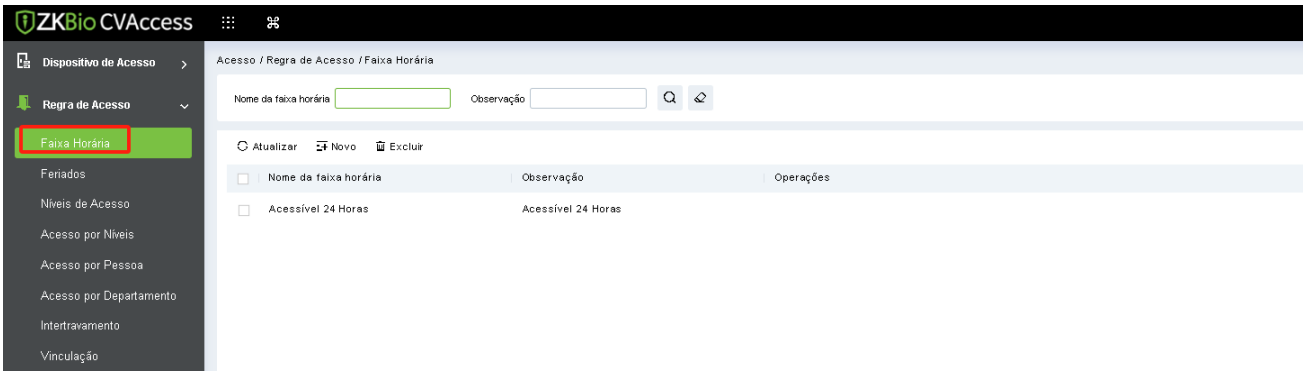
1) Na modificação do mapa, os usuários podem optar por modificar o nome do mapa, mas não o caminho. Os usuários só precisam marcar a caixa para ativar a opção de modificação.
2) O sistema suporta adicionar várias portas ao mesmo tempo. Após adicionar as portas, os usuários precisam definir a posição da porta no mapa e clicar em [Salvar].
3) Ao modificar o ícone da porta, especialmente quando os usuários deram zoom no mapa, a margem superior e esquerda não deve ser menor que 5 pixels, ou o sistema exibirá um erro.
4) É recomendado que os usuários adicionem um tamanho de mapa inferior a 1120 * 380 pixels. Se vários clientes acessarem o mesmo servidor, o efeito de exibição será diferente de acordo com as resoluções da tela e as configurações dos navegadores.

4.2 Gerenciamento de Regras de Acesso

4.2.1 Zonas Horárias

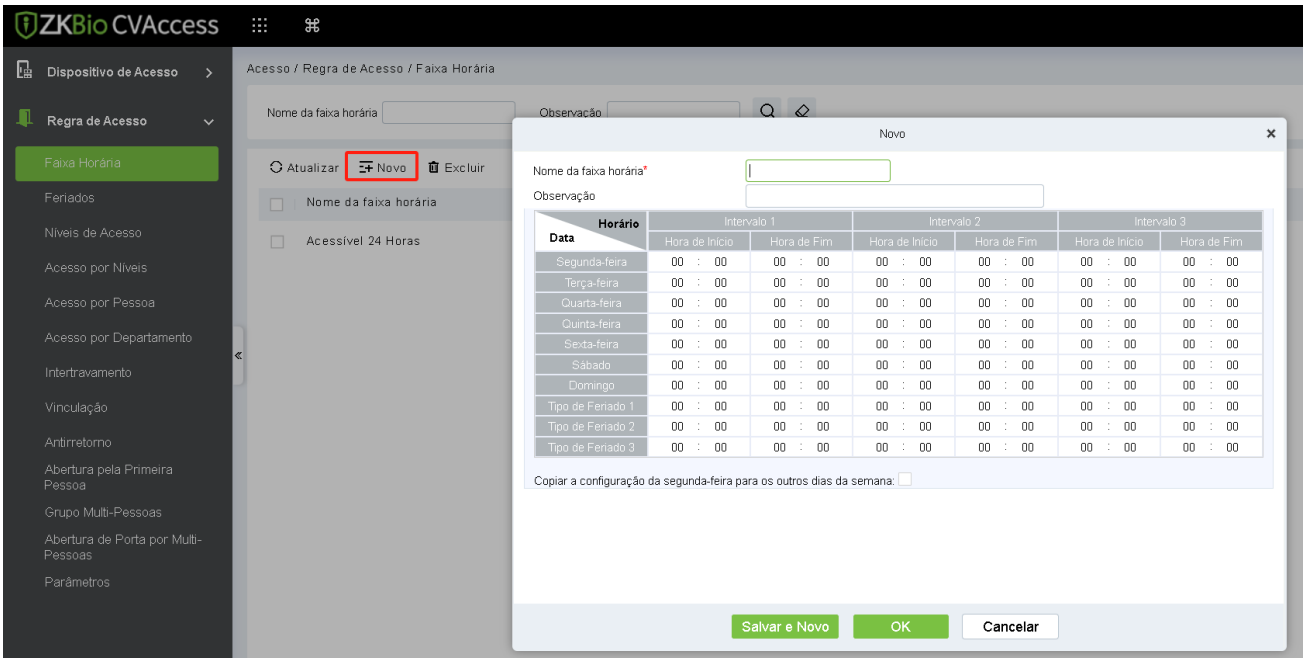
Define o horário de uso de uma porta; o leitor só pode ser usado durante um período de tempo válido de certas portas. A Zona Horária também pode ser usada para definir períodos de tempo de Abertura Normal ou definir níveis de acesso para que usuários específicos só possam acessar portas específicas durante períodos de tempo especificados (incluindo níveis de acesso e Abertura Normal do Primeiro Usuário).

O sistema controla o acesso de acordo com as Zonas Horárias (até 255 zonas horárias). O formato de cada intervalo para uma zona horária: HH:MM-HH:MM. Inicialmente, por padrão, o sistema possui uma zona horária de controle de acesso chamada "Acesso 24 horas". Este período de tempo não pode ser modificado ou excluído. O usuário pode adicionar novas Zonas Horárias conforme necessário.



Adicionar Zona Horária de Controle de Acesso

1) Clique em **[Regra de Acesso]** > **[Zonas Horárias]** > **[Nova]** para acessar a interface de configuração de zona horária.



Os parâmetros são os seguintes:

- **Nome da Zona Horária:** Qualquer caractere, até uma combinação de 30 caracteres.

Nota: Descrição detalhada da zona horária atual, incluindo uma explicação da zona horária atual e aplicações principais. Os usuários podem inserir até 50 caracteres neste campo.

- **Intervalo e Horário de Início/Fim:** Uma Zona Horária de Controle de Acesso inclui 3 intervalos para cada dia da semana e 3 intervalos para cada um dos três Feriados. Defina os horários de início e fim de cada intervalo.
- **Configuração:** Se o intervalo for Abertura Normal, basta inserir 00:00-23:59 como intervalo 1 e 00:00-00:00 como intervalo 2 e 3. Se o intervalo for Fechamento Normal: todas as entradas serão 00:00-00:00. Se os usuários usarem apenas um intervalo, eles só precisam preencher o intervalo 1, e o intervalo 2 e 3 serão o valor padrão. Da mesma forma, quando os usuários usam apenas os dois primeiros intervalos, o terceiro intervalo será o valor padrão. Ao usar dois ou três intervalos, os usuários precisam garantir que os dois ou três intervalos não se sobreponham, e o tempo não deve ultrapassar os dias, ou o sistema exibirá um erro.
- **Tipo de Feriado:** Três tipos de feriados não estão relacionados ao dia da semana. Se uma data for definida como um tipo de feriado, os três intervalos do tipo de feriado serão usados para fins de acesso. O tipo de feriado é opcional. Se o usuário não inserir um, o sistema usará o valor padrão.
- **Copiar em Segunda-feira:** Selecione a caixa de seleção para copiar as configurações de Segunda-feira para outros dias úteis.

2) Após a configuração, clique em [OK] para salvar, e ela será exibida na lista.

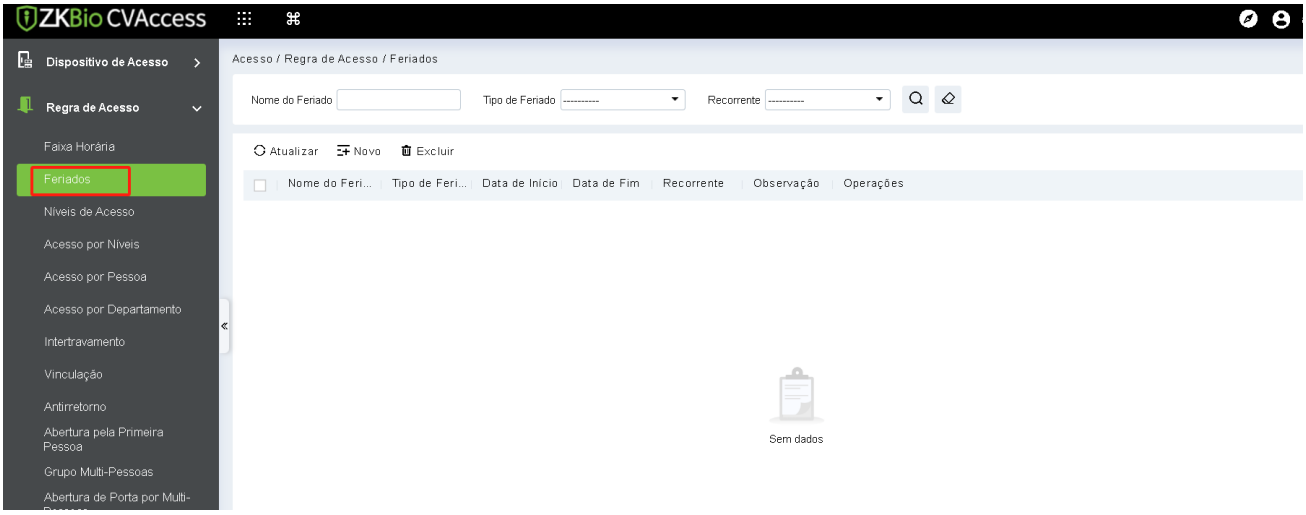
Modificar Zonas Horárias de Controle de Acesso

- **Editar:** Clique no botão no módulo de Operação para entrar na interface de edição. Depois de editar, clique em [OK] para salvar.

- **Excluir:** Clique no botão no módulo de Operação, depois clique em [OK] para excluir, ou clique em [Cancelar] para cancelar a operação. Uma zona horária em uso não pode ser excluída. Uma maneira alternativa é selecionar as caixas de seleção de uma ou mais zonas horárias na lista e clicar no botão [Excluir] sobre a lista, depois clique em [OK] para excluir, ou clique em [Cancelar] para cancelar a operação.

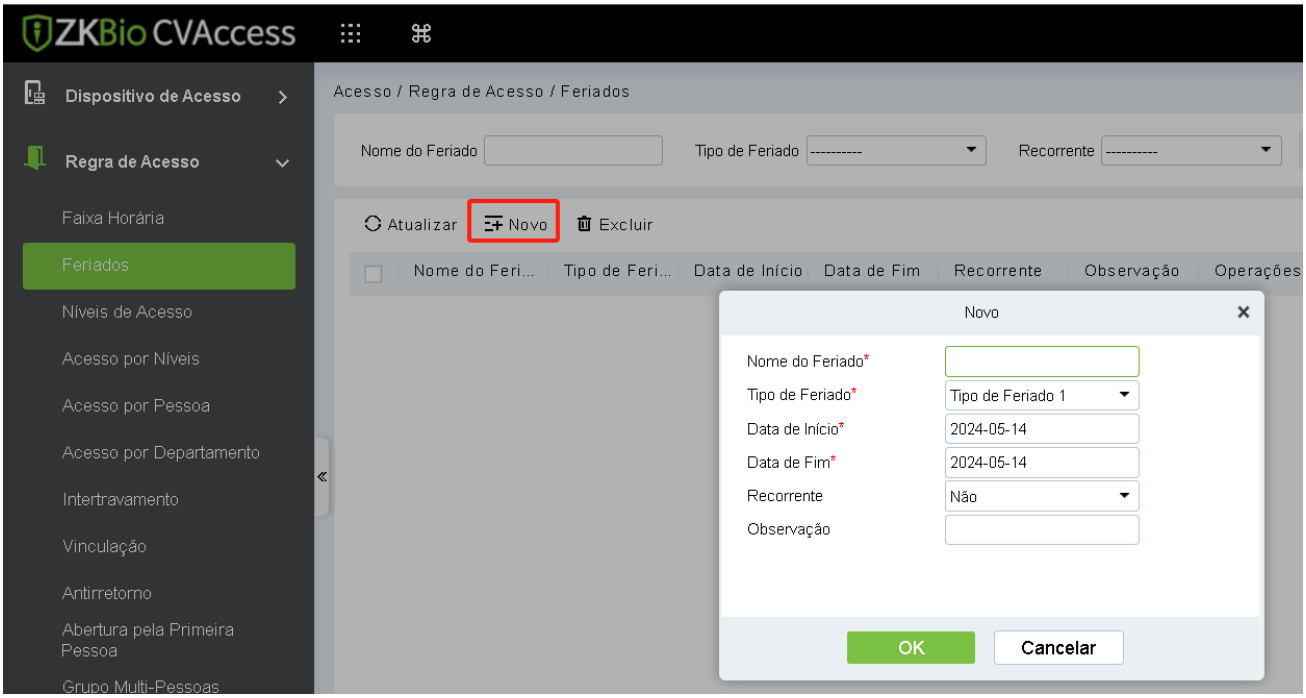
4.2.2 Feriados

O horário de controle de acesso de um feriado pode ser diferente do de um dia da semana. O sistema fornece configuração de horário de controle de acesso para feriados. O Gerenciamento de Feriados de Controle de Acesso inclui Adicionar, Modificar e Excluir.



Adicionar

1) Clique em **[Regra de Acesso] > [Feriados] > [Novo]** para acessar a interface de edição.



Os campos são os seguintes:

- **Nome do Feriado:** Pode conter qualquer caractere, até uma combinação de 30 caracteres.
- **Tipo de Feriado:** Tipo de Feriado 1/2/3, conforme explicado em Feriado. Um registro de feriado atual pertence a um desses três tipos de feriados, cada um incluindo até 32 feriados.
- **Data de Início/Fim:** O formato de data é 2019-01-01. A Data de Início não pode ser posterior à Data de Fim; caso contrário, o sistema emitirá uma mensagem de erro. O ano da Data de Início não pode ser anterior ao ano atual, e o feriado não pode ser definido em dois anos diferentes.
- **Recorrente:** Usado quando o feriado se repete na mesma data a cada ano. O padrão é Não. Por exemplo, o Dia de Ano Novo é em 1º de janeiro de cada ano e pode ser definido como Sim. Algumas datas festivas mudam a cada ano, então não podem ser definidas como recorrentes e devem ser configuradas como Não.

Por exemplo, a data do Dia de Ano Novo é definida como 1º de janeiro de 2019 e o tipo de feriado é 1, então em 1º de janeiro, o Controle de Tempo de Acesso não seguirá o horário de terça-feira, mas o Horário de Controle de Acesso do Tipo de Feriado 1.

2) Após a edição, clique no botão [OK] para salvar e será exibido na lista de feriados.

Modificar

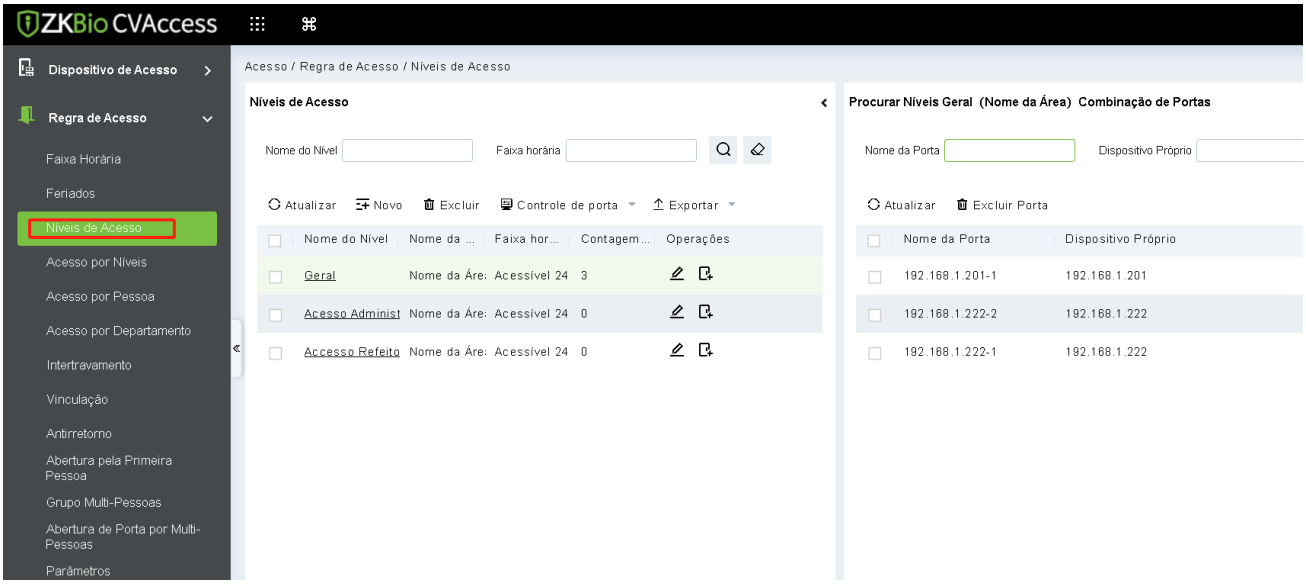
Clique no Nome do Feriado ou no botão sob Operações para acessar a interface de edição. Após a modificação, clique em [OK] para salvar e sair.

Excluir

Na lista de feriados do controle de acesso, clique no botão sob Operações. Clique em [OK] para excluir ou [Cancelar] para cancelar a operação. Um Feriado de Controle de Acesso em uso não pode ser excluído.

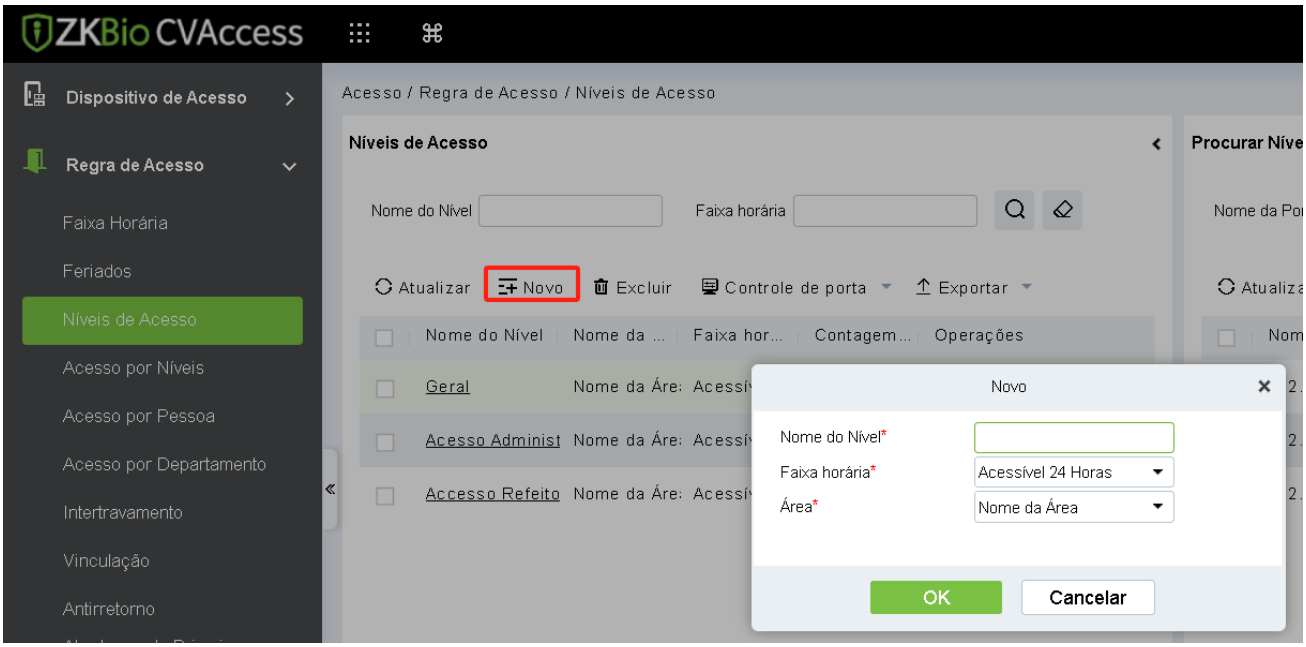
4.2.3 Níveis de Acesso

Os níveis de acesso indicam que uma ou várias portas selecionadas podem ser abertas mediante a autenticação de uma combinação de diferentes pessoas dentro de uma determinada zona horária. A combinação de diferentes pessoas é definida na opção de Nível de Acesso de Pessoal.



Adicionar

1) Clique em **[Regra de Acesso]** > **[Níveis de Acesso]** > **[Novo]** para acessar a interface de edição Adicionar Níveis.

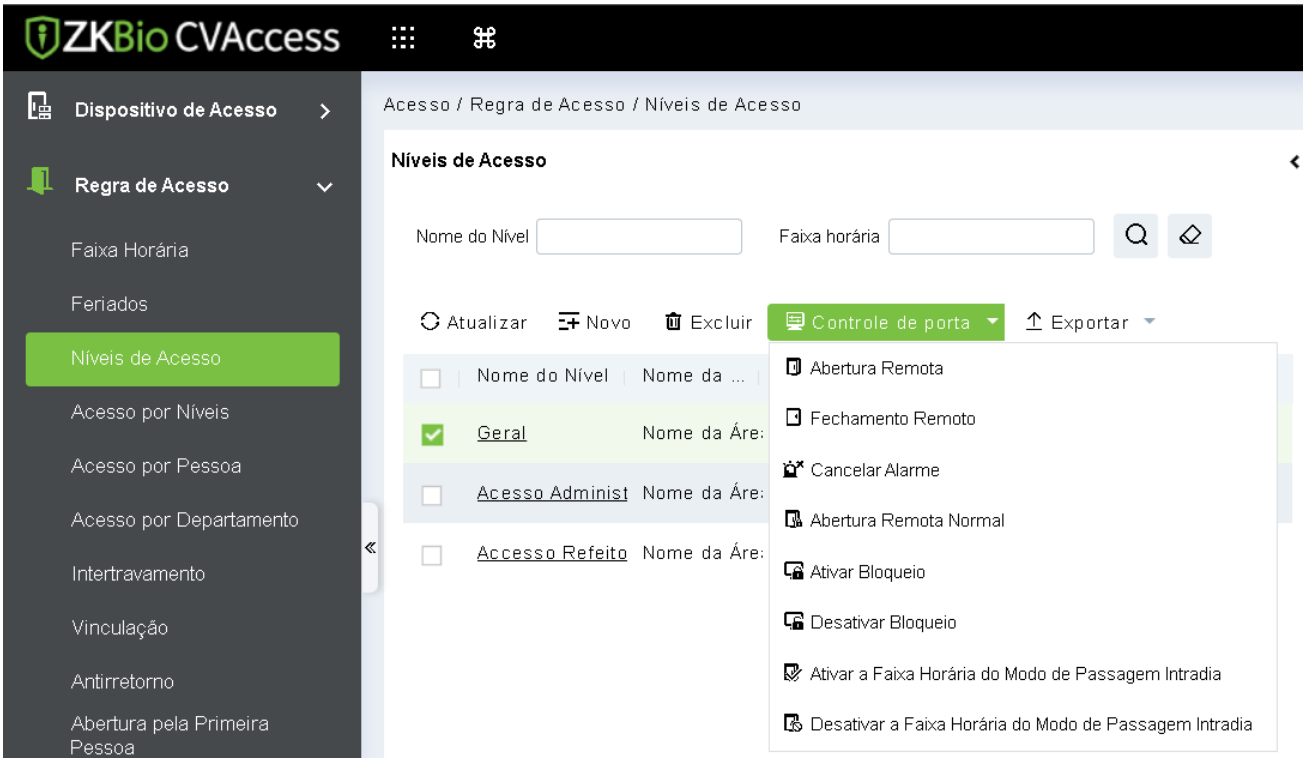


2) Configure cada parâmetro: Nome do Nível (não deve ser o mesmo que outros nomes de níveis), Zona Horária.
3) Clique em **[OK]** e então o sistema irá prompt "Adicionar imediatamente portas ao Nível de Controle de Acesso atual", clique em **[OK]** para adicionar portas, ou você pode clicar em **[Cancelar]** para voltar à lista de níveis de acesso. O nível de acesso adicionado será exibido na lista.

Nota: Diferentes portas de diferentes painéis podem ser selecionadas e adicionadas a um nível de acesso.

Controle de Porta

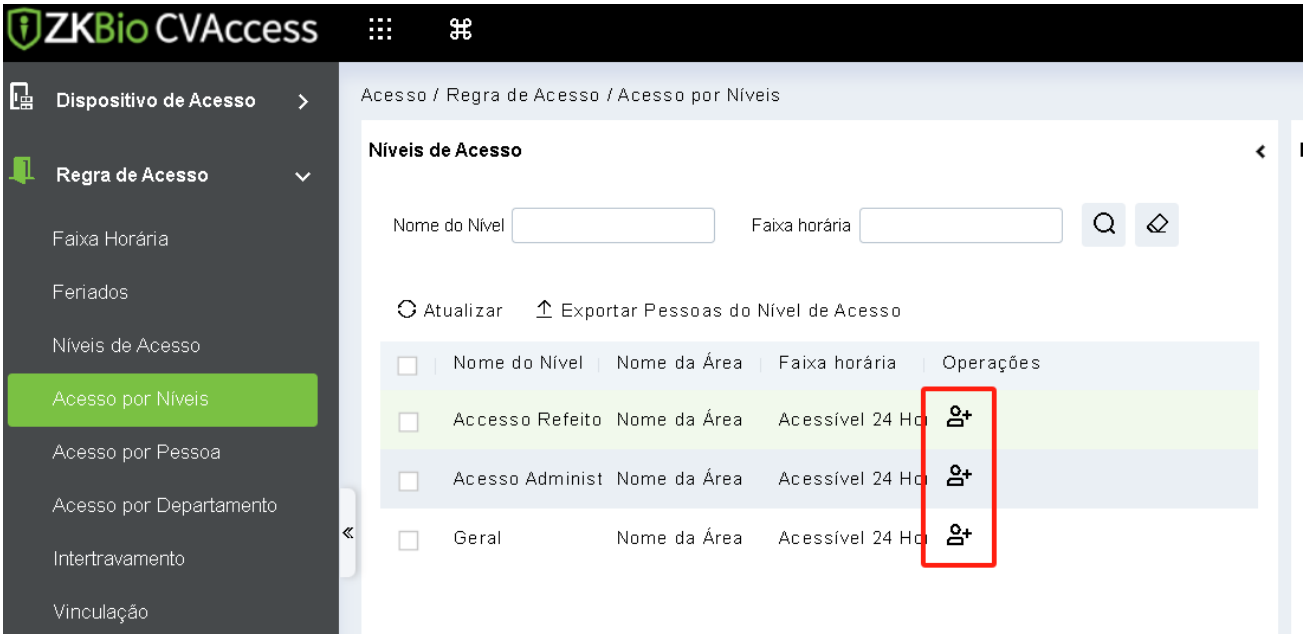
Clique em [Regra de Acesso] > [Níveis de Acesso], escolha o nível de acesso, clique em controle de porta, a operação afetará todas as portas deste nível de acesso.



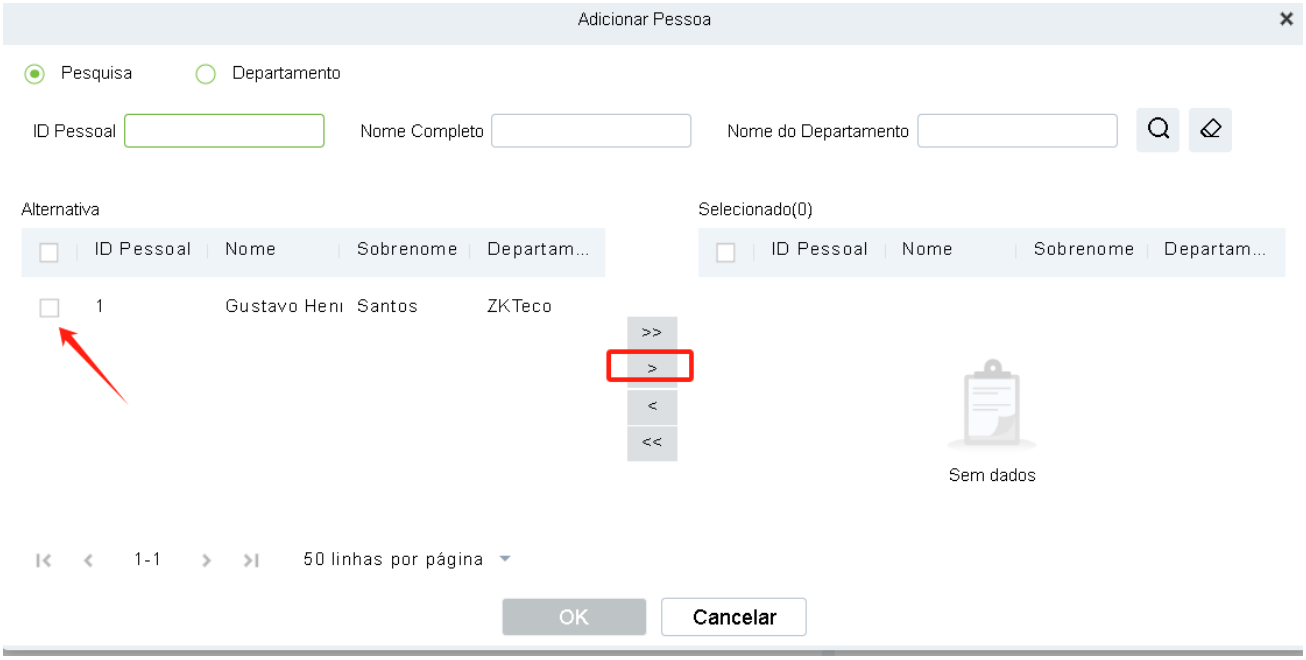
4.2.4 Configuração de Acesso por Níveis

Adicionar/Excluir Pessoa para Níveis

1) Clique em [Regra de Acesso] > [Níveis de Acesso] > [Definir Acesso por Níveis] para acessar a interface de edição, então selecione um Nível de Acesso na lista à esquerda, as pessoas que têm o direito de abrir portas neste nível de acesso serão exibidas na lista à direita.



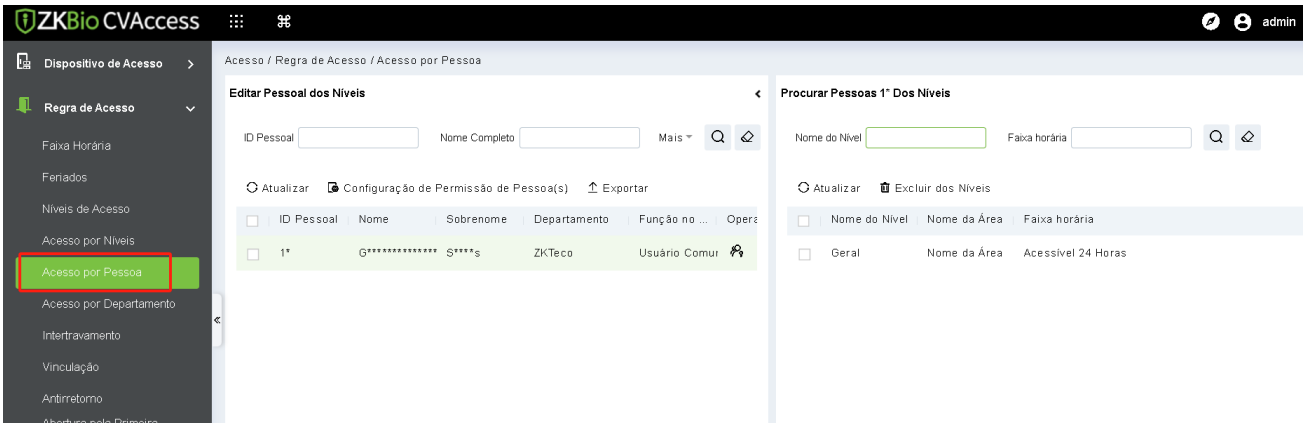
2) Na lista à esquerda, clique em baixo de Operações para abrir a caixa de Adicionar Pessoa; selecione a(s) pessoa(s) e clique para movê-la(s) para a lista selecionada à direita, depois clique em **[OK]** para salvar e sair.



3) Clique no nível para visualizar as pessoas na lista à direita. Selecione as pessoas e clique em **[Excluir Pessoa]** acima da lista à direita, então clique em **[OK]** para excluir.

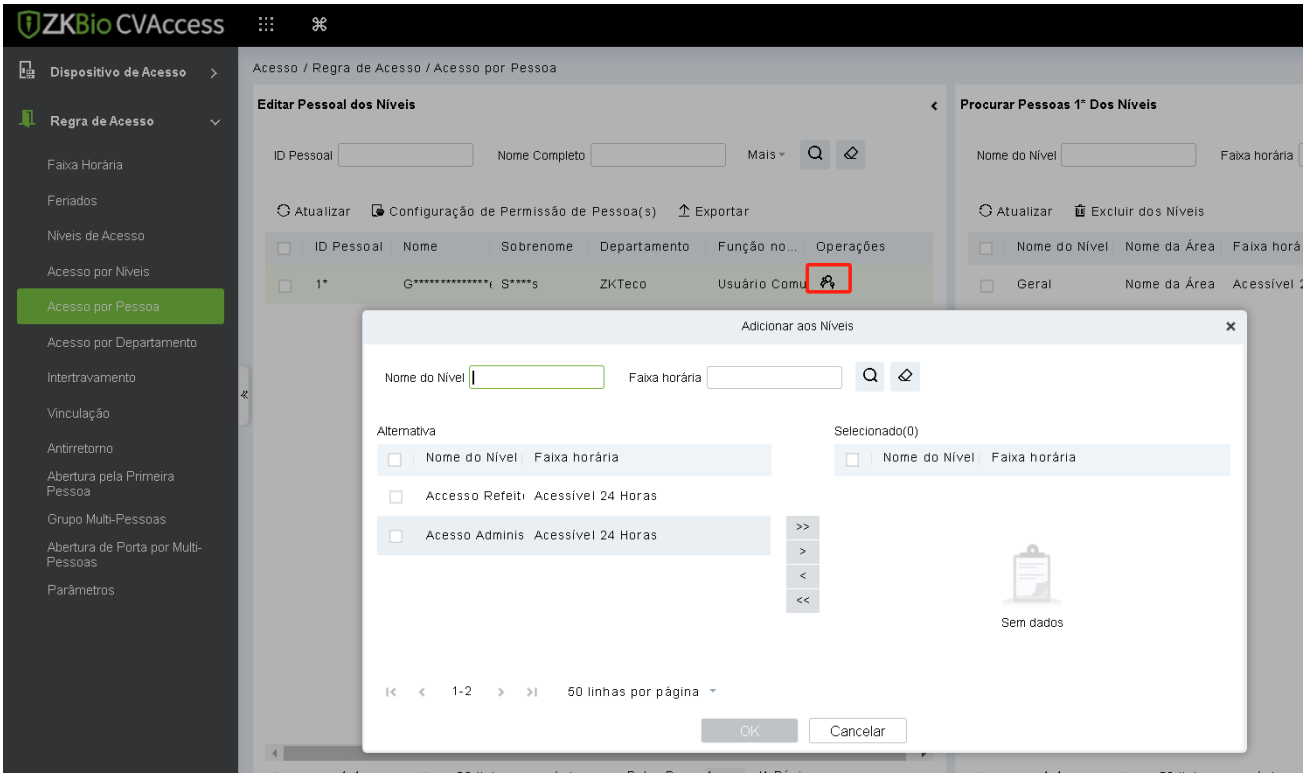
4.2.5 Configurar Acesso por Pessoa

Adicionar pessoas selecionadas aos níveis de acesso selecionados ou excluir pessoas selecionadas dos níveis de acesso.



Adicionar/Excluir níveis para Pessoas Selecionadas

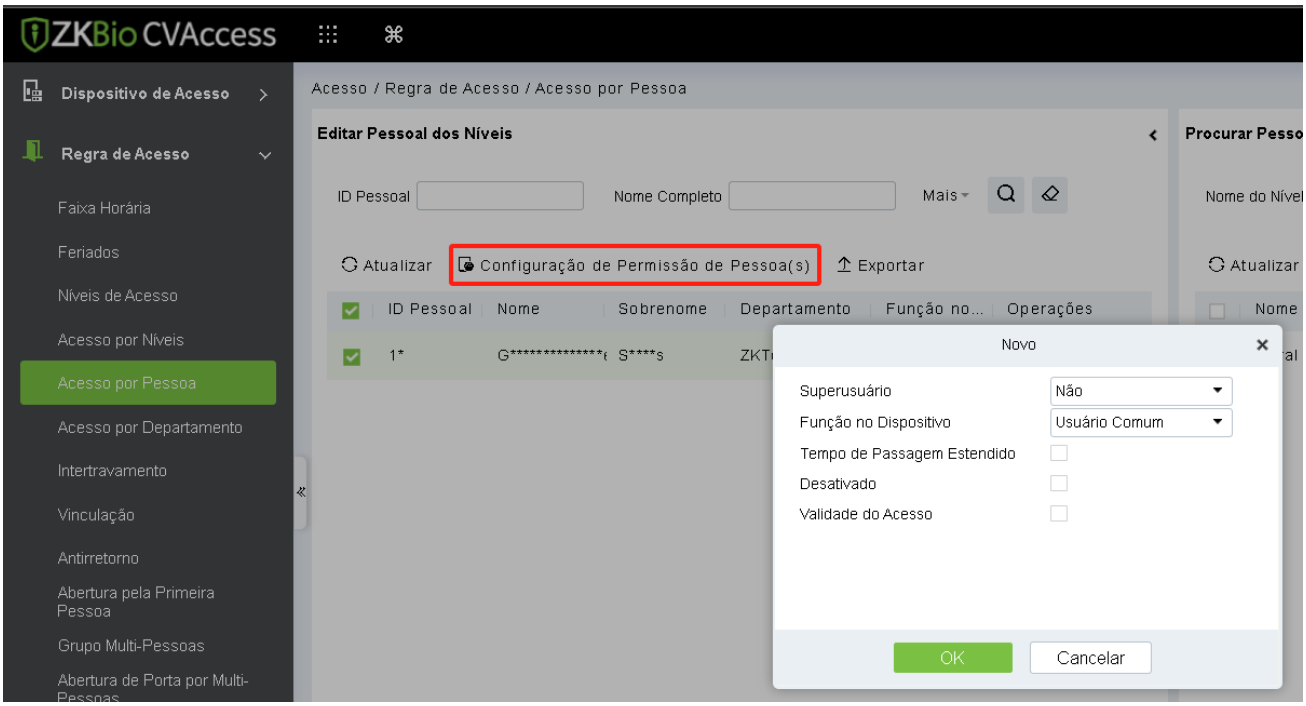
1) Clique em **[Regra de Acesso] > [Níveis de Acesso] > [Definir Acesso por Pessoa],** clique em Funcionário para visualizar os níveis na lista à direita.
2) Clique no botão no módulo de Operações para abrir a caixa Adicionar aos Níveis, selecione o(s) Nível(is) e clique para movê-lo(s) para a lista selecionada à direita; então clique em [OK] para salvar.



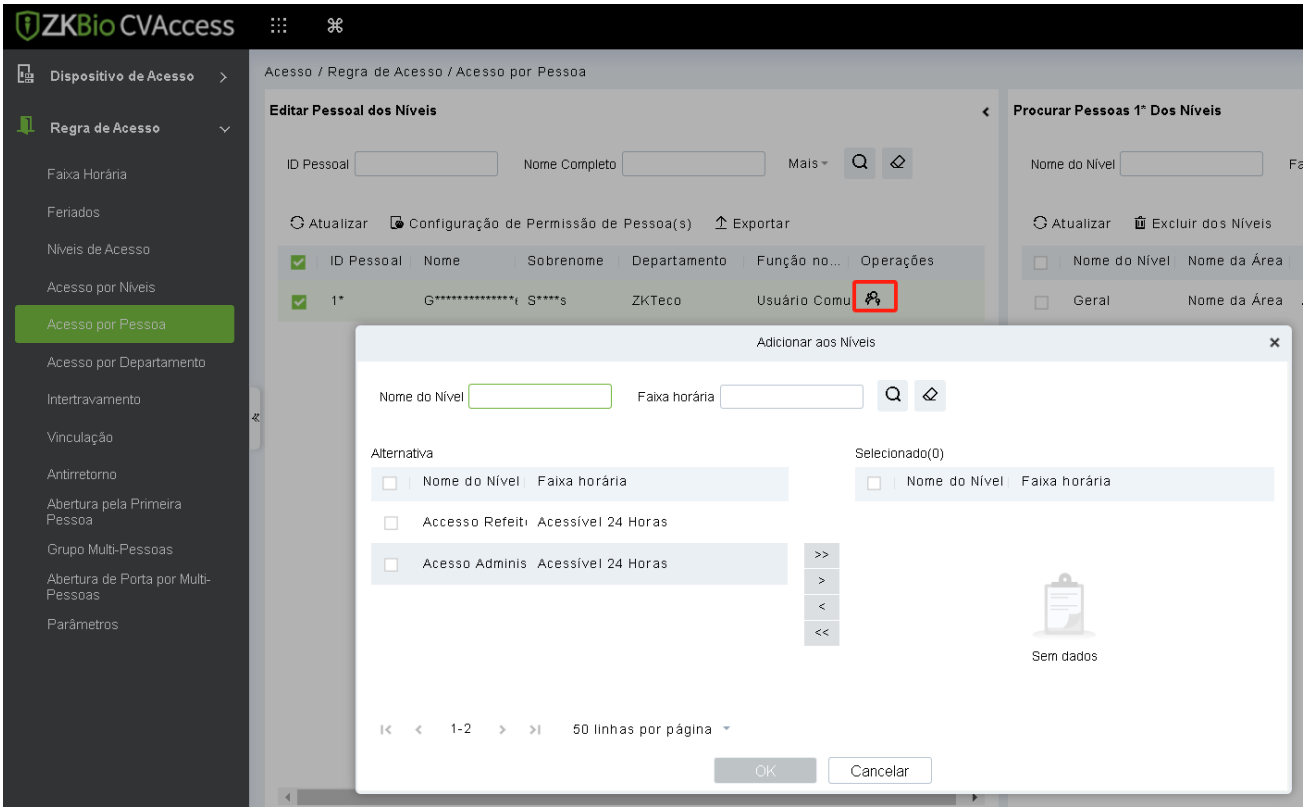
3) Selecione o(s) Nível(is) na lista à direita e clique em [Excluir dos níveis] acima da lista, então clique em [OK] para excluir os níveis selecionados.

Configuração de Controle de Acesso para Pessoas Selecionadas

1) Selecione uma pessoa na lista à esquerda e clique em [Configuração de Controle de Acesso].



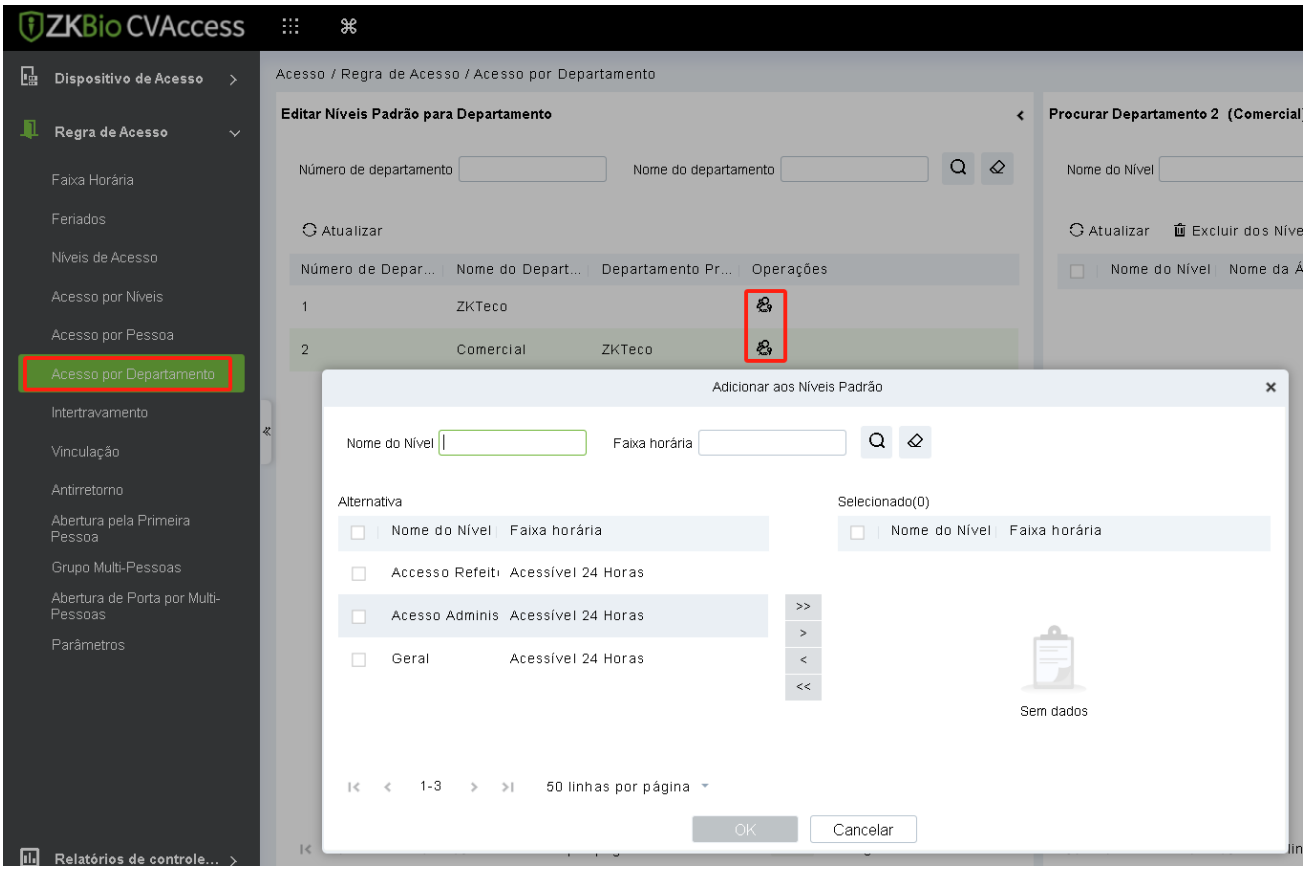
2) Se necessário, defina os parâmetros de controle de acesso e clique em [OK] para salvar as configurações.
3) Agora você precisa adicionar os níveis à(s) pessoa(s).



4) Depois de selecionar o(s) nível(is) necessário(s), clique em OK para salvar e sair.

4.2.6 Configurar Acesso por Departamento

Você pode adicionar o departamento selecionado aos níveis de acesso selecionados ou excluir o departamento selecionado dos níveis de acesso. O acesso das pessoas no departamento será alterado.



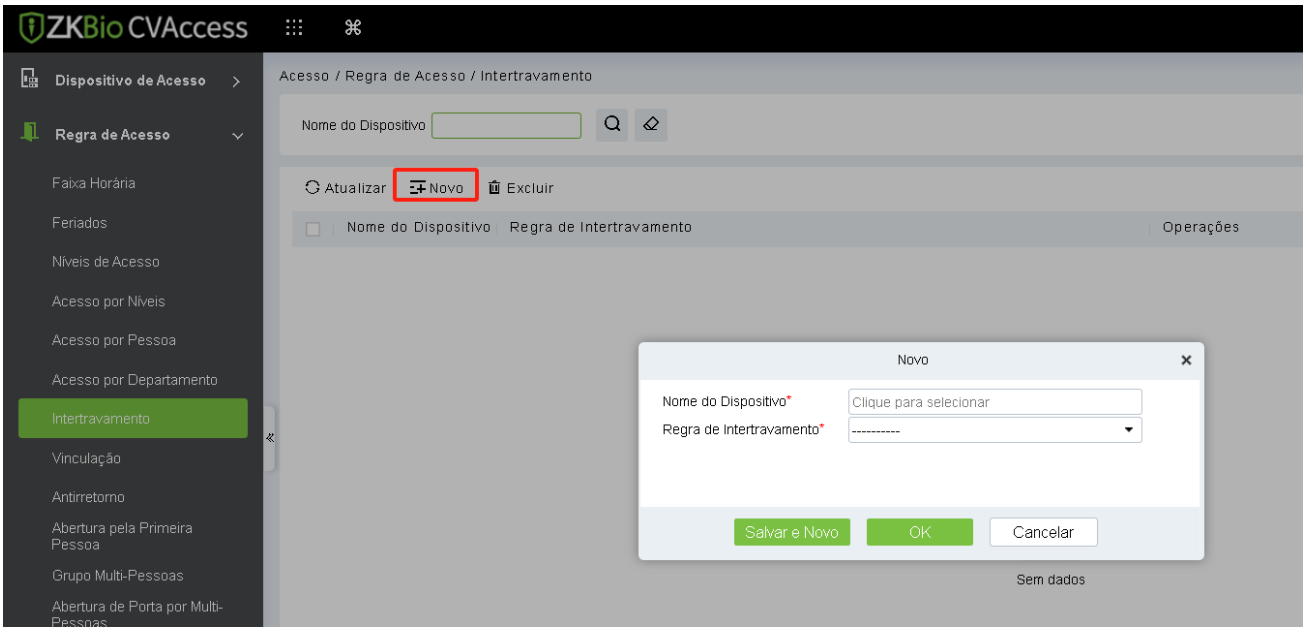
4.2.7 Intertravamento

O intertravamento pode ser configurado para dois ou mais fechaduras pertencentes a um controlador de acesso. Quando uma porta é aberta, as outras serão fechadas, ou você não pode abrir a porta.

Antes de configurar o intertravamento, certifique-se de que o controlador de acesso está conectado ao sensor de porta, que foi definido como estado NC ou NO.

Adicionar Intertravamento

1) Clique **em [Regra de Acesso] > [Intertravamento] > [Novo]** para acessar a interface de edição.



2) Selecione o Dispositivo necessário. Quando os usuários estão adicionando dispositivos, os dispositivos intertravados não podem ser vistos na lista suspensa. Após excluir informações de intertravamento estabelecidas, o dispositivo correspondente retornará à lista suspensa. A configuração de intertravamento variará com o número de portas controladas pelos dispositivos selecionados:

- Um painel de controle de uma porta não possui configurações de intertravamento.
- Um painel de controle de duas portas: 1-2 configurações de intertravamento de duas portas.
- Um painel de controle de quatro portas: 1-2 configurações de intertravamento de duas portas; 3-4 configurações de intertravamento de duas portas; 1-2-3 configurações de intertravamento de três portas; 1-2-3-4 configurações de intertravamento de quatro portas.

3) Selecione a Regra de Intertravamento, selecione um item e clique em [OK] para concluir. As configurações de intertravamento recém-adicionadas serão exibidas na lista.

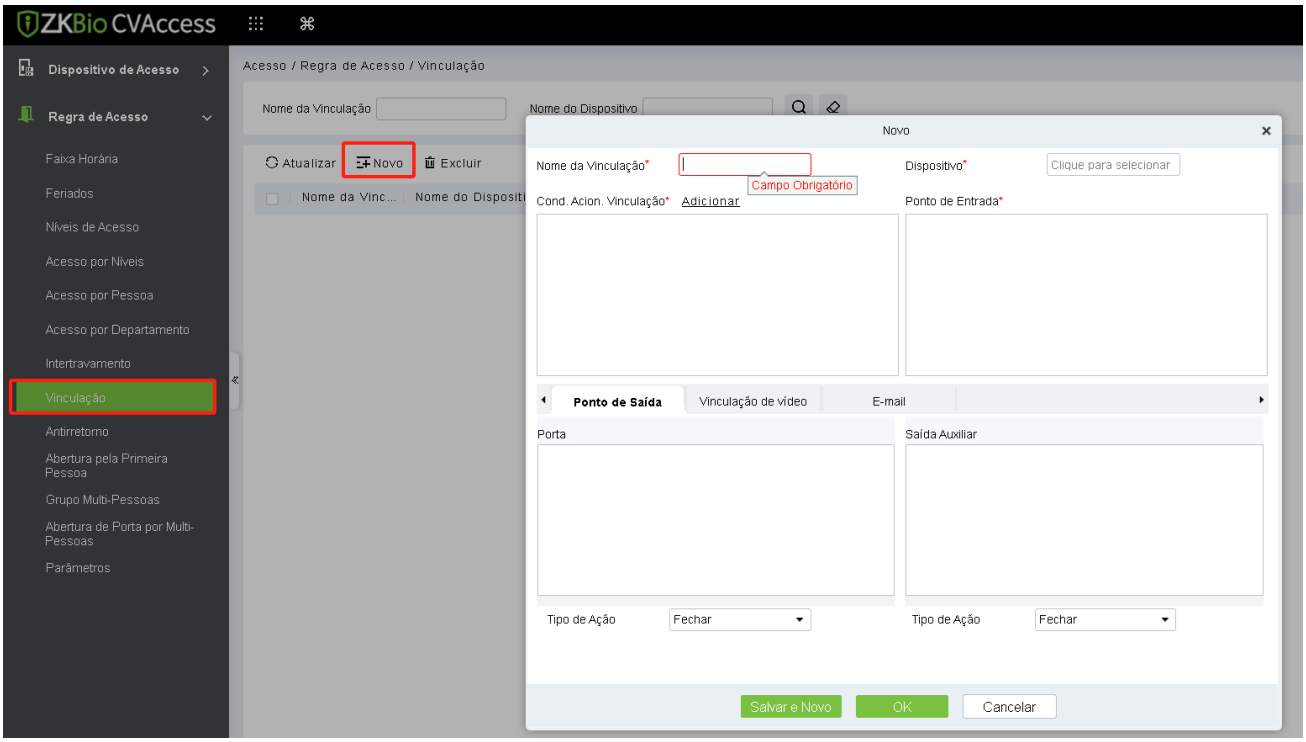
Nota: Durante a edição, o dispositivo não pode ser modificado, mas as configurações de intertravamento podem ser modificadas. Se as configurações de intertravamento não forem mais necessárias para o dispositivo, o registro de configuração de intertravamento pode ser excluído. Se os usuários excluírem um registro de dispositivo, seu registro de configuração de intertravamento, se houver, será excluído.

4.2.8 Vínculo

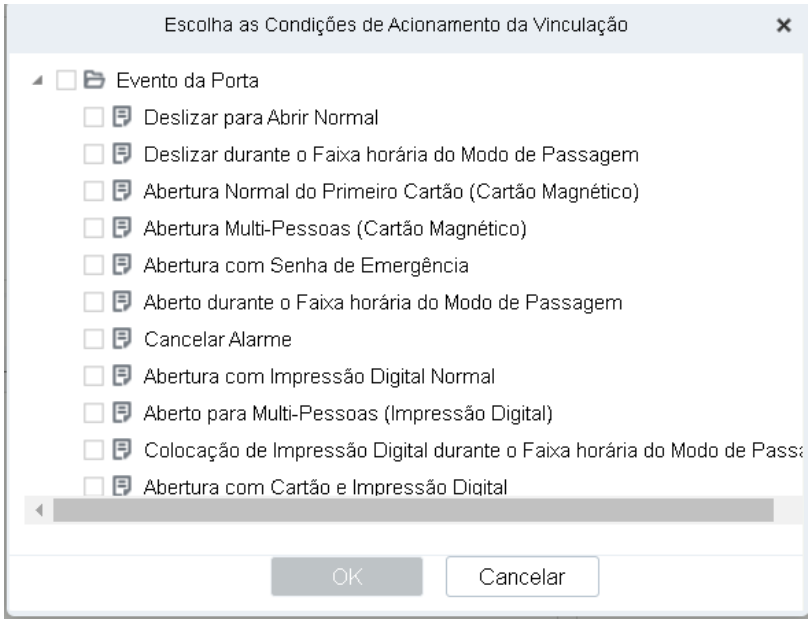
A configuração de vínculo significa que quando um evento é acionado em um ponto de entrada do sistema de controle de acesso, uma ação de vínculo ocorrerá no ponto de saída especificado para controlar eventos como verificação, abertura, alarme e anormalidade do sistema, e listá-los na visualização de monitoramento correspondente.

Adicionar Configuração de Vínculo

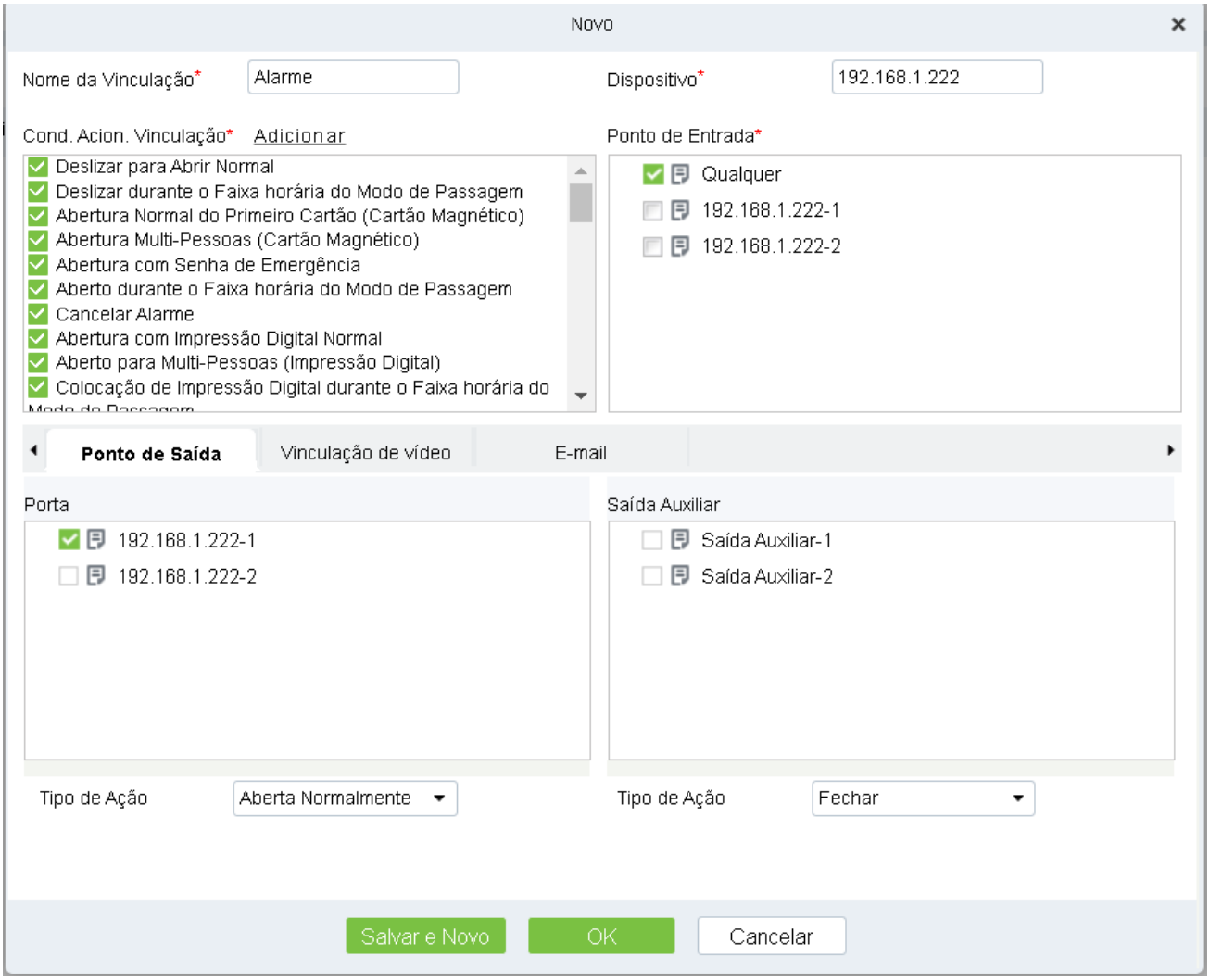
1) Clique em **[Regra de Acesso] > [Vínculo] > [Novo].**



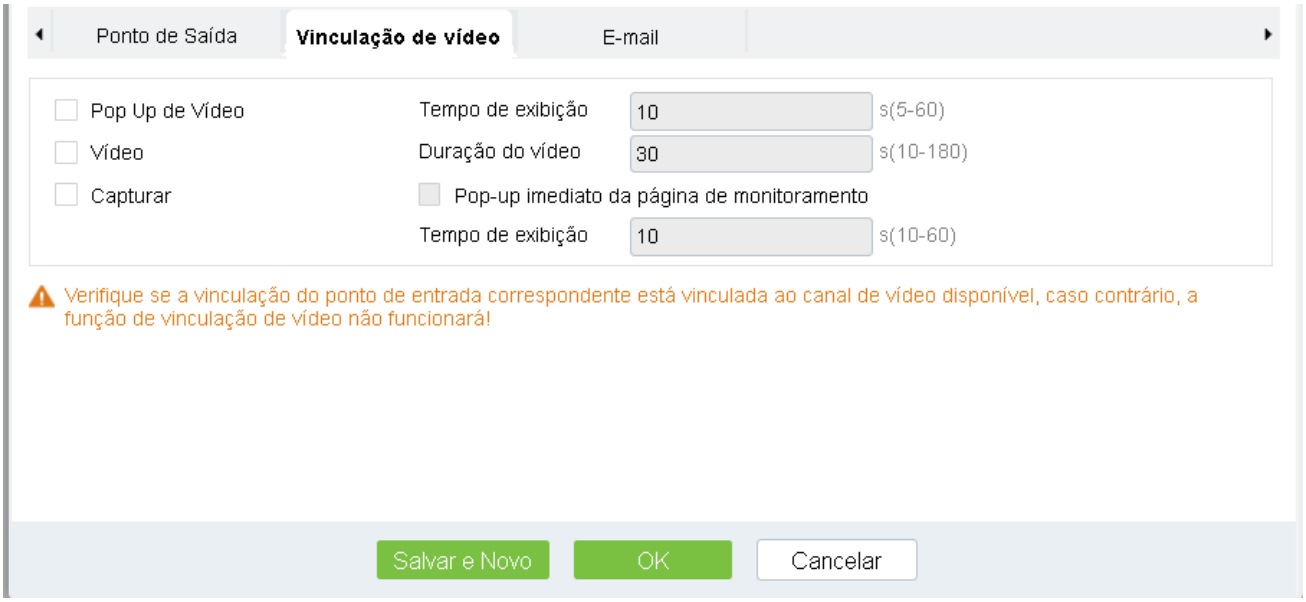
2) Digite o nome do link, selecione um dispositivo de link, condições de acionamento de link, ponto de entrada, ponto de saída e, em seguida, defina a ação de link, vínculo de vídeo e outros parâmetros.
3) Após selecionar os dispositivos, as configurações de vínculo correspondentes serão exibidas. O sistema primeiro julgará se o dispositivo está conectado com sucesso e lê os parâmetros estendidos. Se não houver parâmetros estendidos disponíveis, o sistema não poderá definir nenhum vínculo. Se houver um ou mais parâmetros estendidos disponíveis, o sistema mostrará as configurações de vínculo de acordo com a quantidade de portas, entrada auxiliar e quantidade de saída do dispositivo atualmente selecionado:



Nota: As Condições de Acionamento do Vínculo contêm Evento de Porta e Evento de Entrada Auxiliar. E "Falha ao conectar ao servidor", "Recuperar conexão" e "Desconexão do dispositivo" serão filtrados do Evento de Porta.



4) Selecione o Ponto de Entrada e Ponto de Saída, Ação de Vínculo e Endereço de E-mail.
5) É possível configurar o vínculo de vídeo, usado com o Módulo VMS, para mais detalhes, consulte o módulo VMS.



Os campos são os seguintes:

- **Nome do Vínculo:** Defina um nome para o vínculo.
- **Condição de Acionamento do Vínculo:** Contém condições de acionamento para Porta e Entrada Auxiliar. Essas condições acionam o tipo de evento do dispositivo selecionado. Todos os eventos podem ser uma condição de acionamento.
- **Ponto de Entrada:** Selecione o ponto de entrada de acionamento apropriado (o ponto de entrada específico deve se referir aos parâmetros específicos do dispositivo).
- **Ponto de Saída:** Selecione o ponto de saída necessário (o ponto de saída específico deve se referir aos parâmetros específicos do dispositivo).
- **Tipo de Ação:** Fechar, Abrir, Normal Aberto. O padrão é Fechar. Para abrir, é necessário definir o tempo de atraso ou Normal Aberto.

6) Após editar, clique em [OK] para salvar e sair, em seguida, as configurações de vínculo adicionadas serão exibidas na lista.

Por exemplo, se os usuários selecionarem "Abrir Normalmente ao Bater na Porta" como condição de acionamento, e o ponto de entrada for Porta 1, o ponto de saída for Fechadura 1, o tipo de ação for Abrir e o atraso for de 60 segundos. Quando "Abrir Normalmente ao Bater na Porta" ocorrer na Porta 1, a ação de vínculo de Abrir ocorrerá na Fechadura 1, e a porta ficará aberta por 60 segundos.

Nota: Durante a edição, você não pode modificar o dispositivo, mas pode modificar o nome e a configuração do vínculo. Quando excluir um dispositivo, o registro de configuração do vínculo, se houver, será excluído.

Se o dispositivo e a condição de acionamento forem iguais, e o sistema tiver um registro de configuração de vínculo onde o ponto de entrada é uma porta específica ou entrada auxiliar, ele não permitirá que os usuários adicionem (ou editem) um registro de configuração de vínculo onde o ponto de entrada é qualquer um.

Ao contrário, se o dispositivo e a condição de acionamento forem iguais, e o sistema tiver um registro de configuração de vínculo onde o ponto de entrada é "Qualquer", ele não permitirá que o usuário adicione (ou edite) um registro de configuração de vínculo onde o ponto de entrada é uma porta específica ou entrada auxiliar.

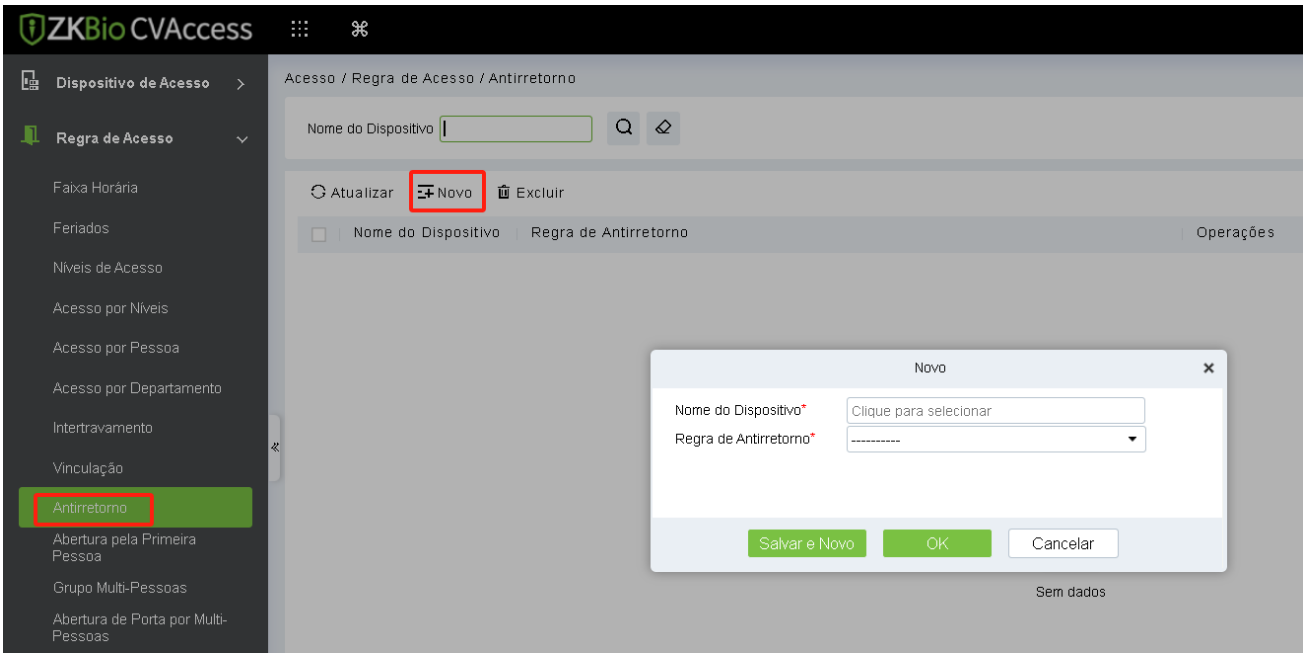
Além disso, o mesmo vínculo no ponto de entrada e ponto de saída não é permitido. O mesmo dispositivo permite configurações de vínculo lógico consecutivas. O sistema permite configurar várias condições de acionamento para um vínculo de uma só vez.

4.2.9 Anti-Passback

Atualmente, as configurações de Anti-Passback suportam Anti-Passback de entrada e saída. Em algumas ocasiões especiais, é necessário que os titulares de cartão que entraram por uma porta ao passar o cartão em um dispositivo na porta também passem o cartão sobre um dispositivo na mesma porta ao sair, para manter os registros de entrada e saída estritamente consistentes. O usuário pode usar essa função apenas habilitando-a nas configurações. Essa função é normalmente usada em prisões, no exército, defesa nacional, pesquisa científica, cofres de banco, etc.

Adicionar Configurações de Anti-Passback

1) Clique em [Regra de Acesso] > [Anti-Passback] > [Novo] para mostrar a interface de edição:



2) Selecione o(s) dispositivo(s) necessário(s). Ao adicionar regras de Anti-Passback, os dispositivos com configurações de Anti-Passback não serão visíveis na lista suspensa. Ao excluir informações estabelecidas de Anti-Passback, o dispositivo correspondente voltará a aparecer na lista suspensa. As configurações variam de acordo com o número de portas controladas pelo dispositivo.

- Configurações de Anti-Passback de um painel de controle de uma porta: Anti-Passback entre leitores de portas.
- Configurações de Anti-Passback de um painel de controle de duas portas: Anti-Passback entre leitores da porta 1; Anti-Passback entre leitores da porta 2; Anti-Passback entre porta 1 e porta 2.
- Configurações de Anti-Passback de um painel de controle de quatro portas: Anti-Passback da porta 1 e porta 2; Anti-Passback da porta 3 e porta 4; Anti-Passback da porta 1/2 e porta ¾; Anti-Passback da porta 1 e porta 2/3; Anti-Passback da porta 1 e porta 2/3/4; Anti-Passback entre leitores de porta 1/2/3/4.

Nota: O leitor de porta mencionado acima inclui o leitor Wigand que está conectado ao controlador de acesso e o leitor Indio. O controlador de uma ou duas portas com leitor Wigand inclui leitor de entrada e saída. Há apenas "Leitor de entrada" para o painel de controle de quatro portas. O número do leitor de 1, 2 (endereço RS485 ou número do dispositivo, o mesmo abaixo) é para a porta 1, o número do leitor de 3, 4 é para a porta 2, etc. Não é necessário considerar se é um leitor Wigand ou leitor InBio ao definir o Anti-Passback entre portas ou entre leitores, apenas certifique-se de que o leitor de entrada ou saída esteja configurado de acordo com os requisitos reais. Para o número do leitor, um número ímpar é para o leitor de entrada, um número par é para o leitor de saída.

3) Seleccione a Regra de Anti-Passback, e seleccione um item, clique em [OK] para concluir, e em seguida, as configurações de Anti-Passback adicionadas serão exibidas na lista.

Nota: Durante a edição, não é possível modificar o dispositivo, mas é possível modificar as configurações de Anti-Passback. Se a configuração de Anti-Passback não for mais necessária para o dispositivo, o registro de configuração de Anti-Passback pode ser excluído. Quando você exclui um dispositivo, seu registro de configuração de Anti-Passback, se houver, será excluído.

4.2.10 Abertura Normal por Primeira Pessoa

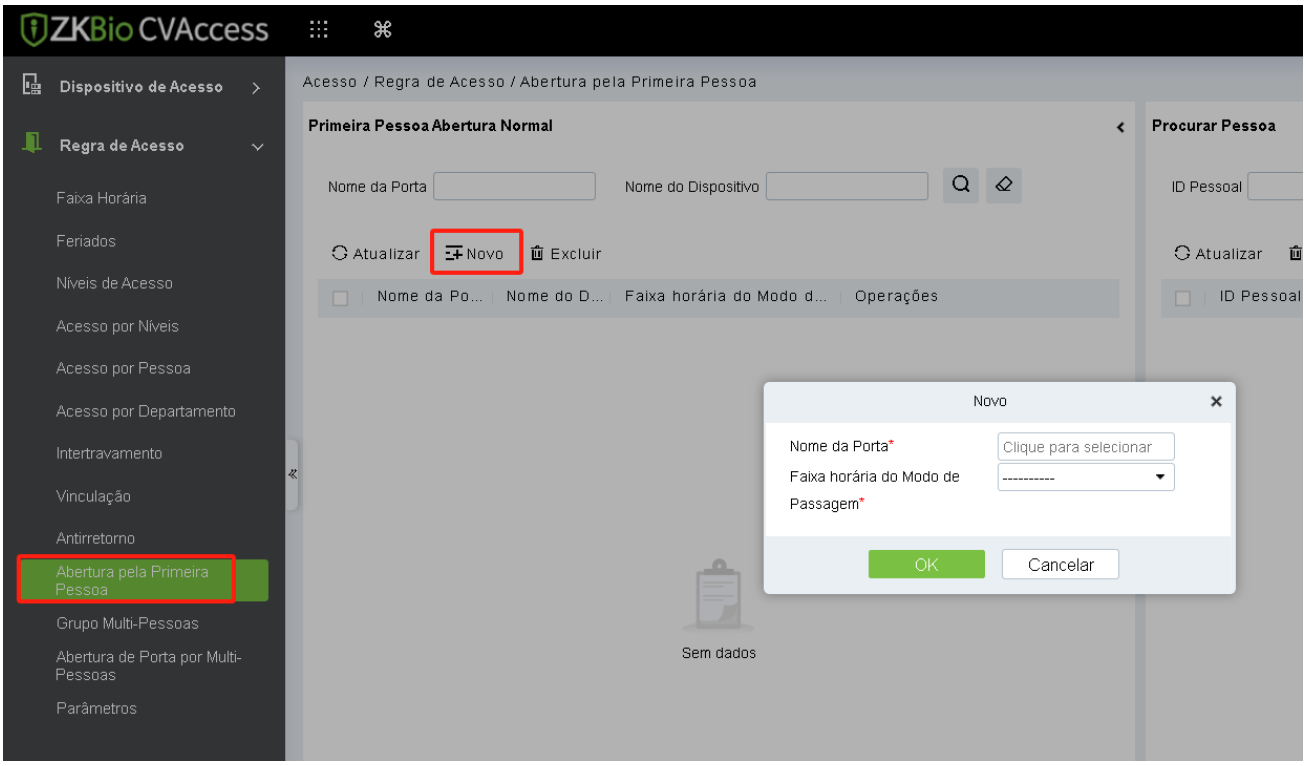
Essa função ajuda a manter a porta aberta por um intervalo de tempo específico após a primeira autenticação pelo pessoal atribuído. Durante o intervalo especificado, se a primeira autenticação for feita por uma pessoa com acesso de Abertura Normal por Primeira Pessoa, então a porta estará Normal Aberta e automaticamente voltará a fechar após expirar o intervalo válido.

Os usuários podem definir Abertura Normal por Primeira Pessoa para uma porta específica (as configurações incluem porta, zona de horário de abertura da porta e pessoal com acesso de Abertura Normal por Primeira Pessoa). Uma porta pode ter Abertura Normal por Primeira Pessoa para múltiplas zonas de horário. A interface de cada porta mostrará o número de Aberturas Normais por Primeira Pessoa existentes.

Ao adicionar ou editar configurações de Abertura Normal por Primeira Pessoa, você só pode selecionar a porta e as zonas de horário. Após uma adição bem-sucedida, o pessoal atribuído pode abrir a porta. Você pode visualizar e excluir o pessoal no lado direito da interface.

Os passos operacionais são os seguintes:

1) Clique em **[Regra de Acesso] > [Abertura Normal por Primeira Pessoa] > [Novo],** selecione o Nome da Porta e o Tempo do Modo de Passagem e clique em [OK] para salvar as configurações.

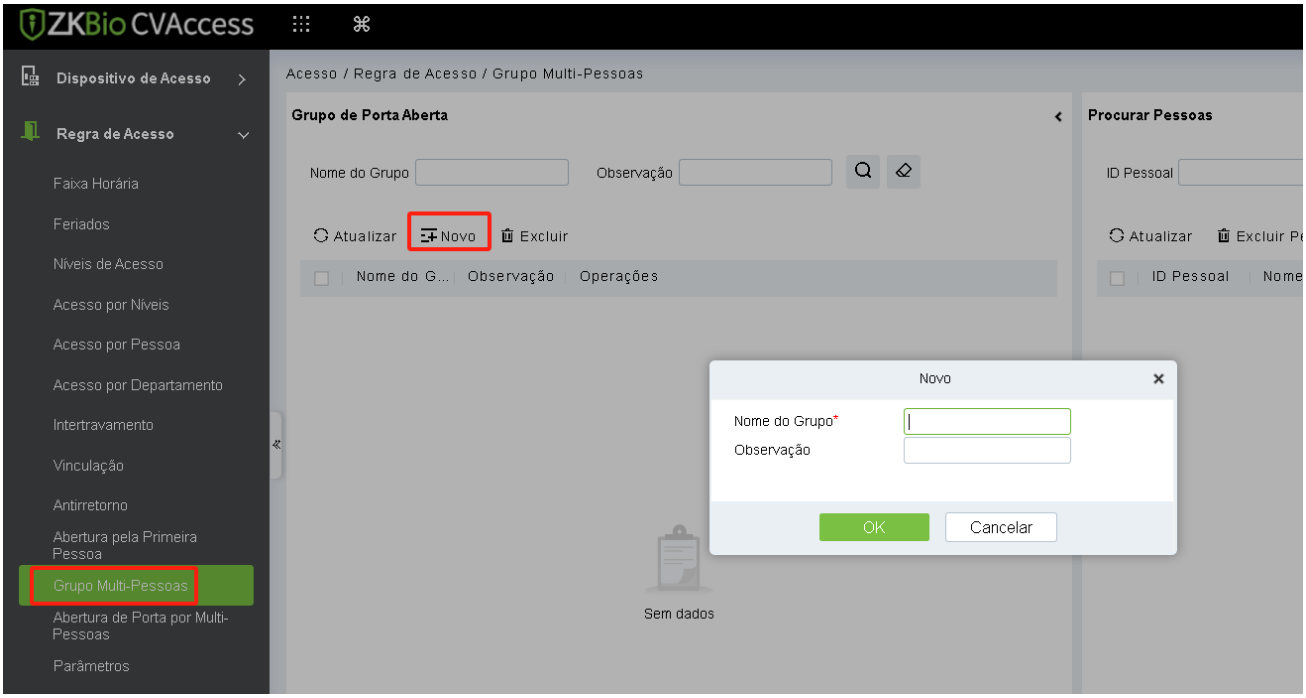


2) Clique no botão na área de Operação para adicionar pessoal com acesso de Abertura Normal por Primeira Pessoa (esse pessoal deve ter nível de controle de acesso), então clique em [OK] para salvar.

4.2.11 Grupo de Múltiplas Pessoas

A porta só será aberta após a verificação consecutiva de múltiplas pessoas. Qualquer pessoa que verifique fora dessa combinação (mesmo que a pessoa pertença a qualquer outra combinação válida) interromperá o procedimento e você precisará esperar 10 segundos para reiniciar a verificação. A porta não pode ser aberta verificando apenas uma das combinações.

1) Clique em **[Regra de Acesso] > [Grupo de Múltiplas Pessoas] > [Novo]** para acessar a seguinte interface de edição:



- **Nome do grupo:** Qualquer combinação de até 30 caracteres que não pode ser idêntica a um nome de grupo existente.

Após editar, clique em **[OK]** para salvar e retornar. O Grupo de Pessoal de Múltiplas Pessoas adicionado aparecerá na lista.

2) Clique no botão na área de Operação para adicionar pessoal ao grupo.
3) Depois de selecionar e adicionar pessoal, clique em [OK] para salvar e retornar.

Nota: Uma pessoa só pode fazer parte de um único grupo.

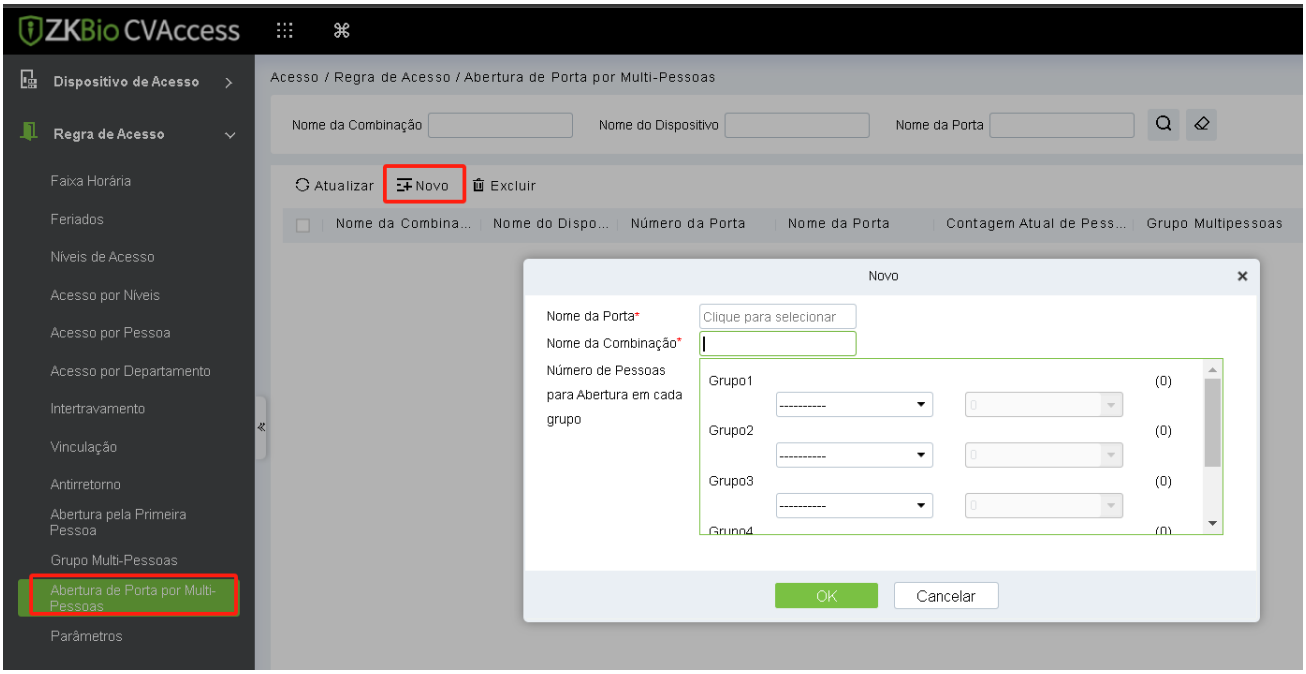
4.2.12 Abertura de Porta por Múltiplas Pessoas

Configure os níveis para o pessoal no Grupo de Pessoal de Múltiplas Pessoas.

É uma combinação do pessoal em um ou mais Grupos de Pessoal de Múltiplas Pessoas. Ao definir o número de pessoas em cada grupo, você pode configurar um grupo (como abertura de porta combinada por duas pessoas em um grupo) ou vários grupos (como abertura de porta combinada por quatro pessoas, incluindo 2 pessoas no grupo 1 e 2 pessoas no grupo 2), e pelo menos um grupo deve consistir em número de pessoas que abrirão a porta em vez de 0, e o número total não deve ser superior a 5. Além disso, se o número de pessoas inseridas for maior do que o do grupo atual, a Abertura de Porta por Múltiplas Pessoas será desativada.

Configurações de Abertura de Porta por Múltiplas Pessoas

1) Clique em **[Regra de Acesso] > [Abertura de Porta por Múltiplas Pessoas] > [Novo]:**

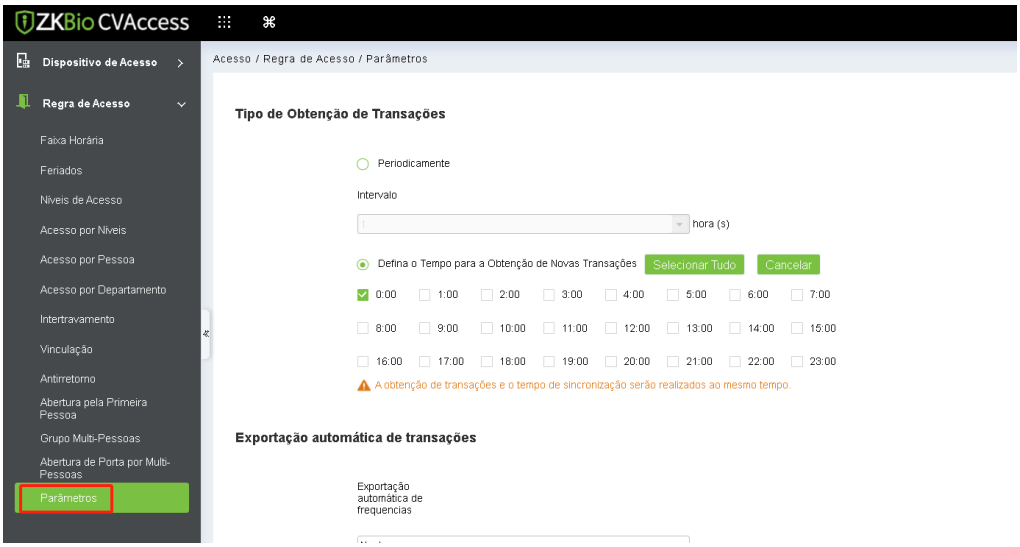


2) O número máximo de pessoas para Abertura de Porta por Múltiplas Pessoas é 5. Os números entre parênteses mostram o número atual real de pessoas em um grupo. Selecione o número de pessoas para a abertura de porta combinada em um grupo e clique em [OK] para completar.

Nota: O Intervalo de Cartão padrão é de 10 segundos, o que significa que o intervalo de verificação de duas pessoas não deve exceder 10 segundos. Você pode modificar o intervalo se o dispositivo suportar.

4.2.13 Parâmetros

Clique em **[Regra de Acesso] > [Parâmetros]** para acessar a interface de configuração de parâmetros:



➢ Tipo de Obtenção de Transações

Periodicamente

O sistema irá baixar novas transações no intervalo de tempo selecionado.

Defina o Tempo para Obter Novas Transações

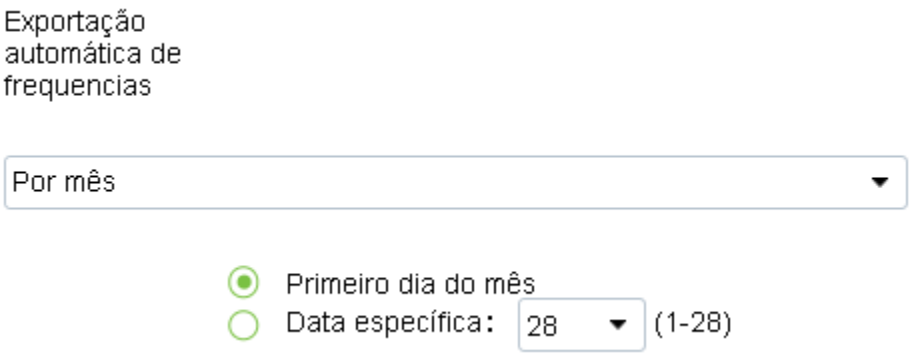
O sistema irá baixar novas transações automaticamente nos momentos selecionados.

➢ **Exportação Automática de Transações**

Frequência de Exportação Automática

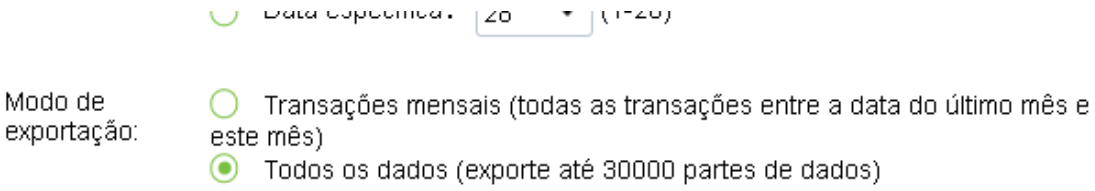
Suporta configurar a Frequência de Exportação Automática por Dia ou Mês. Quando a frequência de exportação automática é configurada por dia, você precisa definir a Hora e o Minuto.

Quando a frequência de exportação automática é configurada por mês, você precisa selecionar se deseja exportar no primeiro dia do mês ou em uma data específica.



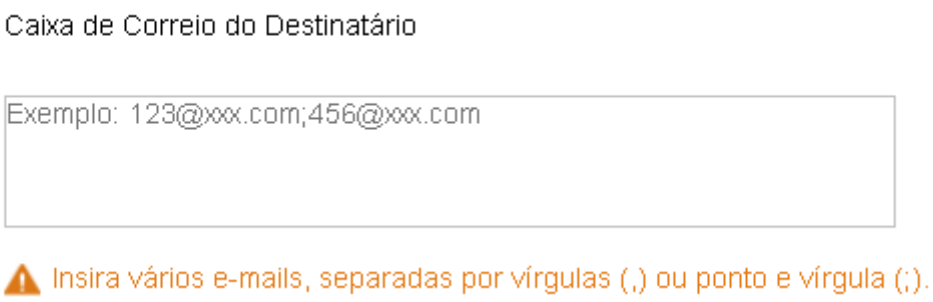
Modo de Exportação

Suporta exportar as Transações Mensais ou Todos os Dados. Em um único momento, o dispositivo pode exportar 30000 dados.



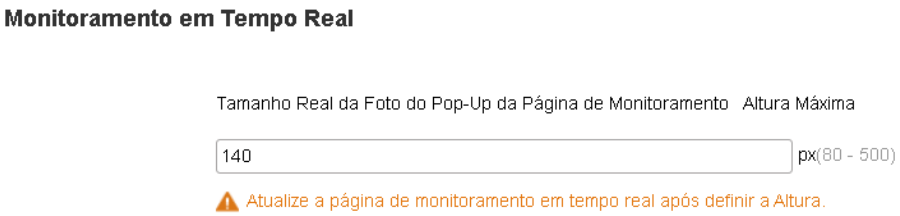
Caixa de Correio do Destinatário

Defina a Caixa de Correio do Destinatário.



➢ **Monitoramento em Tempo Real**

Você pode marcar a caixa de seleção conforme necessário.



Se a exibição de foto estiver selecionada, a página de monitoramento em tempo real exibirá a foto do pessoal durante um evento de controle de acesso. Você pode definir a qualidade da imagem conforme necessário; um valor de px maior fornecerá uma foto mais nítida.

Caixa de Correio do Destinatário para Monitoramento de Alarme: O sistema enviará e-mails para a caixa de correio do destinatário de monitoramento de alarme se houver algum evento.

4.3 Relatórios de Acesso

Inclui "Todas as transações", "Eventos de Hoje", "Todos os Eventos de Exceção" e assim por diante. Você pode exportar após a consulta.

Você pode gerar estatísticas de dados relevantes do dispositivo a partir dos relatórios, incluindo informações de verificação de cartão, informações de operação de porta e informações de abertura normal, etc.

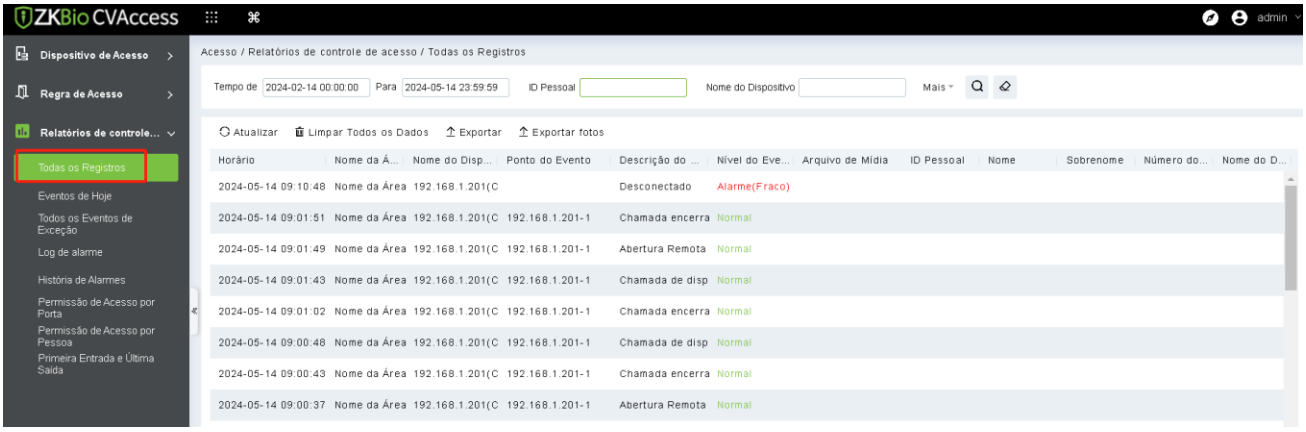
Sobre eventos normais e anormais, consulte o Monitoramento em Tempo Real para obter detalhes.

Modo de Verificação: Apenas Cartão, Apenas Impressão Digital, Apenas Senha, Cartão mais Senha, Cartão mais Impressão Digital, Cartão ou Impressão Digital, etc.

Nota: Somente registros de eventos gerados quando o usuário usa uma senha de emergência para abrir portas incluirão apenas o modo de verificação de senha.

4.3.1 Todas as Transações

Devido à quantidade de dados dos registros de eventos de controle de acesso, você pode visualizar eventos de controle de acesso como uma condição especificada ao consultar. Por padrão, o sistema exibe as transações dos últimos três meses. Clique em **[Relatórios] > [Todas as Transações]** para visualizar todas as transações:



- **Arquivo de Mídia:** Você pode visualizar ou baixar fotos e vídeos.
- **Limpar Todos os Dados:** Clique em [Limpar Todos os Dados] para abrir um prompt e clique em [OK] para limpar todas as transações.
- **Exportar:** Você pode exportar todas as transações em formato Excel, PDF e CSV.

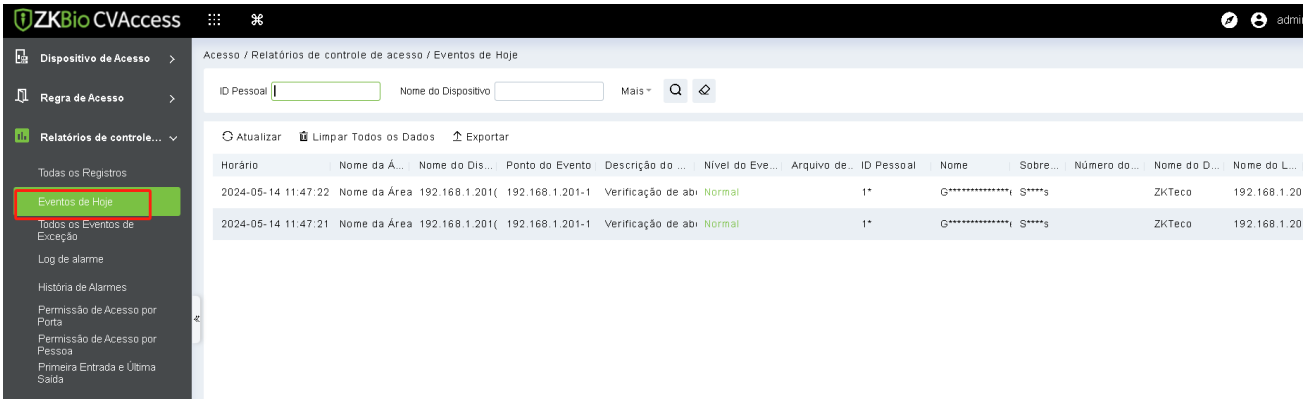
All Transactions

Event ID	Time	Device Name	Event Point	Event Description	Personnel ID	First Name	Last Name	Card Number	Department Number	Department Name	Reader Name	Verification Mode	Area Name	Remark
-1	2018-12-27 19:15:48	SpeedFace-V5		Disconnected							Other	Other	Area Name	
-1	2018-12-27 17:57:30	192.168.213.99		Disconnected							Other	Other	Area Name	
64376	2018-12-27 17:56:04	192.168.213.99		Device Started							Other	Other	Area Name	
64375	2018-12-27 17:48:46	192.168.213.99		Device Started							Other	Other	Area Name	
64374	2018-12-27 17:45:16	192.168.213.99		Device Started							Other	Other	Area Name	
64373	2018-12-27 17:43:24	192.168.213.99		Connected to the server							Other	Other	Area Name	
64372	2018-12-27 17:43:06	192.168.213.99		Device Started							Other	Other	Area Name	
1255	2018-12-27 17:43:01	SpeedFace-V5	SpeedFace-V5-1	Normal Verify Open	575	Jeff			1	ZKTeco	SpeedFace-V5-1-Out	Face	Area Name	
1254	2018-12-27 17:42:53	SpeedFace-V5	SpeedFace-V5-1	Normal Verify Open	575	Jeff			1	ZKTeco	SpeedFace-V5-1-Out	Face	Area Name	
-1	2018-12-27 17:25:29	192.168.213.99		Disconnected							Other	Other	Area Name	
64371	2018-12-27 13:56:46	192.168.213.99		Connected to the server							Other	Other	Area Name	
64370	2018-12-27 13:56:01	192.168.213.99		Device Started							Other	Other	Area Name	
1253	2018-12-27 11:46:48	SpeedFace-V5	SpeedFace-V5-1	Normal Verify Open	575	Jeff			1	ZKTeco	SpeedFace-V5-1-Out	Face	Area Name	

4.3.2 Eventos de Hoje

Verifique os registros do sistema de hoje.

Clique em **[Relatórios]** > **[Eventos de Hoje]** para visualizar os registros de hoje.



Você pode exportar todos os eventos de hoje em formato Excel, PDF e CSV.

ZKTECO

Events From Today

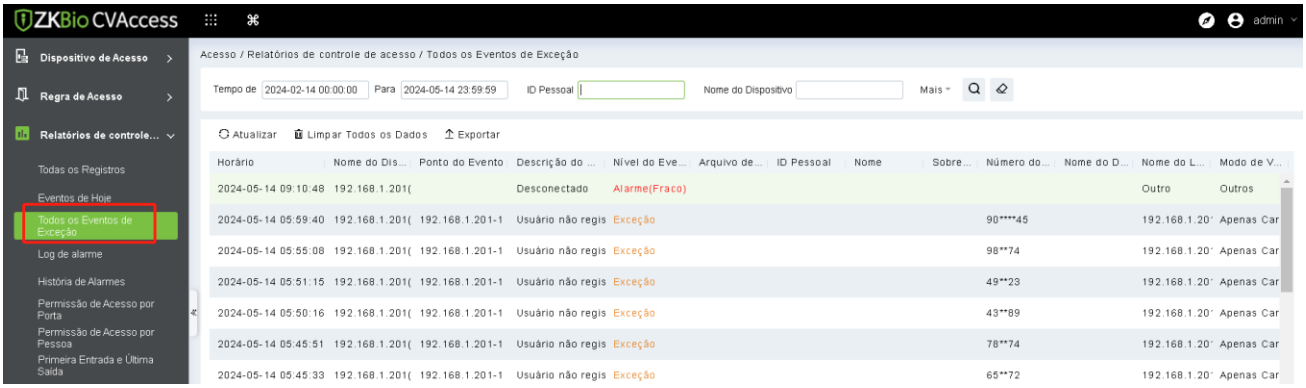
Time	Card Number	Personnel ID	First Name	Last Name	Department Name	Device Name	Event Point	Event Description	Reader Name	Verification Mode	Area Name	Remark
2017-12-15 18:29:02	4628036	6	Amber	Lin	Financial Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:59	4628036	6	Amber	Lin	Financial Department	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:45	13260079	5	Neool	Ye	Marketing Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:41	13260079	5	Neool	Ye	Marketing Department	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:38	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:35	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:23	1411237	2940	Sherry	Yang	Hotel	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:20	1411237	2940	Sherry	Yang	Hotel	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:17	9505930	9	Lilian	Mei	Development Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:13	9505930	9	Lilian	Mei	Development Department	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:28:06	13271770	3	Leo	Hou	Financial Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:28:01	13271770	3	Leo	Hou	Financial Department	192.168.218.60	192.168.218.60-1	Background Verify Success	192.168.218.60-1-In	Only Card	Area Name	
2017-12-15 18:23:52	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:23:16	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:23:12	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:23:02	6155266	2	Lucky	Tan	Development Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:22:21	4461253	1	Jerry	Wang	General	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	
2017-12-15 18:20:24	9505930	9	Lilian	Mei	Development Department	192.168.218.60	192.168.218.60-2	Background Verify Success	192.168.218.60-2-In	Only Card	Area Name	

Created on: 2017-12-15 18:36:55

1/30

4.3.3 Todos os Eventos de Exceção

Clique em **[Relatórios]** > **[Todos os Eventos de Exceção]** para visualizar eventos de exceção em condição especificada. As opções são as mesmas de [Todas as Transações].



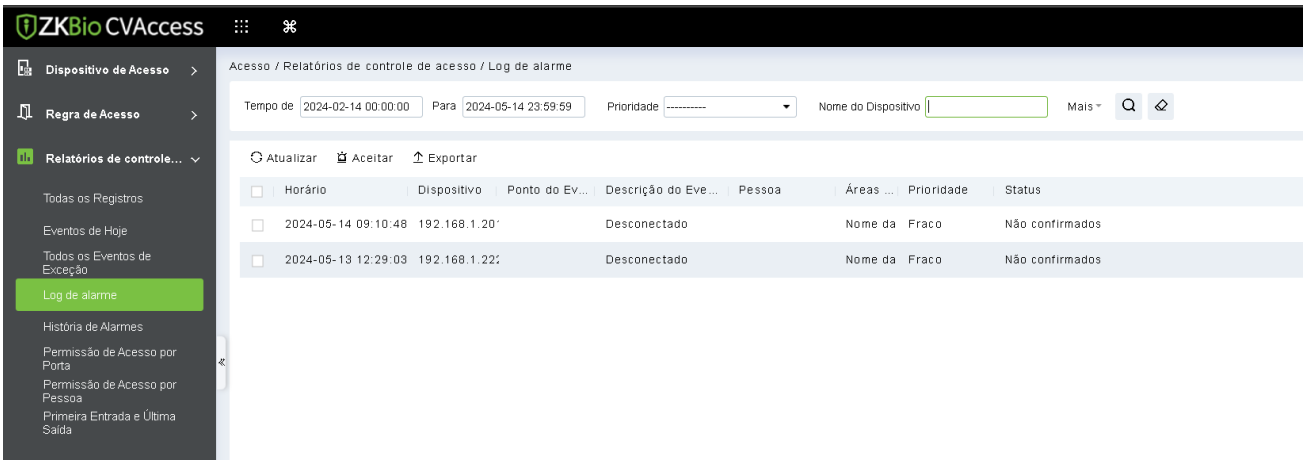
- **Limpar Todos os Dados:** Clique em [Limpar Todos os Dados] para abrir um prompt e, em seguida, clique em [OK] para limpar todos os eventos de exceção.
- **Exportar:** Você pode exportar todos os eventos de exceção em formato Excel, PDF e CSV.

All Exception Events

Event ID	Time	Device Name	Event Point	Event Description	Personnel ID	First Name	Last Name	Card Number	Department Number	Department Name	Reader Name	Verification Mode	Area Name	Remark
-1	2018-12-27 19:15:48	SpeedFace-V5		Disconnected							Other	Other	Area Name	
-1	2018-12-27 17:57:30	192.168.213.99		Disconnected							Other	Other	Area Name	
-1	2018-12-27 17:25:29	192.168.213.99		Disconnected							Other	Other	Area Name	
-1	2018-12-26 18:45:08	SpeedFace-V5		Disconnected							Other	Other	Area Name	
1220	2018-12-26 18:16:58	SpeedFace-V5	SpeedFace-V5-1	Unregistered Personnel							SpeedFace-V5-1-Out	Face	Area Name	
1218	2018-12-26 18:16:52	SpeedFace-V5	SpeedFace-V5-1	Unregistered Personnel							SpeedFace-V5-1-Out	Face	Area Name	
1215	2018-12-26 18:15:19	SpeedFace-V5	SpeedFace-V5-1	Unregistered Personnel							SpeedFace-V5-1-Out	Face	Area Name	
1214	2018-12-26 18:14:40	SpeedFace-V5	SpeedFace-V5-1	Unregistered Personnel							SpeedFace-V5-1-Out	Face	Area Name	
1213	2018-12-26 18:14:27	SpeedFace-V5	SpeedFace-V5-1	Unregistered Personnel							SpeedFace-V5-1-Out	Face	Area Name	
1212	2018-12-26 18:12:48	SpeedFace-V5	SpeedFace-V5-1	Unregistered Personnel							SpeedFace-V5-1-Out	Face	Area Name	
1211	2018-12-26 18:11:12	SpeedFace-V5	SpeedFace-V5-1	Unregistered Personnel							SpeedFace-V5-1-Out	Face	Area Name	
1210	2018-12-26 18:10:46	SpeedFace-V5	SpeedFace-V5-1	Unregistered Personnel							SpeedFace-V5-1-Out	Face	Area Name	
1209	2018-12-26 18:10:42	SpeedFace-V5	SpeedFace-V5-1	Unregistered Personnel							SpeedFace-V5-1-Out	Face	Area Name	
1208	2018-12-26 18:10:38	SpeedFace-V5	SpeedFace-V5-1	Unregistered Personnel							SpeedFace-V5-1-Out	Face	Area Name	

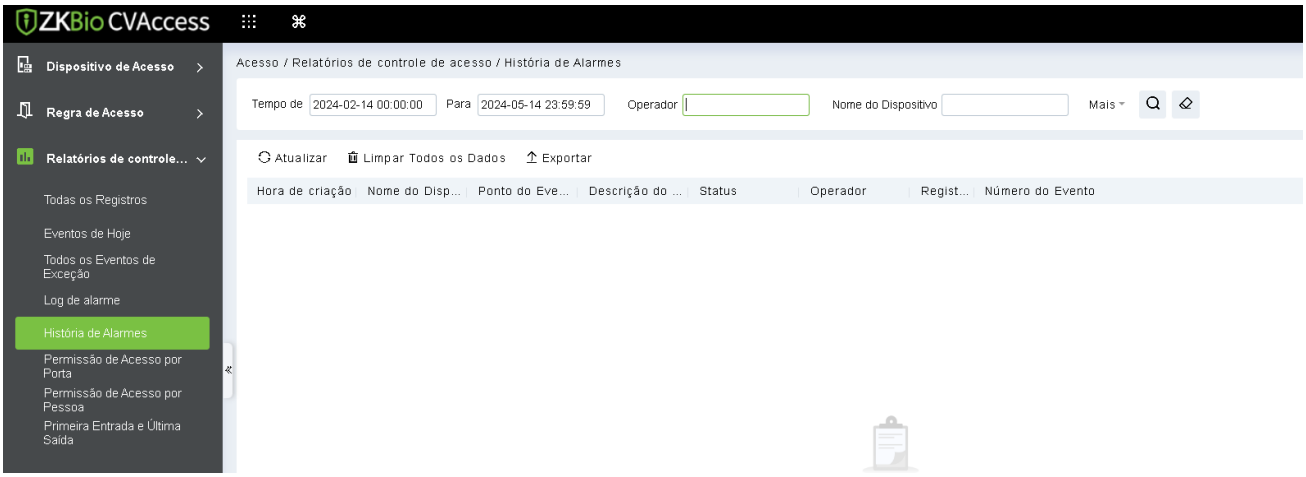
4.3.4 Registro de Alarme

Clique **em [Relatórios] > [Registro de Alarme]** para visualizar declarações históricas no Monitoramento de Alarme.



4.3.5 Histórico de Processamento de Alarme

Clique **em [Relatórios] > [Histórico de Processamento de Alarme]** para visualizar relatórios de registros de processamento no Monitoramento de Alarme.



4.3.6 Direitos de Acesso por Porta

Visualize os níveis de acesso relacionados pela porta. Clique em **[Relatórios] > [Direitos de Acesso por Porta]**, a lista de dados no lado esquerdo mostra todas as portas no sistema, selecione uma porta, e as pessoas com níveis de acesso à porta serão exibidas na lista de dados do lado direito.

Você pode exportar todos os dados das pessoas com níveis de acesso à porta em formato Excel, PDF e CSV.

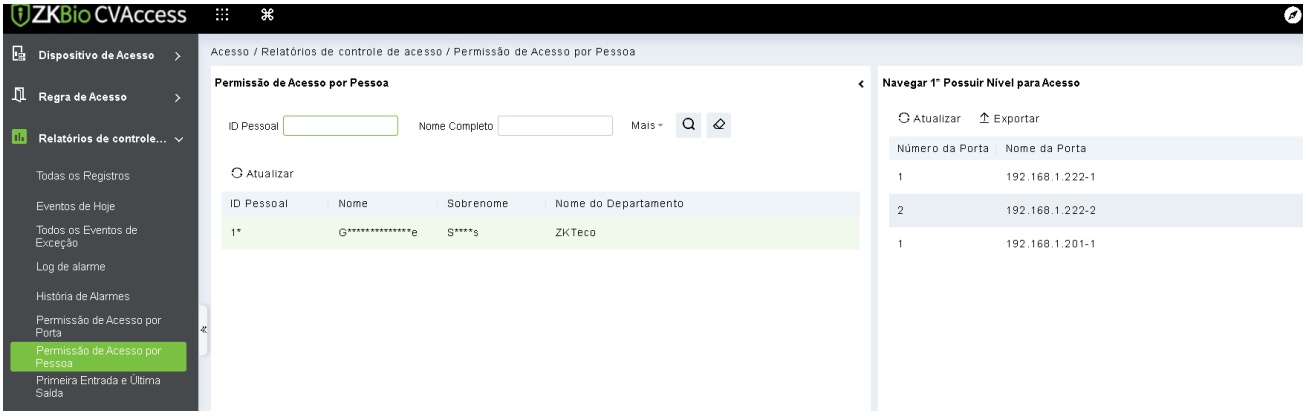
Personnel

Personnel ID	First Name	Last Name	Department Name
575	Jeff		ZKTeco
1	abc	xyz	Marketing Department
2	abc1	xyz1	Development Department
343	example		Financial Department
432	ex		Marketing Department

4.3.7 Direitos de Acesso por Pessoa

Visualize os níveis de acesso relacionados pela pessoa.

Clique em **[Relatórios] > [Direitos de Acesso por Pessoa],** a lista de dados no lado esquerdo mostra todas as portas no sistema, selecione uma pessoa, e as pessoas com níveis de acesso à porta serão exibidas na lista de dados do lado direito.



Você pode exportar todas as informações da porta em formato Excel, PDF e CSV.

Door

Door Number	Door Name
1	SpeedFace-V5-1
1	192.168.213.99-1
2	192.168.213.99-2

4.3.8 Primeiro a Entrar e Último a Sair

Clique **em [Relatórios] > [Primeiro a Entrar e Último a Sair]** para visualizar relatório de primeira entrada e última saída, usado para filtrar rapidamente a primeira entrada e última saída do dia.

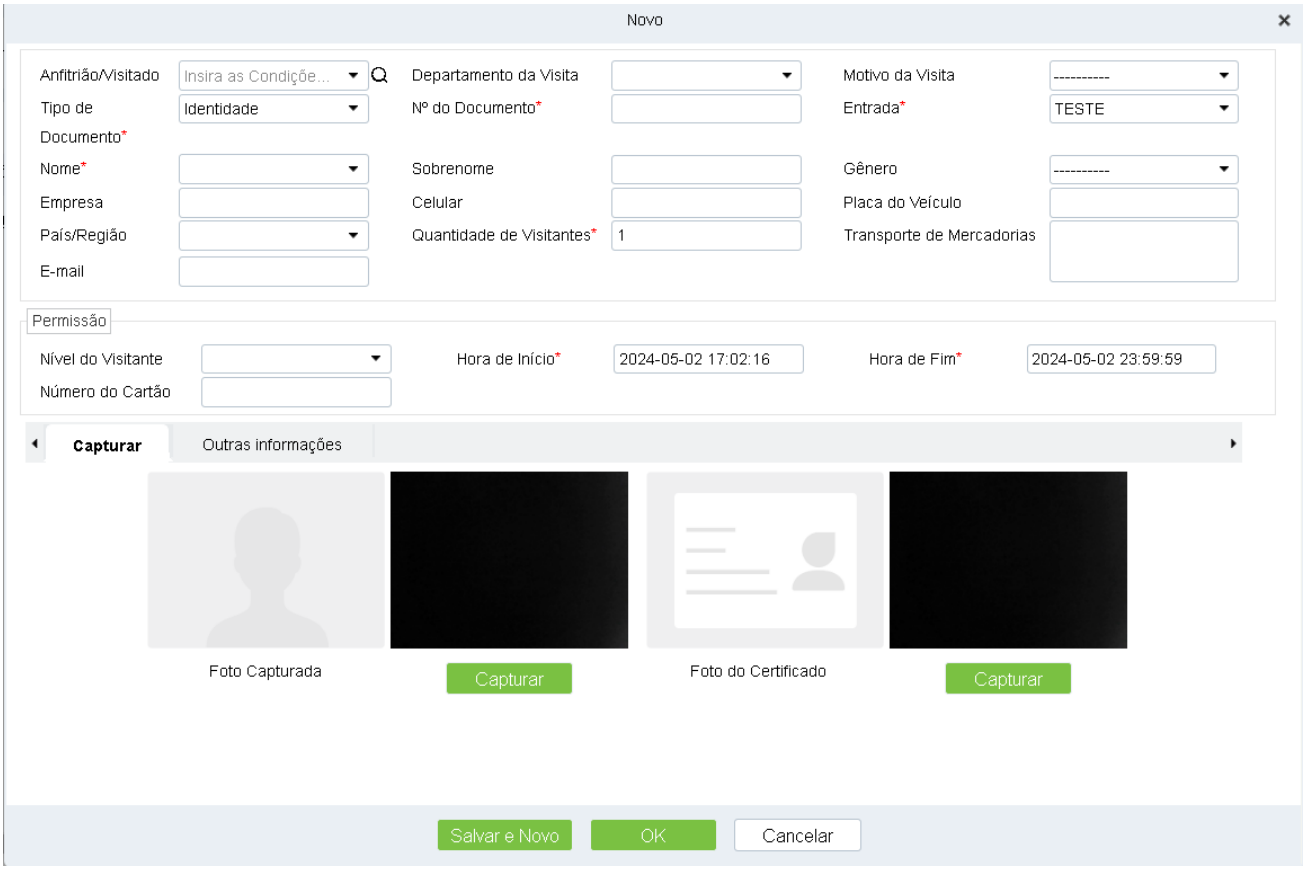
5 Gerenciamento de Visitantes

5.1 Registro de Visitantes

5.1.1 Registro de Entrada

Clique em **Registro de Visitante > Registro de Entrada > Registro de Entrada.**

Através da aba abaixo, você poderá realizar o check-in de novos visitantes e também reutilizar os cadastros de visitantes anteriores. Basta informar o tipo de documento e o número correspondente para concluir o processo de registro.



➢ Informações básicas

- **Anfitrião/Visitado:** Anfitrião a ser visitado.(Quem vai receber a visita)
- **Departamento da Visita:** Departamento que a visita irá visitar (Quando o anfitrião é selecionado esse campo é preenchido automáticamente).
- **Motivo da Visita:** Motivo que justifica a visita da pessoa.
- **Tipo de Documento:** O documento que vai ser utilizado como identificador do visitante.
- **N° do Documento:** O número do documento selecionado
- **Entrada:** Por qual portaria está sendo feito o check-in
- **Nome:** Nome do visitante
- **Sobrenome:** Sobrenome do Visitante
- **Gênero:** Gênero do Visitante
- **Empresa:** Empresa do Visitante
- **Celular:** Celular do Visitante
- **Placa do Veículo:** Placa do Veículo do Visitante
- **Pais/Região:** Nacionalidade do Visitante
- **Quantidade de Visitantes:** Quantidade de pessoas na visita
- **Trasporte de Mercadorias:** Informar se o visitante possui alguma mercadoria.

➢ Permissão

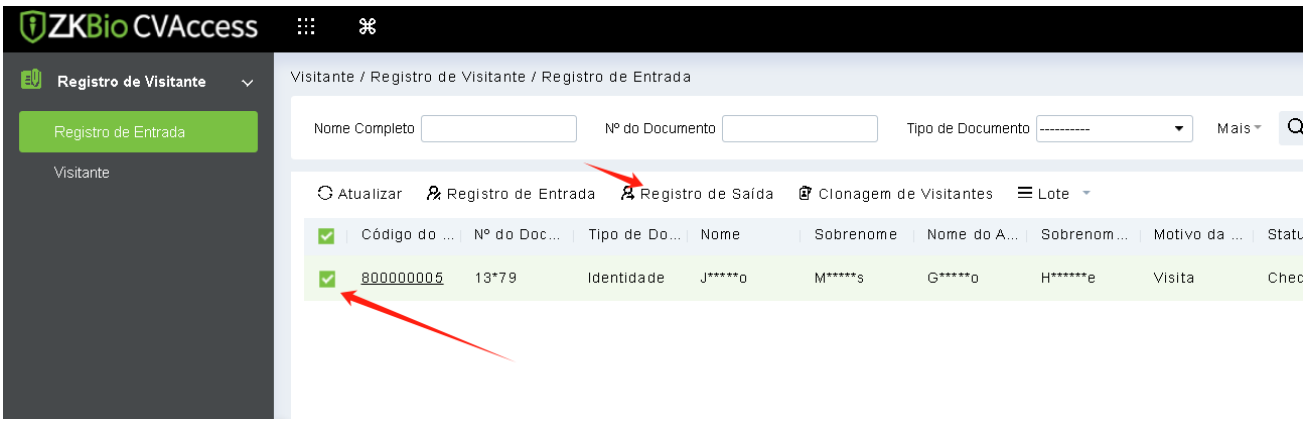
- **Nível do Visitante:** Definir o nivel de acesso do visitante
- **Hora de Início:** Hórario de inicio da visita

- **Hora de Fim:** Hórario fim da visita.
- **Número do Cartão:** Número do cartão/qrcode da visita.

5.1.1.1 Registro de Saída

Clique em **Registro de Visitante > Registro de Entrada > Registro de Saída**

Através da aba abaixo, você pode realizar o check-out manual de um visitante. Após o check-out, o visitante perderá o acesso ao local.



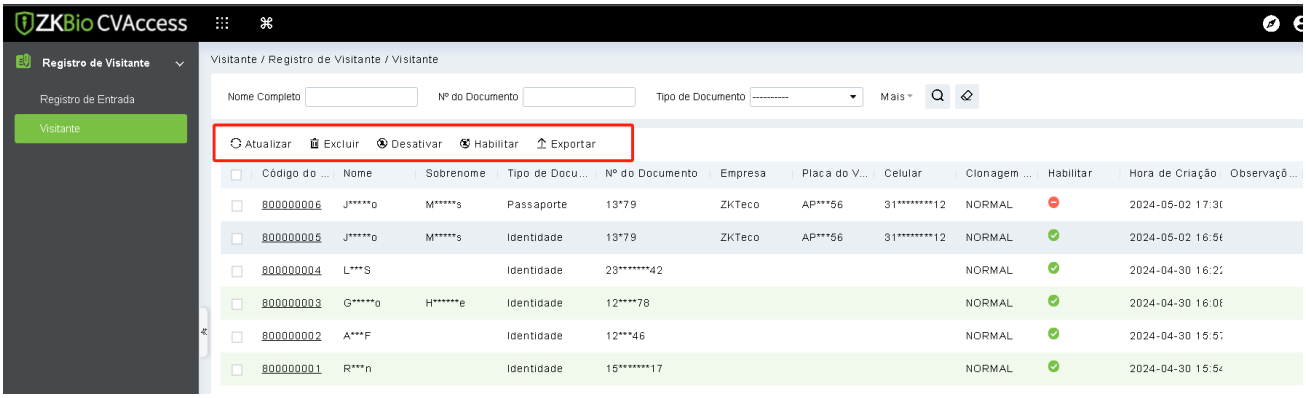
5.1.1.2 Clonagem de Visitantes

Para aproveitar dados de um registro selecionado, clique em **"Registro de Visitante" > "Registro de Entrada" > "Clonagem de Visitantes"**. Esse botão permite copiar informações específicas do registro, como Anfitrião/Visitado, Departamento de Visita, Motivo da Visita, Tipo de Documento, Horário de Entrada e Saída, Empresa, País/Região, Nível de Acesso e Horário de Início e Fim.

5.1.2 Visitante

Clique em **Registro de Visitante > Registro de Entrada > Visitante.**

Através desta aba, é possível visualizar todos os visitantes que foram registrados no sistema.

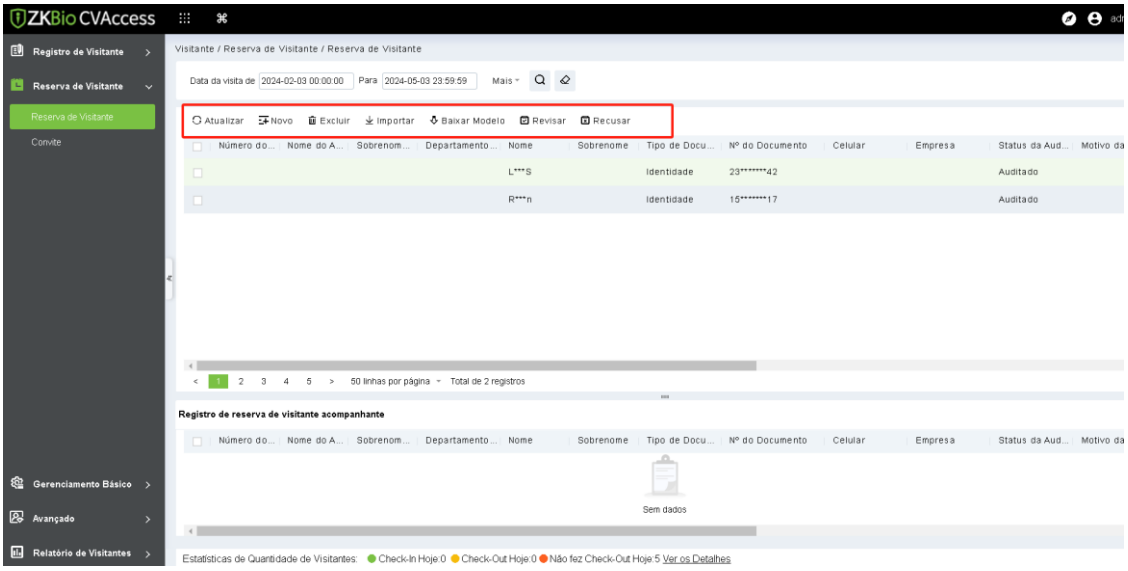


- **Excluir:** Remove o visitante do sistema.
- **Desativar/Habilitar:** Permite desativar um visitante. Quando desativado, não é possível realizar o check-in do visitante.
- **Exportar:** Permite exportar uma lista com as informações dos visitantes.

5.2 Reserva de Visitantes

5.2.1 Reserva de Visitantes

Ao acessar a seção "**Reserva de Visitante**" e clicar em "**Reserva de Visitante**", você terá acesso a uma aba que facilita a gestão das reservas feitas por visitantes, seja por meio de formulários web ou diretamente nessa aba. Aqui, você pode criar novas reservas, além de aprovar ou reprovar as reservas existentes.

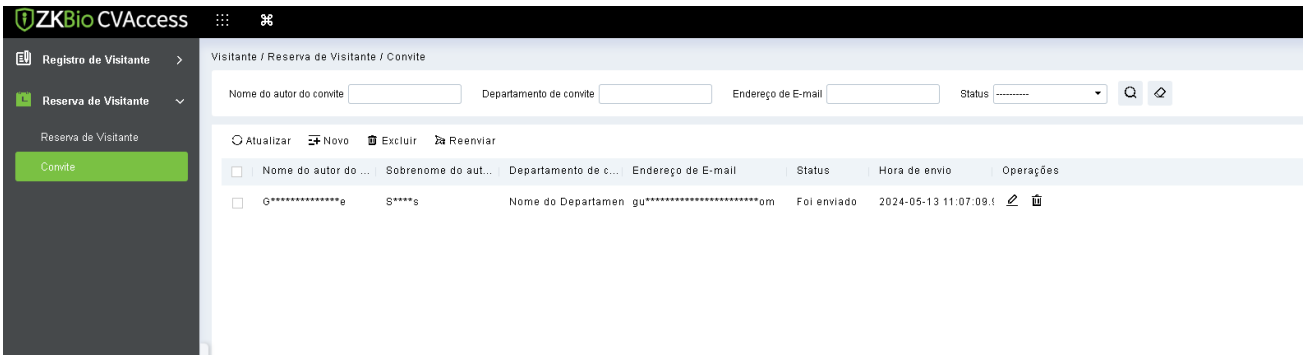


- **Novo:** Realiza a reserva de uma nova visita.
- **Excluir:** Remove uma reserva do sistema.
- **Importar:** Permite importar uma planilha exel preenchida com os dados das reservas.
- **Baixar Modelo:** Permite baixar o modelo da planilha exel.

- **Revisar:** Aprovação da reserva. Após aprovado todos os dados da reserva poderão ser reaproveitados no momento do check-in.
- **Recusar:** Reprovação da reserva.Após reprovado os dados da reserva não serão utilizados no check-in do usuário. Sendo necessário preencher os campos no momento do check-in.

5.2.2 Convite

Ao acessar a seção "**Reserva de Visitante**" e clicar em "**Convite**", você terá acesso a uma aba para enviar convites para os visitantes. Através desse convite os visitates poderão preencher um formulário para realizar a reserca das visitas.

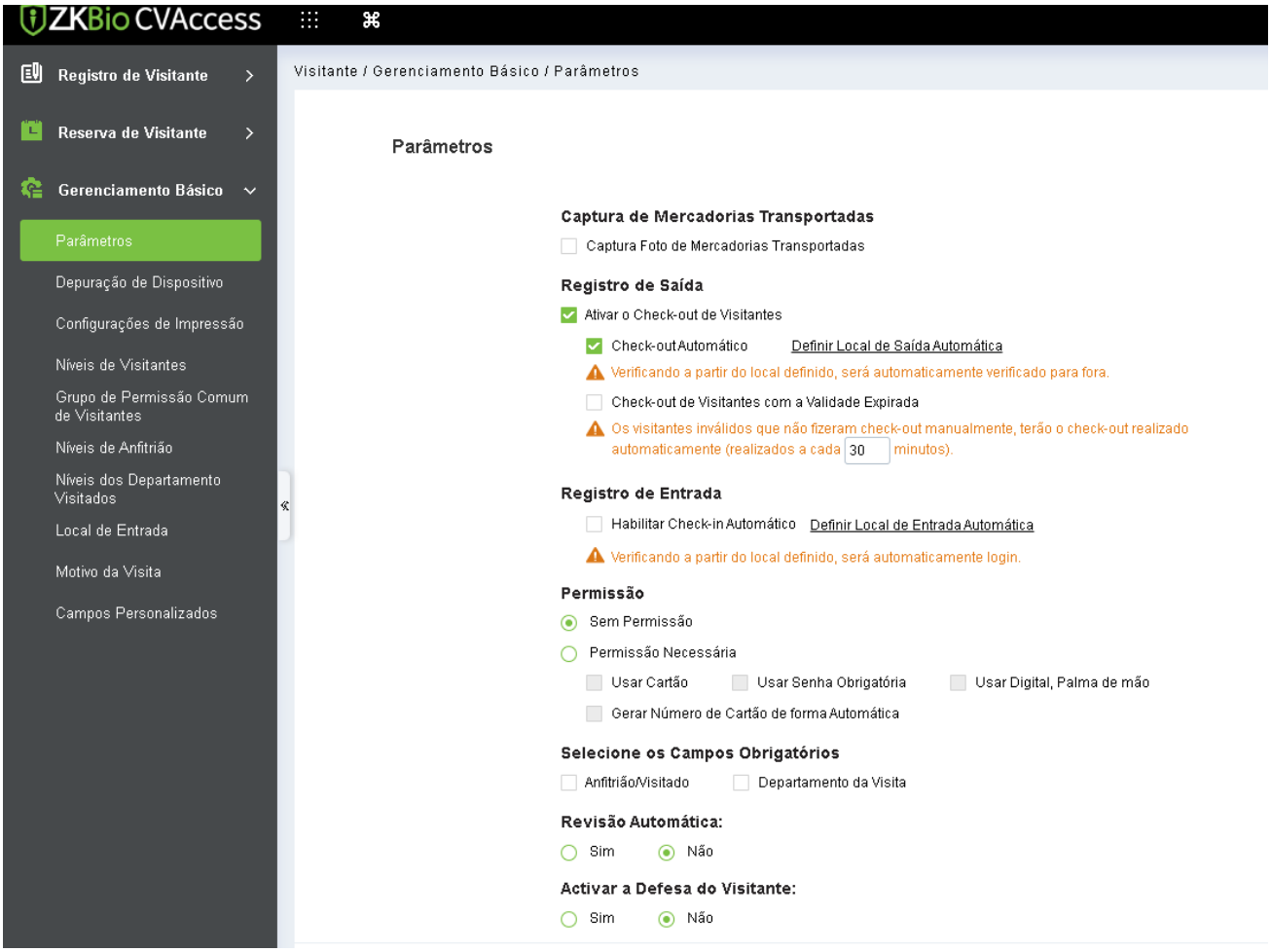


- **Novo:** Enviar um novo convite de reserva.
- **Excluir:** Excluir um convite de reserva do sistema.
- **Reenviar:** Reenviar o convite de reserva para o e-mail do visitante.

5.3 Gerenciamento Básico

5.3.1 Parâmetros

Ao acessar a seção "**Gerenciamento Básico**" e clicar em "**Parâmetros**", você terá acesso a uma aba para realizar configurações de funcionamento do módulo de visitante. Com a opção de defirnir check-in e check-out automático de visitantes entre outras configurações.



➢ Captura de Mercadorias Transportada

- **Captura de Mercadorias Transportada:** Ao selecionar essa opção será adicionar um campo para captura de foto para mercadorias na aba de cadastro de visitantes

➢ Registro de Saída

- **Abrir a Função de Saída do Visitante:** Exibe as configurações de check-out.
- **Saída Automática:** Ao ser ativada, é necessário definir um dispositivo. Quando um visitante autenticar nesse dispositivo, seu status será automaticamente alterado para check-out, e ele não poderá mais acessar o local.
- **Finalizar Sessão de Visitantes Expirados:** Ao ser ativada, uma rotina será acionada a cada 30 minutos. Todos os visitantes com status de check-out tardio, ou seja, com validade expirada, terão seu status alterado para check-out e perderão o acesso ao local.

➢ Registro de Entrada:

- **Habilitar Entrada Automática:** Ao ativar esta opção, é necessário configurar um dispositivo específico. Quando um visitante fizer uma reserva, ele será automaticamente direcionado para o dispositivo definido. Ao autenticar-se neste equipamento, o check-in dele será automaticamente registrado no sistema.

➢ Permissão

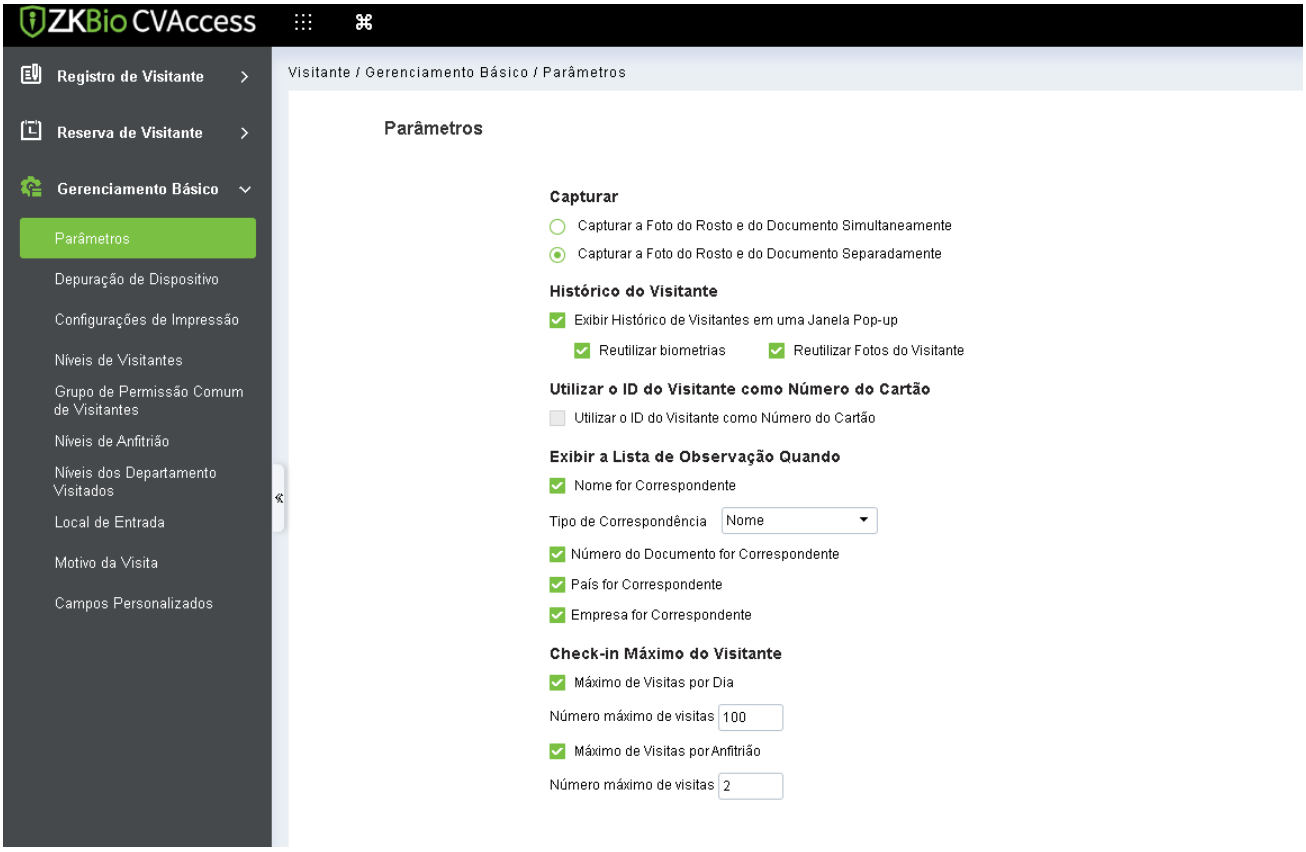
- **Emitir Cartão:** Ao ser selecionado é adicionado um campo de cartão no registro de visitantes.
- **Senha Obrigatória:** Ao ser selecionado é adicionado um campo de senha no registro de visitantes.
- **Modelo biológico:** Ao ser selecionado é adicionado a possibilidade de cadastro de digitais e palma da mão no registro de visitantes.
- **Código de Leitura:** Ao ser selecionado é adicionado um campo de cartão preenchido automaticamente no registro de visitantes.

➢ Selecione o Campo Obrigatório

- **Anfitrição/Visitado:** Ao ser selecionado o campo anfitrição passa ser obrigátorio.
- **Departamento da Visita:** Ao ser selecionado o campo departamento visitado passa ser obrigátorio.

➢ Ativar revisão automática de compromissos de convidados

- **Sim:** Ao ser selecionado os cadastro de reserva de visitantes via formulário são aprovados automáticamente.
- **Não:** Ao ser selecionado os cadastro de reserva de visitantes via formulário precisam ser aprovados manualmente.



➢ Capturar

- **Capturar a Foto e a Foto do Certificado Juntas:** Ao ser selecionado a foto do rosto do visitante e a foto do documento são tiradas com um clique no mesmo botão.
- **Capturar a Foto e a Foto do Certificado Separadamente:** Ao ser selecionado a foto do rosto do visitante e a foto do documento são tiradas separamente.

➢ Informações de Histórico do Visitante

- **Abra a Caixa Pop-up Para Exibir Informações do Histórico de Visitantes:** Ao ser selecionado, ao fazer o check-in de um visitante que já visitou o local será aberto uma aba com o hístorico de visitas possibilitando reutilizar alguns dados.
- **Modelo de biografia do visitante de preenchimento:** Ao ser selecionada, a biometria da última visita do visitante é reutilizada em novos cadastros.
- **Substituição da Foto do Visitante:** Ao ser selecionada, a foto da última visita do visitante é reaproveitada em novos cadastros.

➢ Copiar o Número do ID como o Número do Cartão Automaticamente

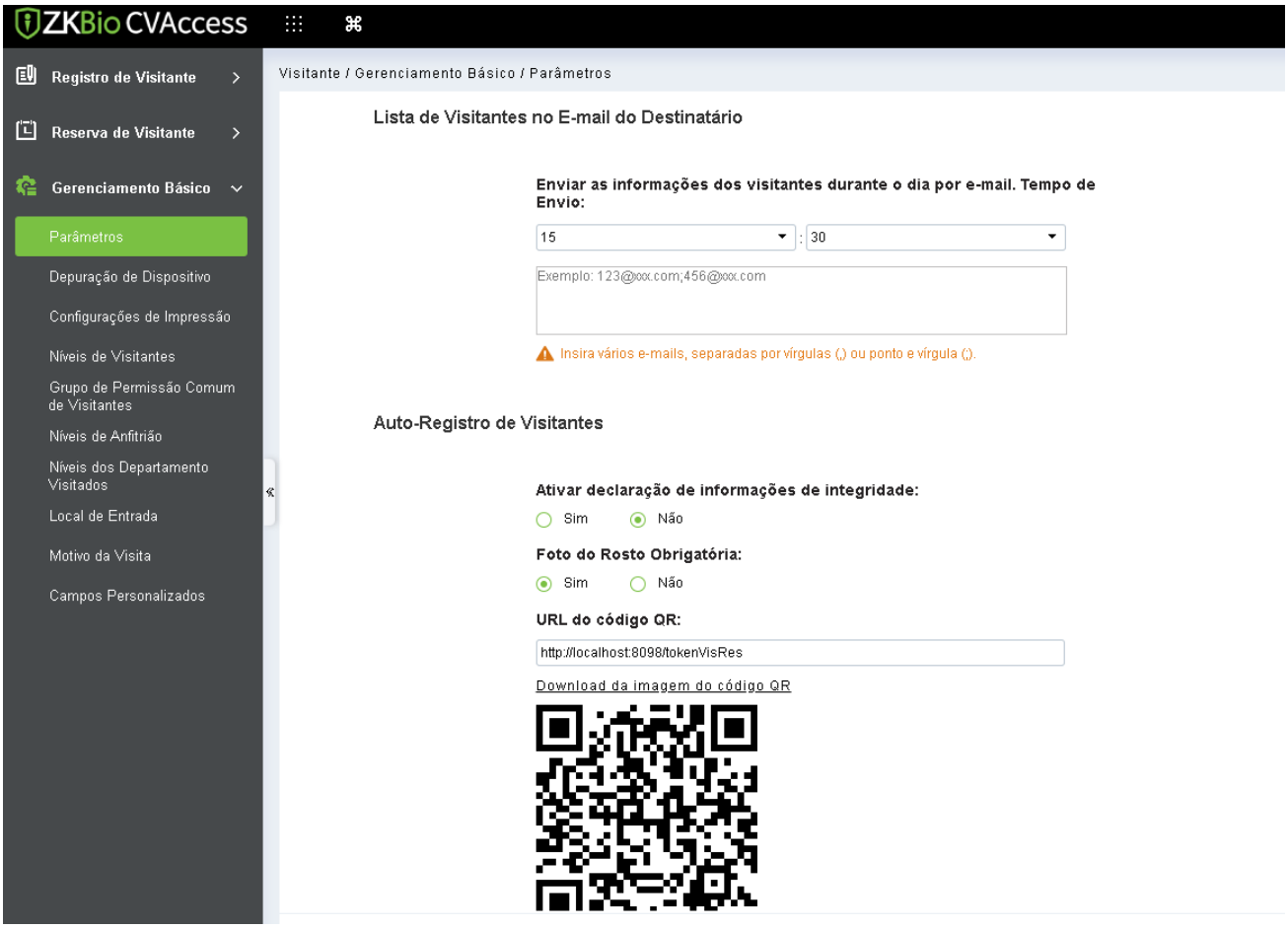
- **Copiar número do ID como Número do Cartão:** Ao ser selecionado, o ID do visitante será utilizado como número de cartão.

➢ Opção WatchList

- **No prompt de Entrada se o Nome for Correspondente:**Ao ser selecioando, caso o nome do visitante esteja na lista de observação as informações da lista serão exibidas.
- **Entrada Correspondente por Certificado:** Ao ser selecioando, caso o número do documento do visitante esteja na lista de observação as informações da lista serão exibidas.
- **Entrada Correspondente por País:** Ao ser selecioando, caso o país do visitante esteja na lista de observação as informações da lista serão exibidas.
- **Entrada Correspondente por Empresa:** Ao ser selecioando, caso a empresa do visitante esteja na lista de observação as informações da lista serão exibidas.

➢ Check-in máximo do visitante

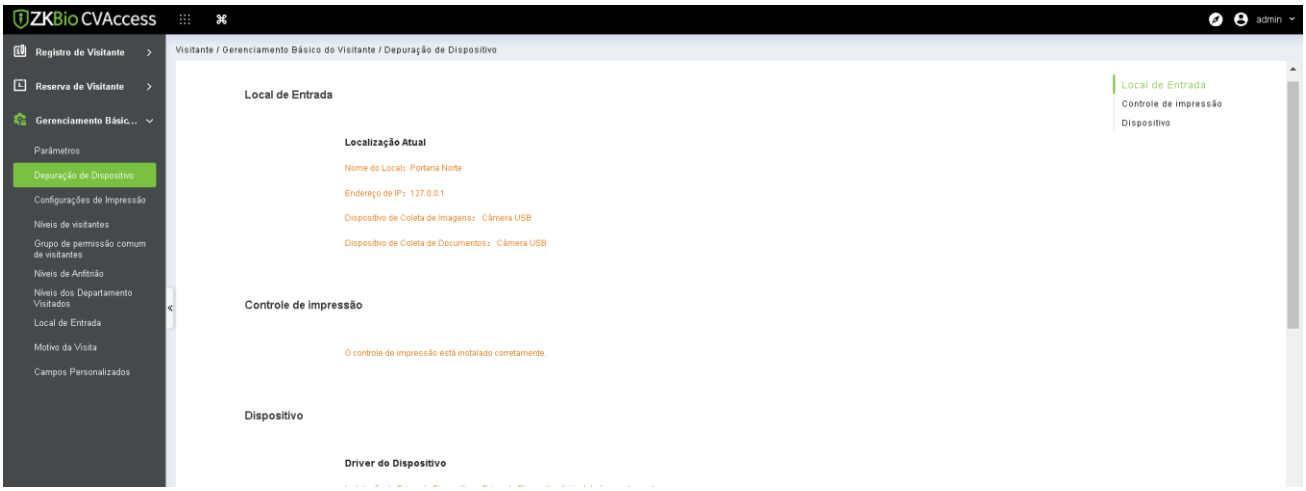
- **Monitoramento de abertura máxima de visitas do visitante em um único dia Número máximo de visitas:** Você pode definir a quantidade máxima de visitas por dia.
- **Monitoramento de abertura máxima de visitas do visitante único em um único dia Número máximo de visitas:** Você pode definir a quantidade máximas de visitas que um anfitrião pode receber no dia.



- **Lista de Visitantes no E-mail do Destinatário**
  - **Enviar as informações dos visitantes durante o dia por e-mail. Tempo de Envio:** Você pode definir um hórario que que seja encaminhado um e-mail com as informações dos visitantes.
- **Auto-registro de visitantes**
  - **Ativar declaração de informações de integridade**: Ao ser selecionado, antes do visitantes iniciar o cadastro via formulário ele deve responder a uma declaração de integridade.
  - **Enviar fotografias faciais:** Ao ser selecionado, o campo foto passa ser obrigatório no cadastro de visitantes via formulário.
  - **URL do código QR:** Deve ser preenchido com o endereço do servidor. Será utilizado para que os visitantes consigam acessar o formulário de cadastro.

5.3.2 Depuração de Dispositivo

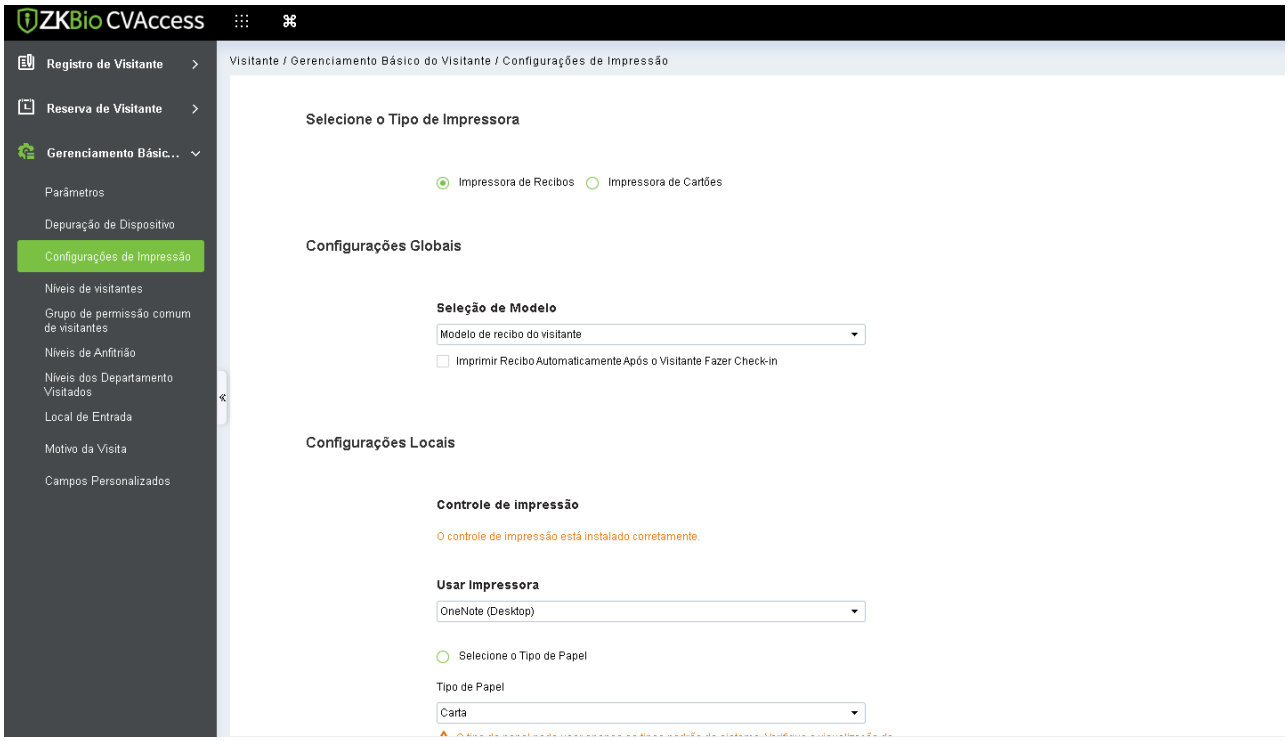
Ao acessar a seção "**Gerenciamento Básico**" e clicar em "**Depuração de Dispositivo**", você terá acesso a uma aba para visualizar as informações de identifiação da máquina e de testes de dispositivos expernos como as câmeras USB.



- **Local de Entrada:** Apresenta algumas informações da máquina servidor.
- **Controle de Impressão**: Verifica se o drive de impressão já foi instalado.
- **Dispositivo:** As opções disponíveis são utilizadas para testar e calibrar os equipamentos ligados ao computador.

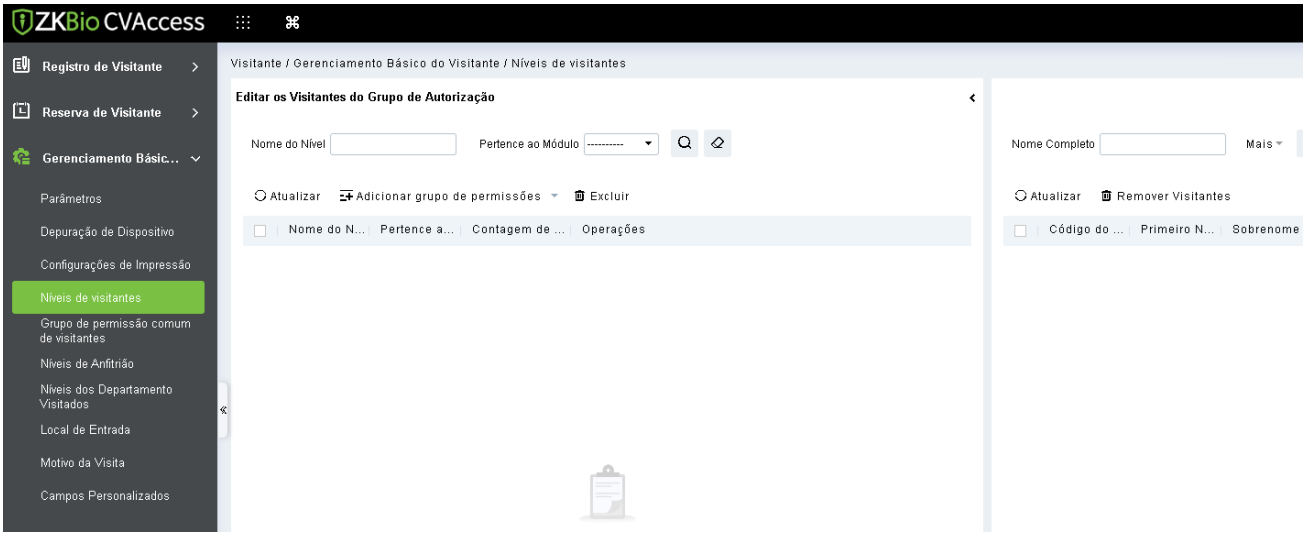
5.3.3 Configuração de Impressão

Ao acessar a seção "**Gerenciamento Básico**" e clicar em "**Configuração de Impressão**", você terá acesso a uma aba para realizar as configurações da impressão de cartões e recibos dos visitantes.



5.3.4 Níveis de Visitantes

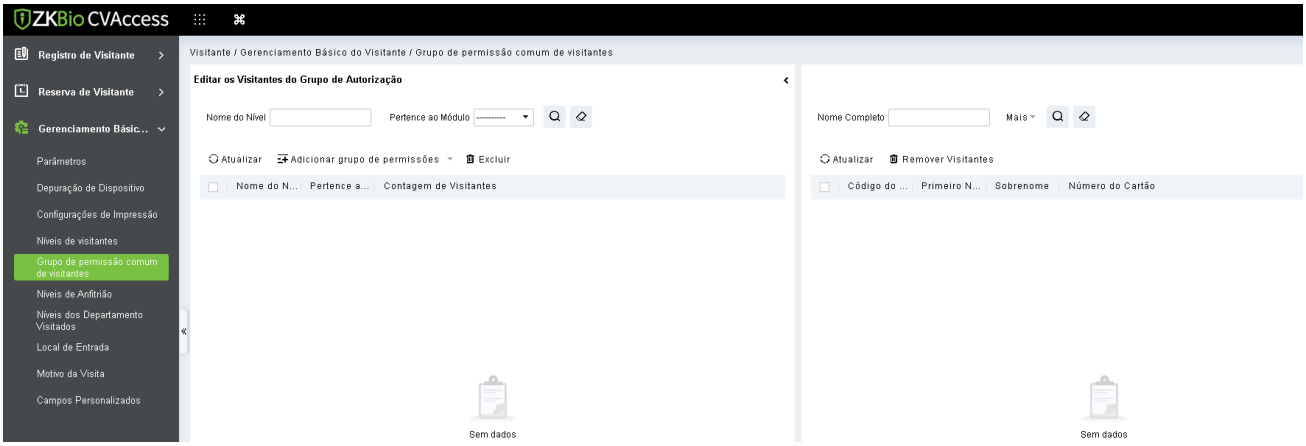
Ao acessar a seção "**Gerenciamento Básico**" e clicar em "**Nível de Visitantes**", você terá acesso a uma aba para definir quias são os níveis de acesso que podem ser utilizado para visitas.



- **Adicionar grupo de permissão:** Ao clicar nesta opção, você poderá definir os níveis de acesso que os visitantes poderão utilizar. É importante notar que esses níveis de acesso disponíveis para seleção são aqueles que foram previamente criados no módulo de acesso.

5.3.5 Grupo de permissão comum de visitantes

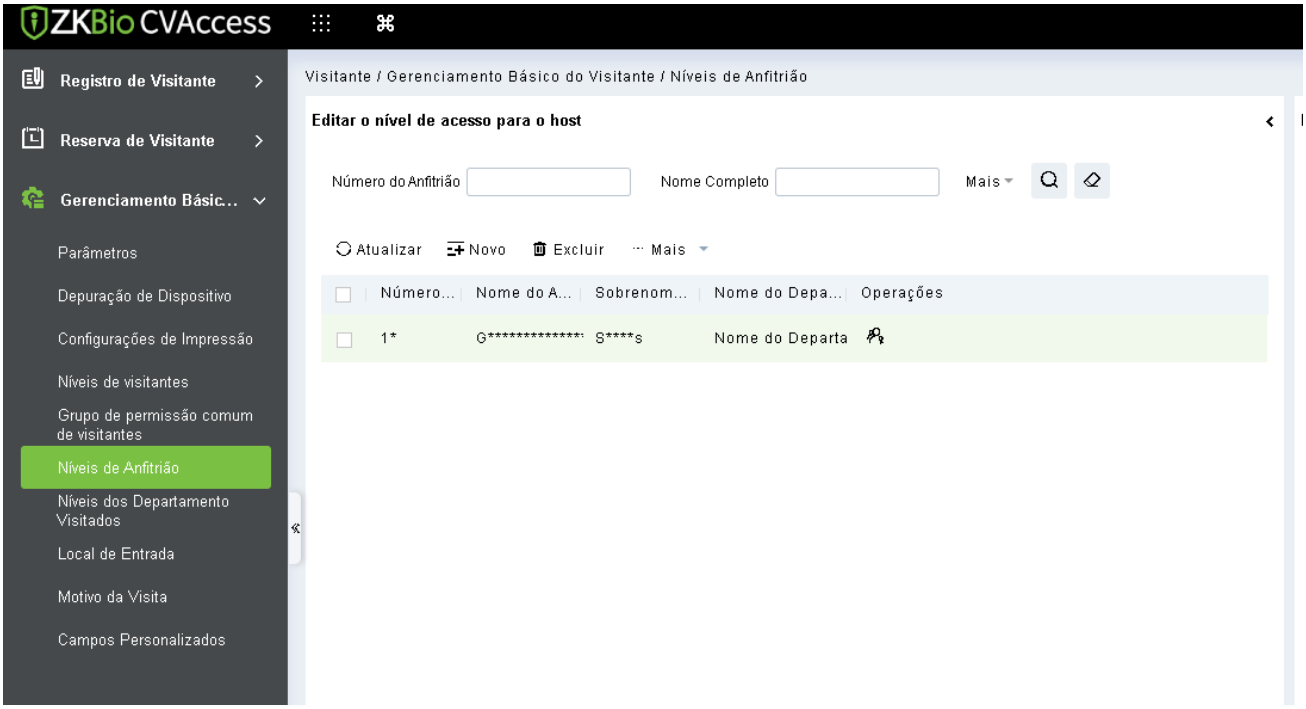
Ao acessar a seção "**Gerenciamento Básico**" e clicar em "**Grupo de permissão comum de visitantes**", você terá acesso a uma aba para definir os níveis de acesso padrões em qualquer visita.



- **Adicionar grupo de permissão:** Ao clicar nesta opção, você poderá configurar os níveis de acesso padrão para todas as visitas. Isso significa que todas as visitas terão automaticamente acesso nos níveis selecionados como padrão.

5.3.6 Nível de Anfitrião

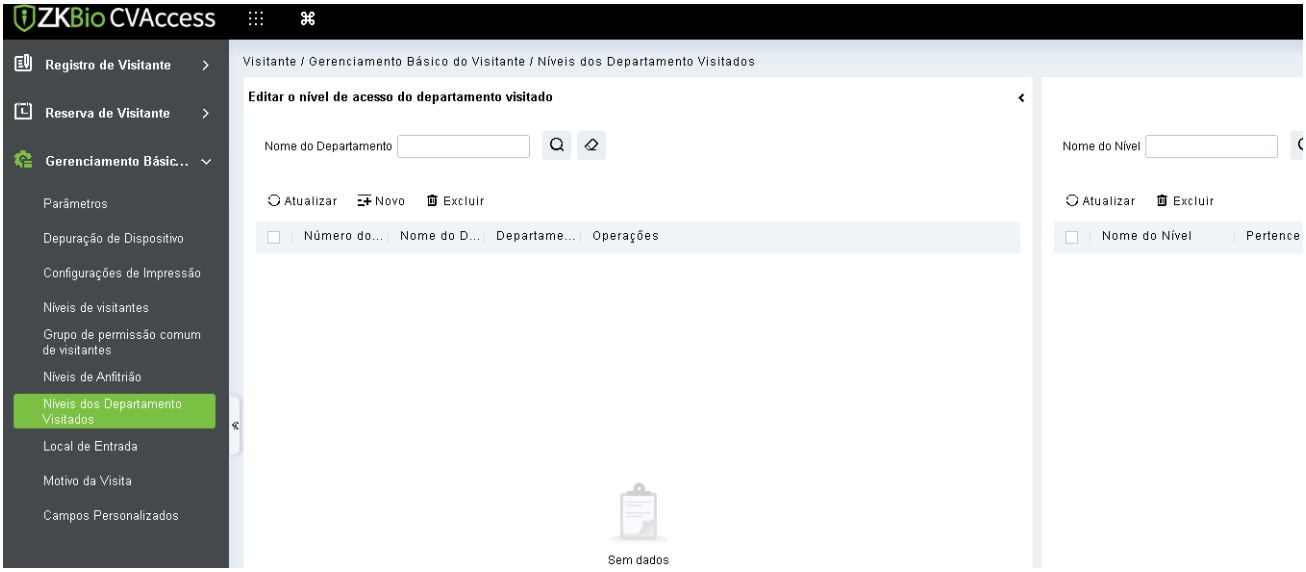
Ao acessar a seção "**Gerenciamento Básico**" e clicar em "**Nível de Anfitrião**", você terá acesso a uma aba para definir os níveis de acesso padrões por anfitrião.



- **Novo:** Ao clicar nesta opção, você poderá escolher um anfitrião ao qual deseja vincular níveis de acesso. Após essa seleção, todos os visitantes que visitarem esse anfitrião terão permissão para utilizar todos os níveis de acesso vinculados a ele.
- **Exluir:** Ao clicar nessa opção você vai excluir a vinculação do anfitrião com os níveis de acesso.

5.3.7 Níveis dos Departamentos Visitados

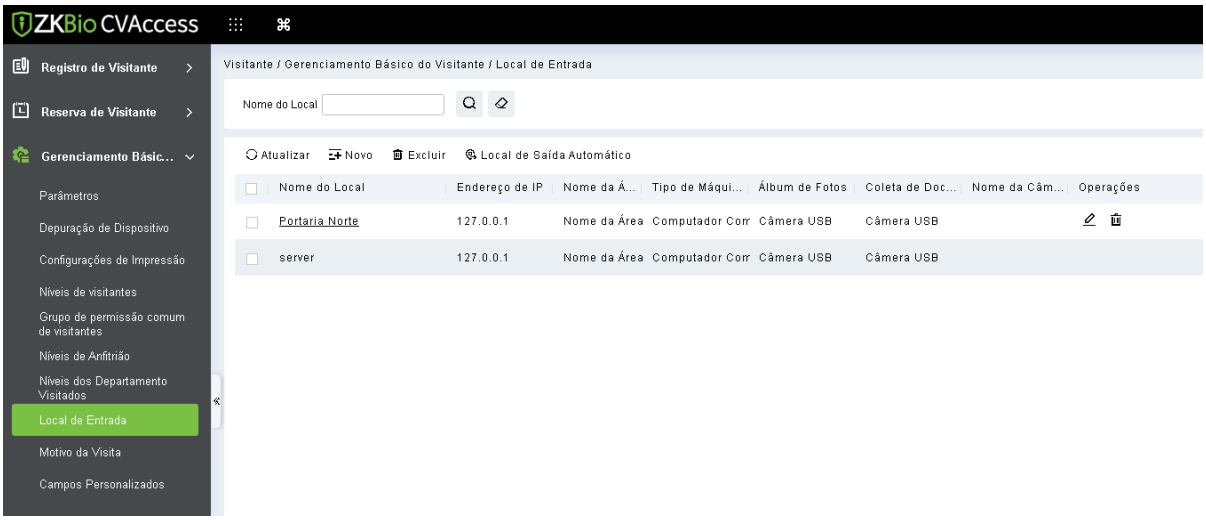
Ao acessar a seção "**Gerenciamento Básico**" e clicar em **"Nível dos departamentos visitados**", você terá acesso a uma aba para definir os níveis de acesso padrões por departamento visitado.



- **Novo:** Ao clicar nesta opção, você poderá estabelecer uma ligação entre os departamentos visitados e os níveis de acesso. Dessa forma, os visitantes que forem visitar um departamento terão acesso aos níveis vinculados a ele.
- **Exluir:** Ao clicar nessa opção você vai excluir a vinculação do departamento com os níveis de acesso.

5.3.8 Local de Entrada

Ao acessar a seção "**Gerenciamento Básico**" e clicar em "**Local de Entrada**", você terá acesso a uma aba para definir os pontos de entrada dos visitantes.

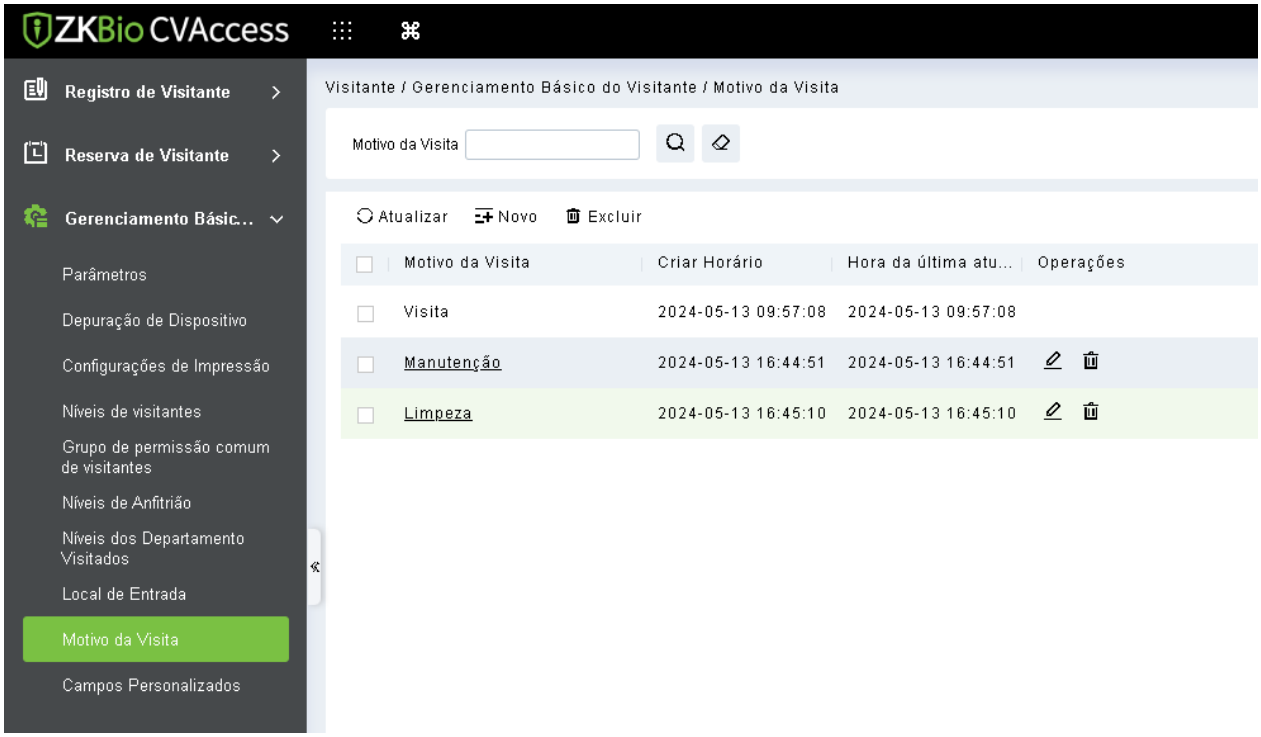


- **Novo:** Ao clicar nesta opção, você poderá criar um novo ponto de cadastro de visitantes. Cada computador consome 1 ponto de registro da licença.
- **Excluir:** Ao clicar nesta opção, você poderá exluir um ponto de cadastro de visitantes.

- **Local de Saída:** Ao clicar nesta opção, você poderá configurar um ponto de saída automática. Quando um visitante se autenticar em um dispositivo configurado para saída automática, ele receberá um check-out automático e não terá mais acesso ao local.

5.3.9 Motivo da Visita

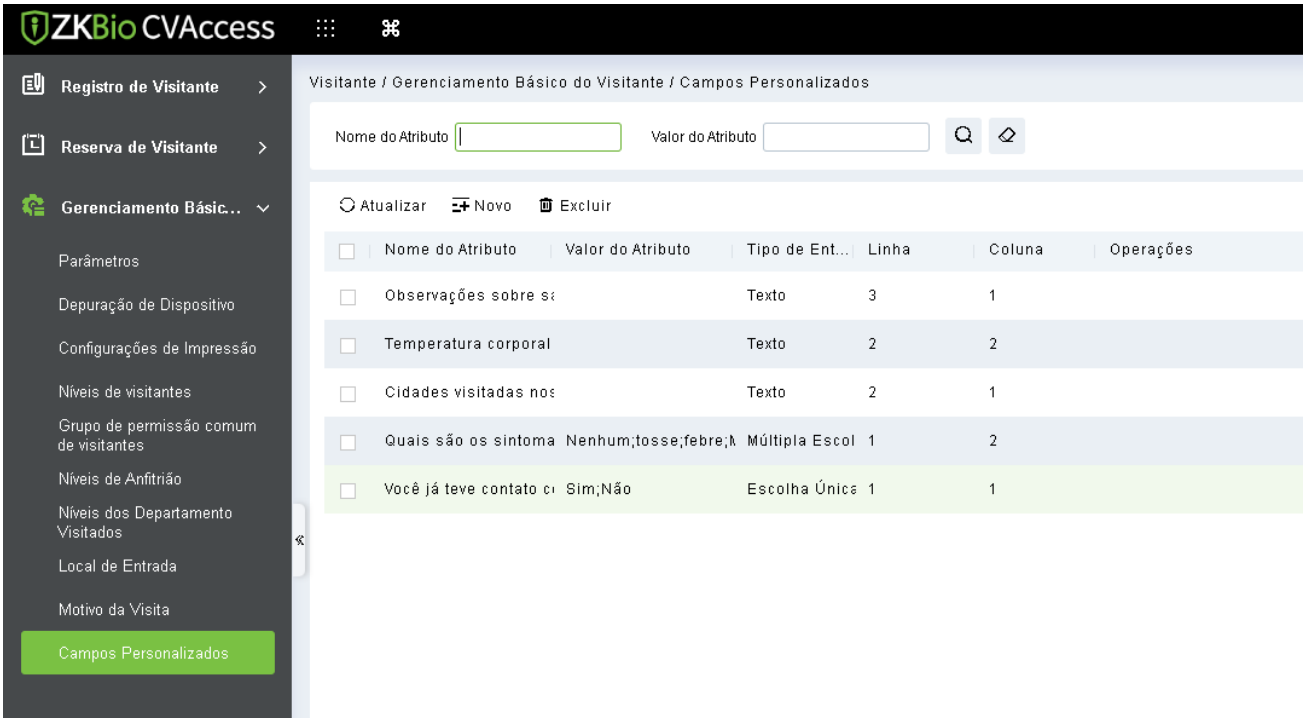
Ao acessar a seção "**Gerenciamento Básico**" e clicar em "**Motivo da Visita**", você terá acesso a uma aba para definir os motivo da visita que vão ser utilizados no check-in dos visitantes.



- **Novo:** Ao clicar nesta opção, você poderá criar um novo motivo de visita para ser usado no check-in dos visitantes.
- **Excluir:** Ao clicar nesta opção, você poderá exluir um motivo de visita.

5.3.10 Campos Personalizados

Ao acessar a seção "**Gerenciamento Básico**" e clicar em "**Campo Personalizados**", você terá acesso a uma aba para criar novos campos para que seja feito o check-in do visitante.

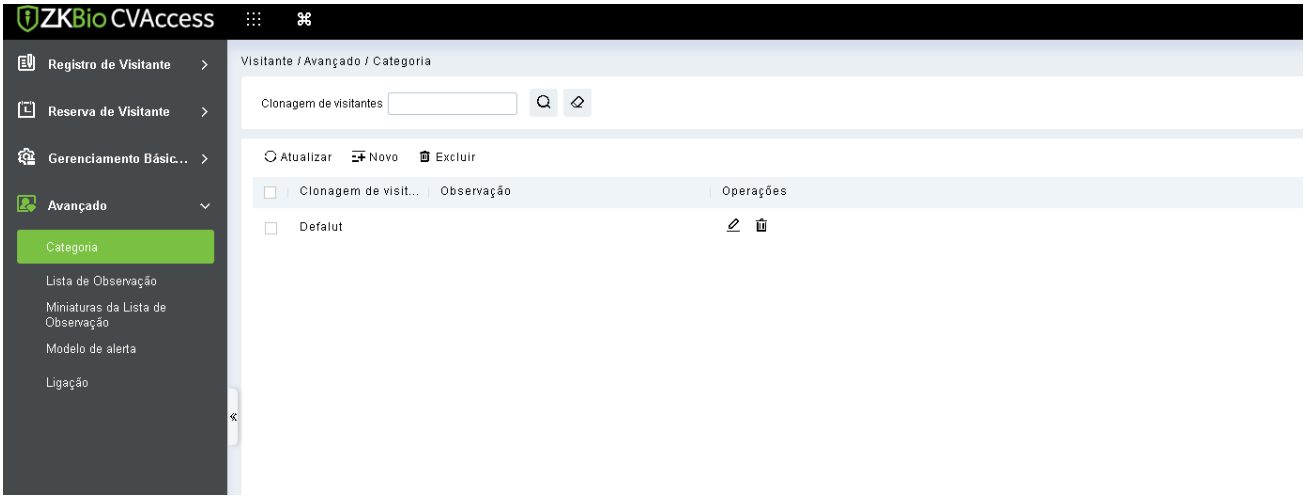


- **Novo:** Ao clicar nesta opção, você poderá criar um campo personalizado que poderá ser utilizado no check-in dos visitantes.
- **Excluir:** Ao clicar nesta opção, você poderá exluir os campos personalizados.

5.4 Avançado

5.4.1 Categoria

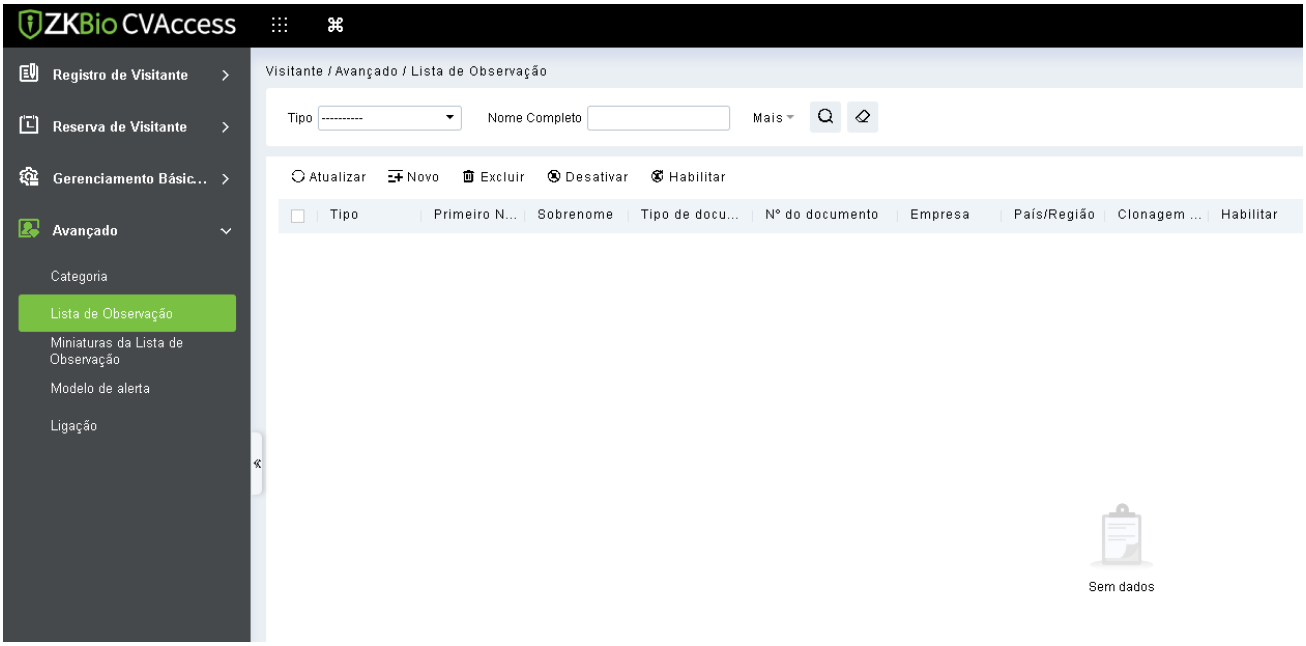
Ao acessar a seção "**Avançado"**e clicar em "**Categoria",** você terá acesso a uma aba para criar novas categorias que serão utilizadas nas lista de observações de visitantes.



- **Novo:** Ao clicar nesta opção, você poderá criar uma nova categoria que será utilizada na lista de observação.
- **Excluir:** Ao clicar nesta opção, você poderá exluir uma categoria .

5.4.2 Lista de Observações

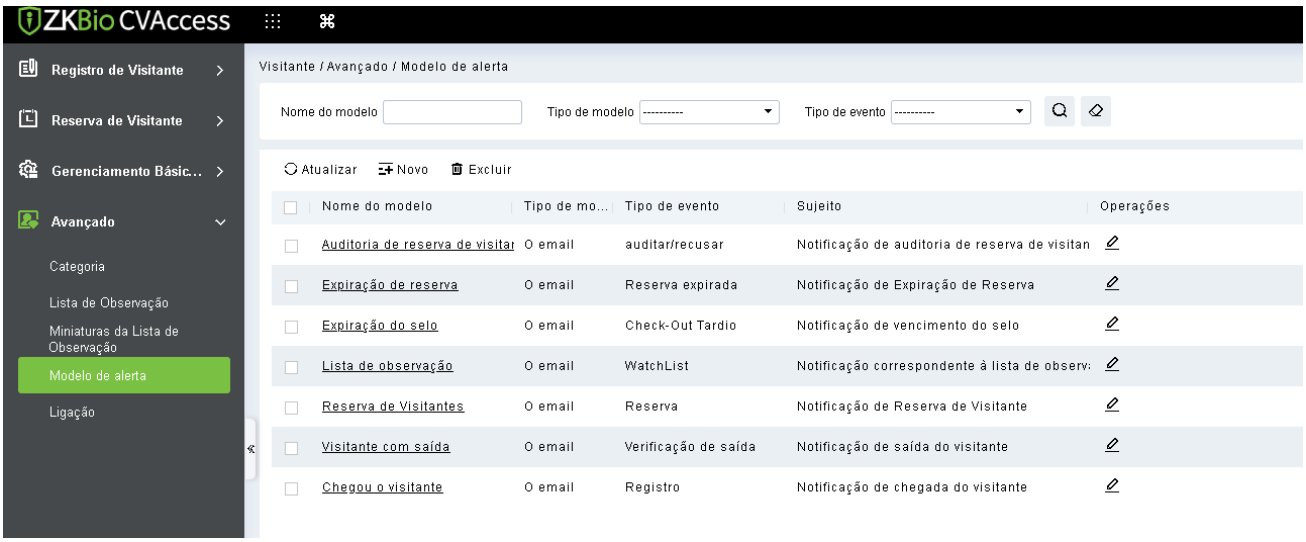
Ao acessar a seção "**Avançado**" e clicar em "**Lista de Observações**", você poderá adicionar visitantes a uma lista de observações. Quando esses visitantes fizerem o check-in, uma aba será aberta com as informações adicionadas, dando ao operador a opção de recusar o check-in ou continuar o processo.



- **Novo:** Ao clicar nesta opção, você poderá adicionar uma empresa, pessoa ou país na lista de observação.
- **Excluir:** Ao clicar nesta opção, você poderá excluir uma empresa, essoa ou país da lista de observação.
- **Desativar:** Ao clicar nesta opção, você poderá desativar a observação para empresas, pessoas ou países na lista de observação. Após isso, as informações de observação não serão exibidas durante o check-in.
- **Habilitar:** Ao clicar nesta opção, você poderá ativar a observação para empresas, pessoas ou países na lista de observação. Depois disso, as informações de observação serão exibidas durante o check-in dos visitantes.

5.4.3 Modelo de Alerta

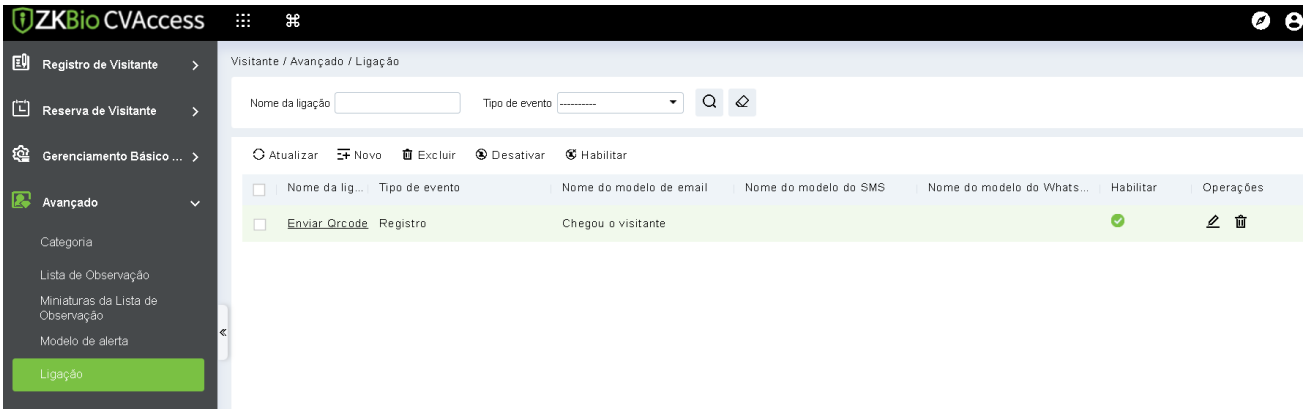
Ao acessar a seção "**Avançado**" e clicar em "**Modelo de Alerta**", você poderá criar e editar modelos de alerta. Esses modelos de alerta são ações que ocorrem após a configuração de uma ligação. Eles permitem o envio de e-mails, códigos QR para os visitantes, entre outros tipos de alertas.



- **Novo:** Ao clicar nesta opção, você poderá criar um novo modelo de alerta.
- **Excluir:** Ao clicar nesta opção, você poderá exluir um modelo de alerta.

5.4.4 Ligação

Ao acessar a seção "**Avançado**" e clicar em "**Ligação**", você poderá criar e editar ligações. As ligações são compostas por um gatilho e uma ação. Uma possibilidade é configurar a ação de enviar um QR code para o e-mail do visitante quando o registro dele ocorrer.

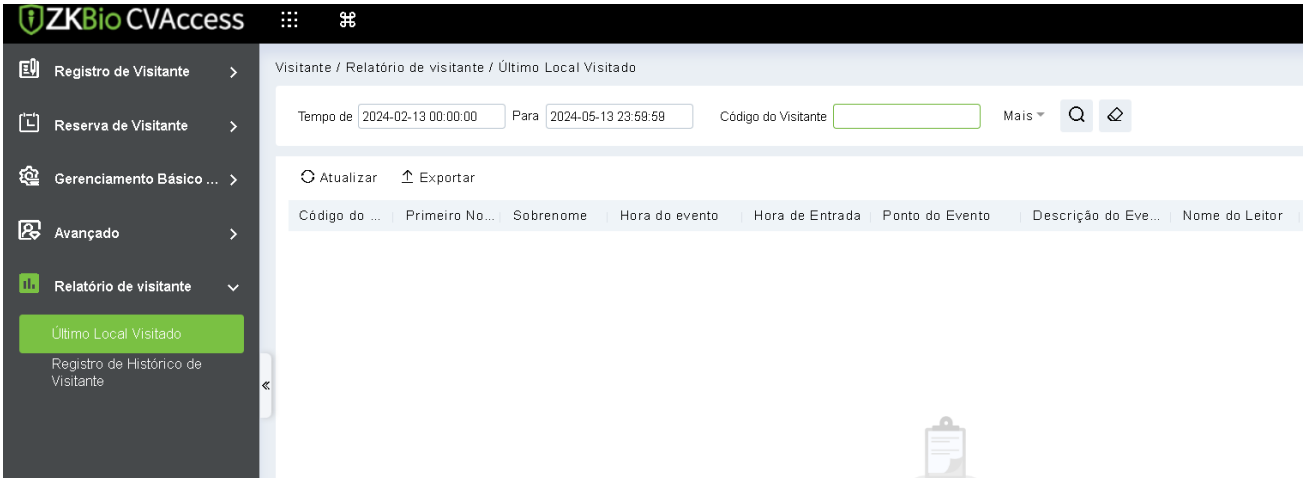


- **Novo:** Ao clicar nesta opção, você poderá criar uma nova ligação.
- **Excluir:** Ao clicar nesta opção, você poderá exclui uma ligação.
- **Desativar:** Ao clicar nesta opção, você poderá desativar uma ligação.
- **Habilitar:** Ao clicar nesta opção, você poderá habilitar uma ligação.

5.5 Relatório de visitante

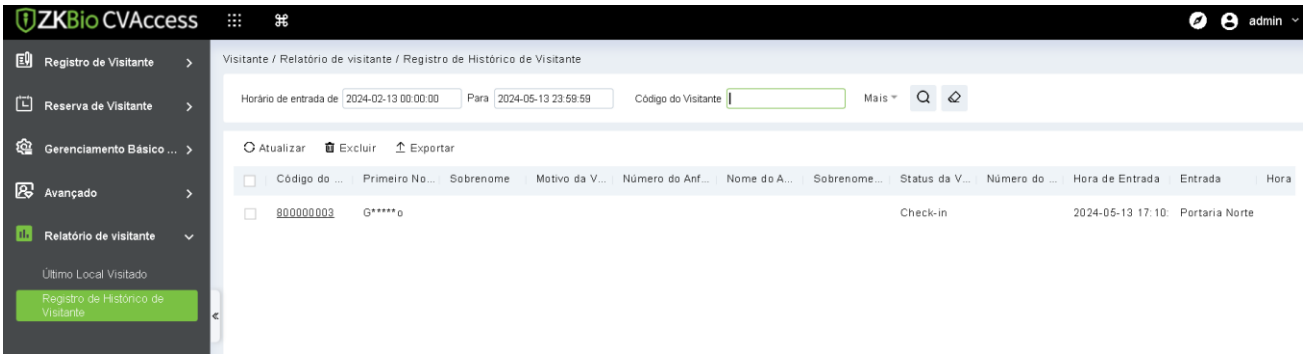
5.5.1 Último Local Visitado

Ao acessar a seção "**Relatório de Visitante**" e clicar em **"último Local Visitado**", você poderá visualizar o último acesso de cada visitante.



5.5.2 Registro de Histórico de Visitante

Ao acessar a seção "**Relatório de Visitante**" e clicar em "**Registro de Histórico de Visitante**", você poderá visualizar o histórico de todos os visitantes que realizaram o check-in



6 Gerenciamento de Vídeo

6.1 Visualização de Vídeo

Clique em **[Vigilância por Vídeo Inteligente] > [Visualização de Vídeo].**

Nesse módulo, você pode acessar os vídeos como Pré-visualização de Vídeo e Reprodução de Vídeo.

6.1.1 Pré-visualização de Vídeo

Clique em **[Vigilância por Vídeo Inteligente] > [Visualização de Vídeo] > [Pré-visualização de Vídeo].**

Você pode revisar os vídeos gravados aqui.

6.1.1.1 Pré-visualização Ao Vivo

Ao aplicar produtos de monitoramento por vídeo, siga estritamente as leis e regulamentos aplicáveis para a aplicação e manutenção de monitoramento por vídeo, gravação, captura de fotos e outros serviços. É proibido que empresas ou indivíduos instalem dispositivos de monitoramento em áreas de escritório, monitorem comportamentos de funcionários ou usem dispositivos de monitoramento por vídeo para espionar a privacidade de outras pessoas para fins ilegais.

➢ **Pré-visualização ao vivo de uma câmera única**

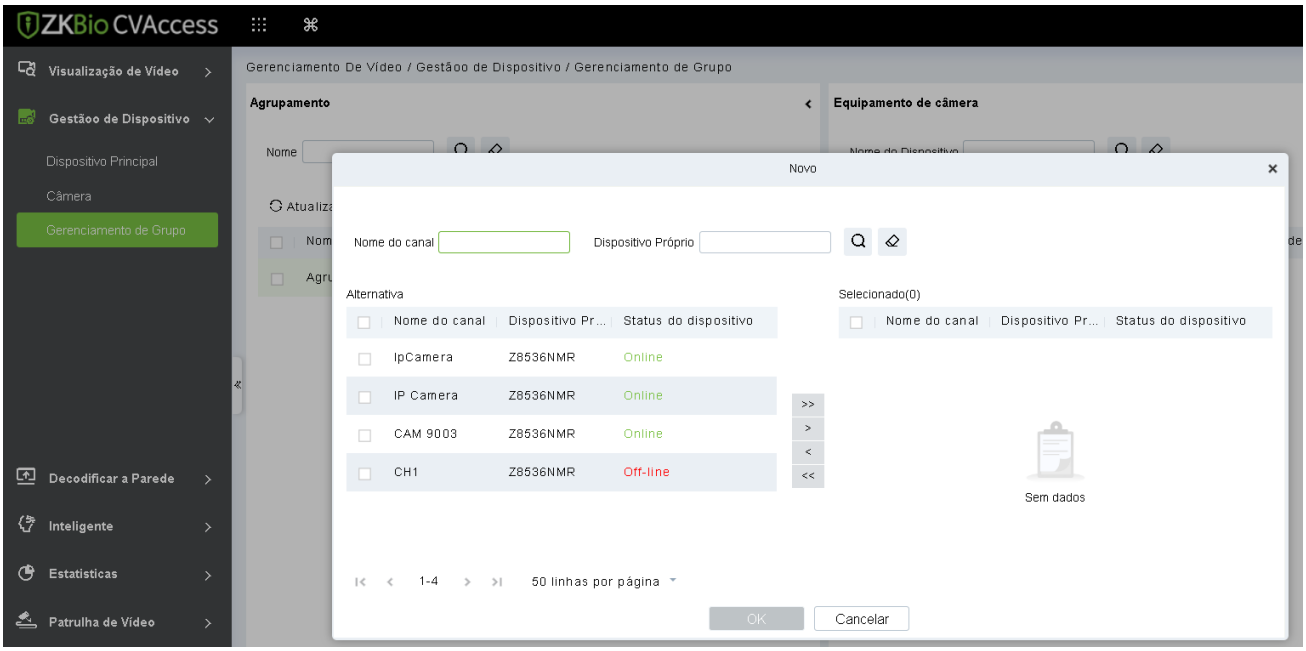
1. Clique em **[Vigilância por Vídeo Inteligente] > [Visualização de Vídeo] > [Pré-visualização de Vídeo].**
2. Na lista de dispositivos, clique duas vezes na câmera online para abrir a pré-visualização ao vivo.

Nota: Durante a pré-visualização ao vivo, evite sobrepor janelas, interfaces ou caixas de diálogo de outros programas na janela que abre a visualização ao vivo, pois isso pode causar lentidão na tela ou na reprodução do vídeo.

➢ **Visualização ao vivo da câmera em grupo**

1. Clique em **[Vigilância de Vídeo Inteligente] > [Gerenciamento de Dispositivos] > [Gerenciamento de Agrupamento].**
2. Clique em **[Adicionar]** na lista de agrupamento, insira o nome do agrupamento e clique em "Confirmar" para concluir a adição do agrupamento de câmeras.
3. Selecione o grupo de câmeras recém-criado e clique em **[Adicionar Câmera]** no lado direito. Dê um clique duplo na câmera na nova interface que aparece e clique em **[OK]** para adicioná-la ao agrupamento, conforme mostrado na figura abaixo.
4. No módulo Inteligente, **selecione [Visualização de Vídeo] > [Visualização ao Vivo],** e em "Dispositivos em Agrupamento", dê um clique duplo na câmera online para abrir a visualização ao vivo.

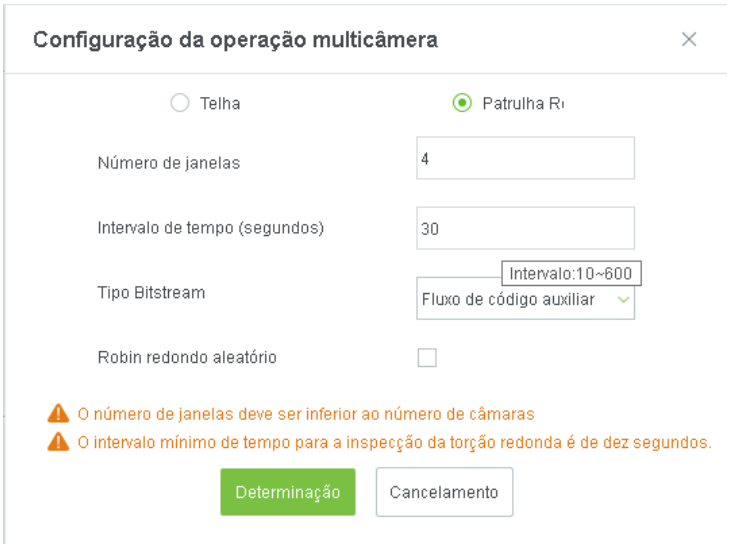
Nota: Durante a visualização ao vivo, por favor, não sobreponha as janelas, interfaces ou caixas de diálogo de outros programas na janela que abre ao vivo, caso contrário, pode causar problemas na exibição do vídeo ou tela ao vivo.



6.1.1.2 Visualização de Vídeo

Usando a função de patrulha circular, o usuário pode alternar as imagens ao vivo monitoradas por várias câmeras regularmente. Por exemplo, se houver múltiplas câmeras em uma cena e a situação ao vivo de todas as câmeras não puder ser exibida em uma interface dividida ao vivo, o administrador pode alternar automaticamente as câmeras de uma cena para monitorar a situação ao vivo a cada 30 segundos usando a função de patrulha circular e realizar a navegação ao vivo de todas as câmeras em lotes e períodos de tempo.

1) Clique em **[Vigilância de Vídeo Inteligente] > [Visualização de Vídeo] > [Visualização ao Vivo].**
2) Na lista de dispositivos agrupados ou dispositivos completos, clique em " " no lado direito para abrir a página "Configurações de Operação de Múltiplas Câmeras".
3) Clique em [Patrulha Circular] para abrir a janela de configuração de patrulha circular e configurar as informações de patrulha circular.



Descrição dos Campos:

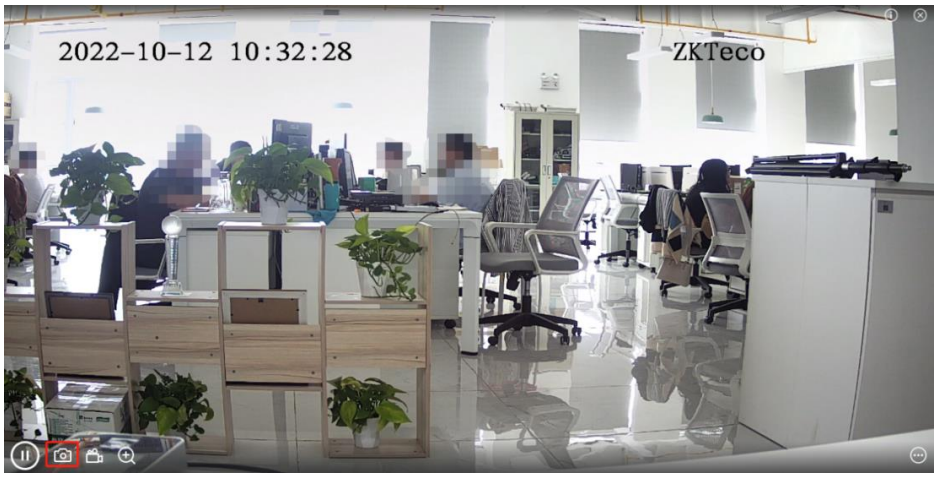
- **Número de janelas:** O número de janelas de rotação circular deve ser menor que o número de câmeras de rotação circular.
- **Intervalo de tempo (segundos):** Configure o tempo de permanência da rotação da câmera sob o dispositivo principal selecionado.
- **Tipo de fluxo:**
    1. Fluxo de código principal: grande fluxo de código, alta definição e alta ocupação de largura de banda.
    2. Fluxo de código auxiliar: O fluxo de código é pequeno, a definição é baixa e a largura de banda é pequena.
    3. Descrição: Quando há limitação de largura de banda, é recomendável selecionar o fluxo de código secundário.

4) Clique em **[OK]** para iniciar a patrulha circular.
5) Termine a patrulha e clique na barra de ferramentas abaixo para fechar todas as telas.

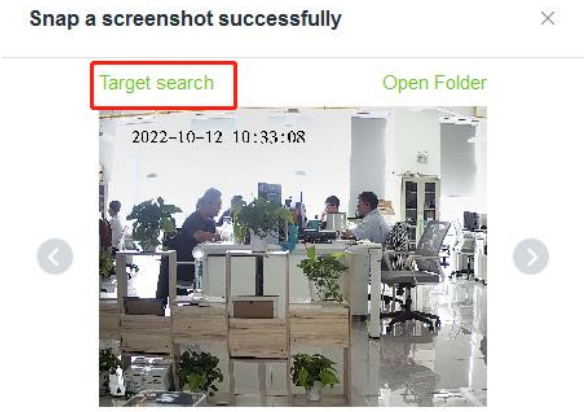
➢ Pesquisa Rápida de Alvos

Captura de tela para pesquisa rápida de alvos durante a visualização ou reprodução: Quando os guardas de segurança visualizam vigilância em tempo real ou vídeos de reprodução e encontram uma pessoa suspeita na tela, eles podem dar zoom nessa pessoa e tirar uma captura de tela para apoiar a "pesquisa rápida de alvos" para pular para a pesquisa de alvos e mapeamento de rastreamento de pessoa.

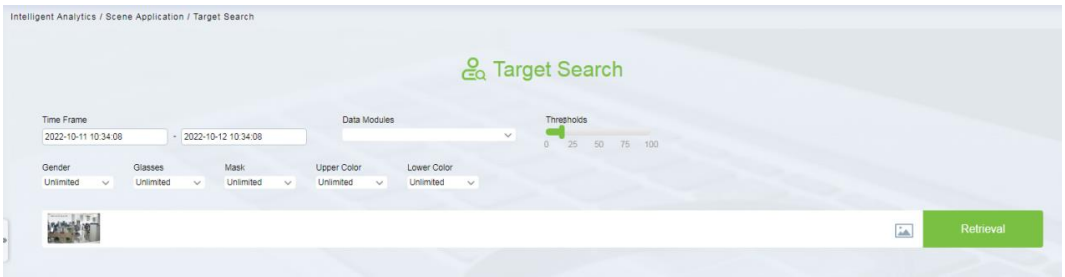
1. Vá para [Vigilância de Vídeo Inteligente] > [Visualização de Vídeo], clique



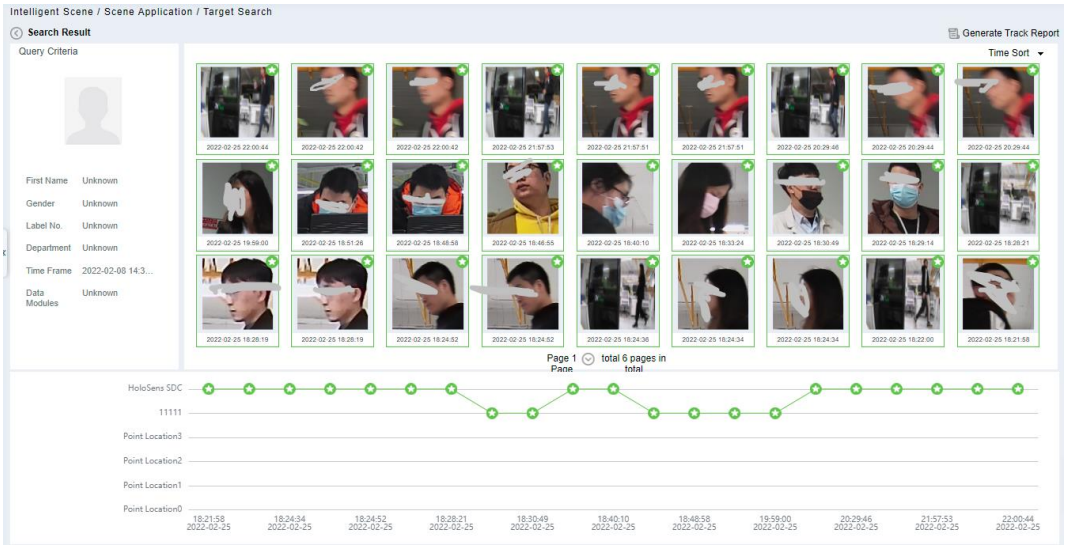
2. Em seguida, clique em [Pesquisa de Alvo].



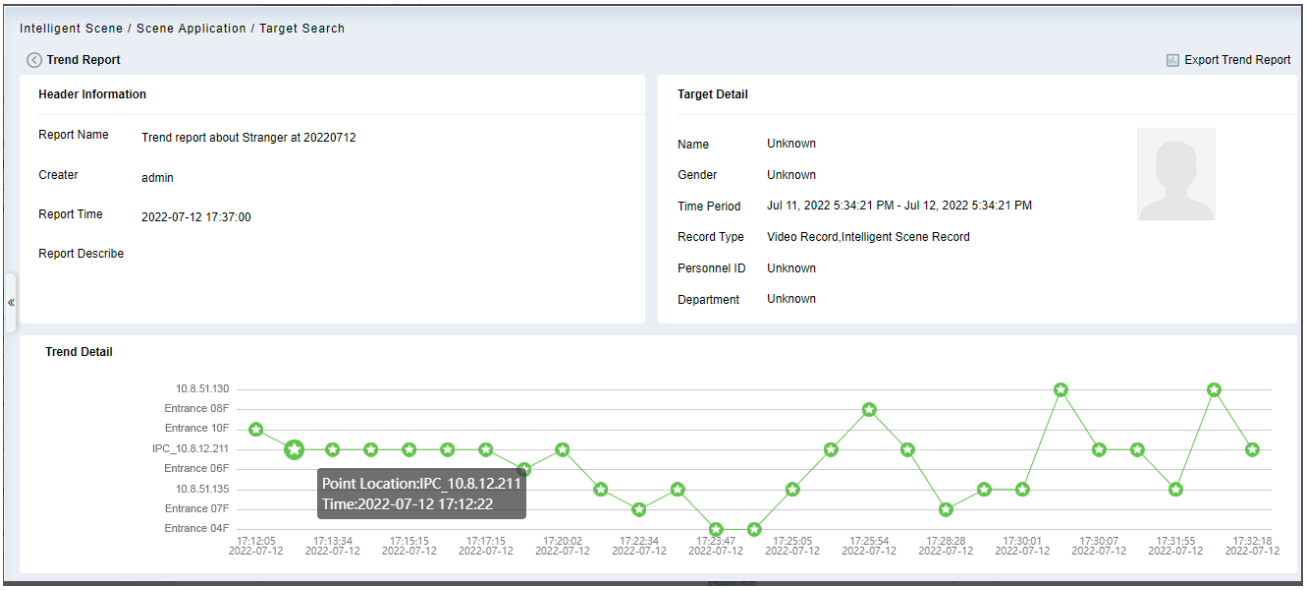
3. Depois clique em [Recuperação].

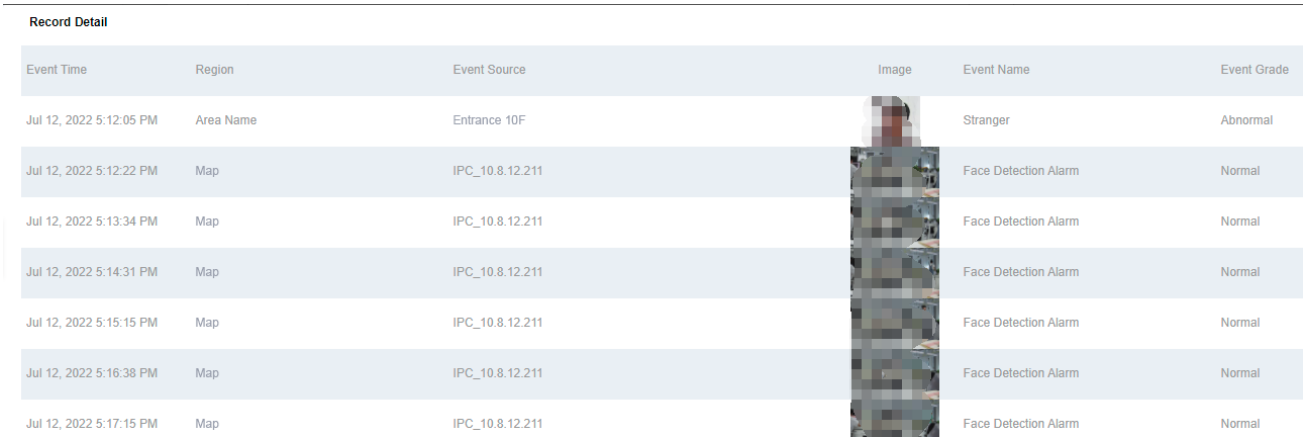


4. Após a recuperação, os resultados de recuperação aparecem.



5. Nos resultados de recuperação, você pode clicar em Gerar Relatório de Tendências no canto superior direito da interface para exportar o relatório de tendências em formato PDF, conforme mostrado na figura abaixo.





6.1.2 Reprodução de Vídeo

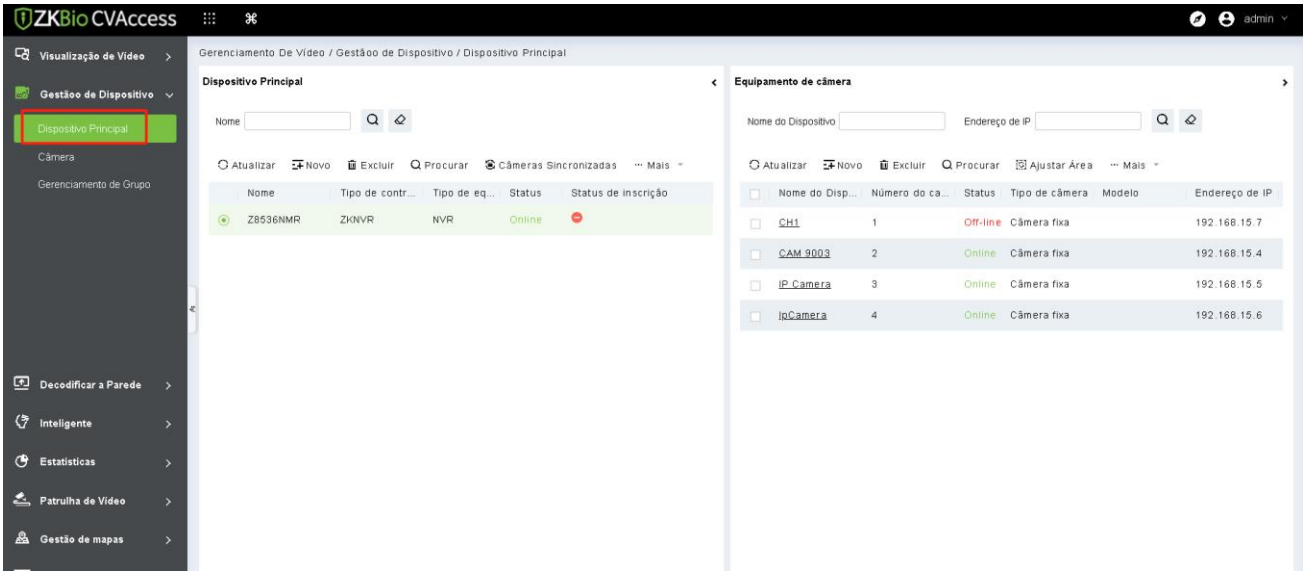
Clique em **[Vigilância de Vídeo Inteligente] > [Visualização de Vídeo] > [Reprodução de Vídeo].**

6.2 Gerenciamento de Dispositivos

6.2.1 Dispositivo

Esta operação é usada para instruir os usuários sobre como conectar o NVR à plataforma e às câmeras, para que a plataforma possa gerenciar os dispositivos conectados de forma uniforme, como visualizar a transmissão ao vivo e as gravações de vídeo das câmeras.

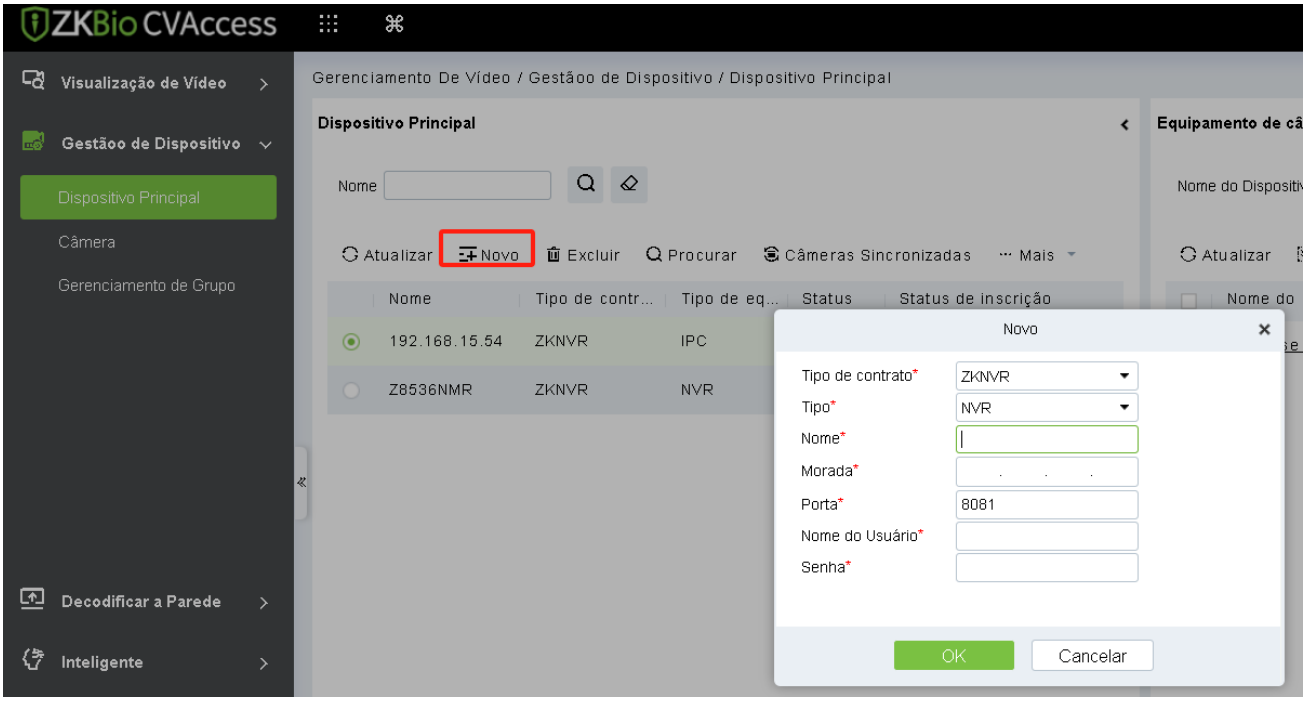
Clique em **[Vigilância de Vídeo Inteligente] > [Gerenciamento de Dispositivos] > [Dispositivo].**



6.2.1.1 Adicionar Dispositivos (Novo)

Suporta no máximo 1024 canais de vídeo, suporta 64 canais de pré-visualização e 16 canais de reprodução em tempo real simultaneamente.

1. Clique em [Novo] na lista de dispositivos principais para exibir a interface de adição.



Existem 4 tipos que você pode selecionar (IVS1800/NVR800/ZKNVR/TD NVR3000). Se o dispositivo adquirido for ZKNVR, selecione "ZKNVR" para o tipo.

Descrição dos Campos:

- **Tipo:** Selecione o tipo de dispositivo.
- **Nome:** Personalize o nome do dispositivo.
- **Endereço:** Configure o endereço do dispositivo. O formato é: xxx.xxx.xxx.xxx, por exemplo: 192.168. 6.5. Porta: Configure a porta do dispositivo. O padrão do ZKNVR é 8081.
- **Nome de Usuário e Senha:** Nome de usuário e senha do NVR.

Nota:

- Para ZKNVR, a conta padrão é (admin,12345678)
- Para IVS1800, você deve fazer login na página web para adicionar uma nova conta.

2. Clique em **[OK].**

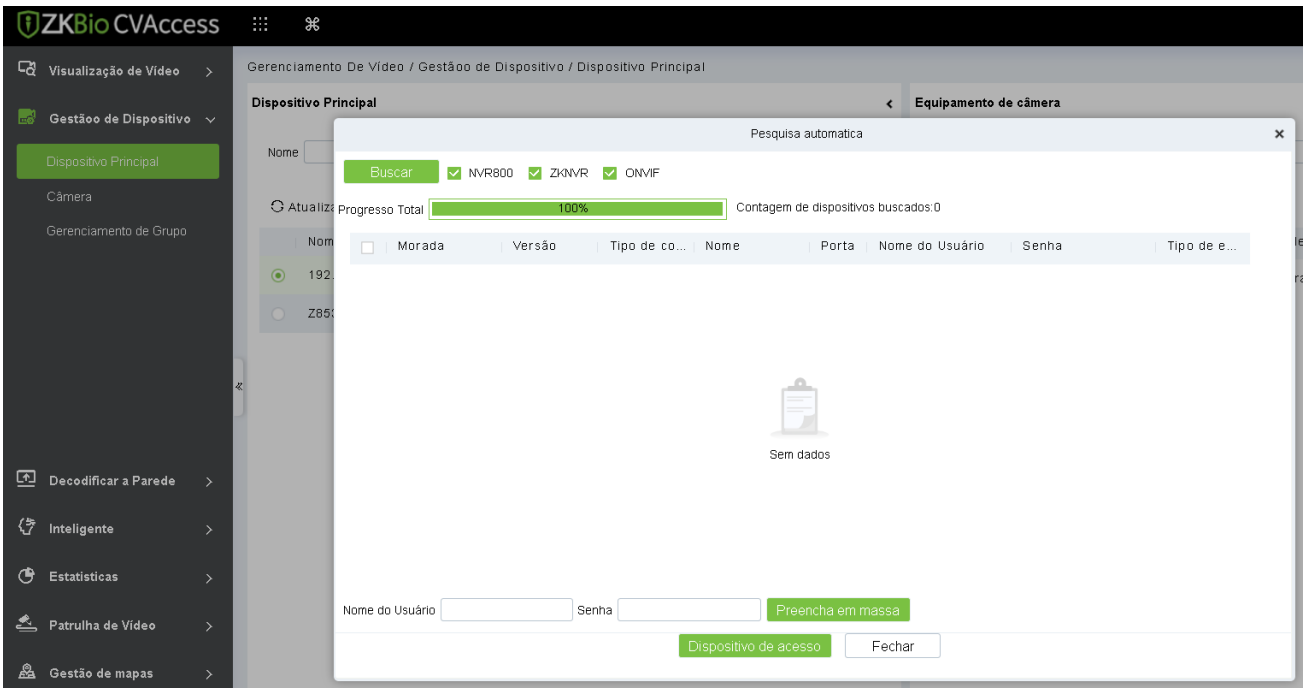
6.2.1.2 Excluir

Clique em **[Vigilância de Vídeo Inteligente] > [Gerenciamento de Dispositivos] > [Dispositivo],** então selecione **[Excluir].**

6.2.1.3 Pesquisar

Clique em **[Vigilância de Vídeo Inteligente] > [Gerenciamento de Dispositivos] > [Dispositivo]**, você pode selecionar o tipo de dispositivo e clicar em Pesquisar.

Nota: A pesquisa não é suportada para IVS1800/TD NVR3000.

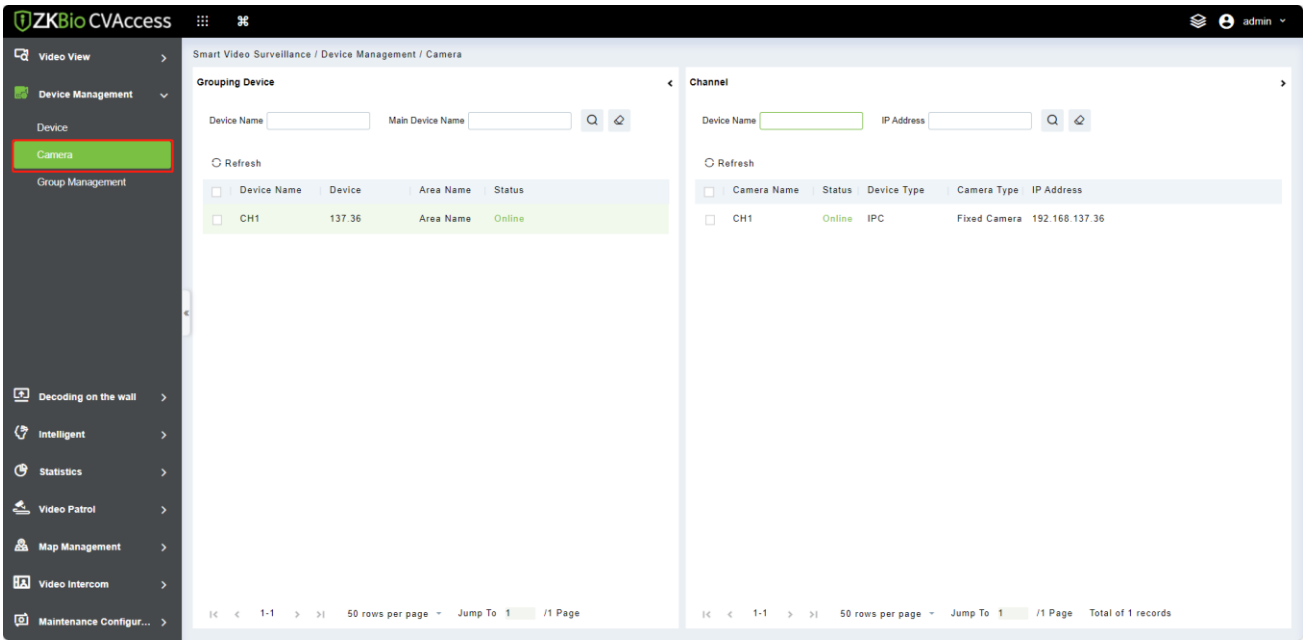


6.2.1.4 Sincronizar Câmera

Clique em **[Vigilância de Vídeo Inteligente] > [Gerenciamento de Dispositivos] > [Dispositivo],** então clique em **[Sincronizar Câmera].**

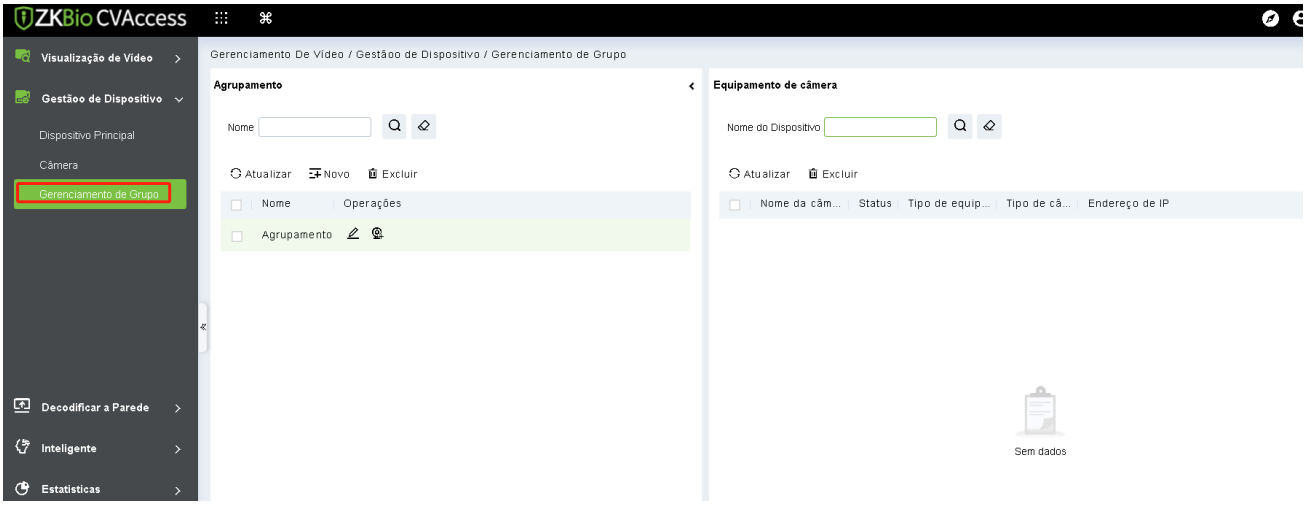
6.2.2 Câmera

Clique em **[Vigilância de Vídeo Inteligente] > [Gerenciamento de Dispositivos] > [Câmera].**



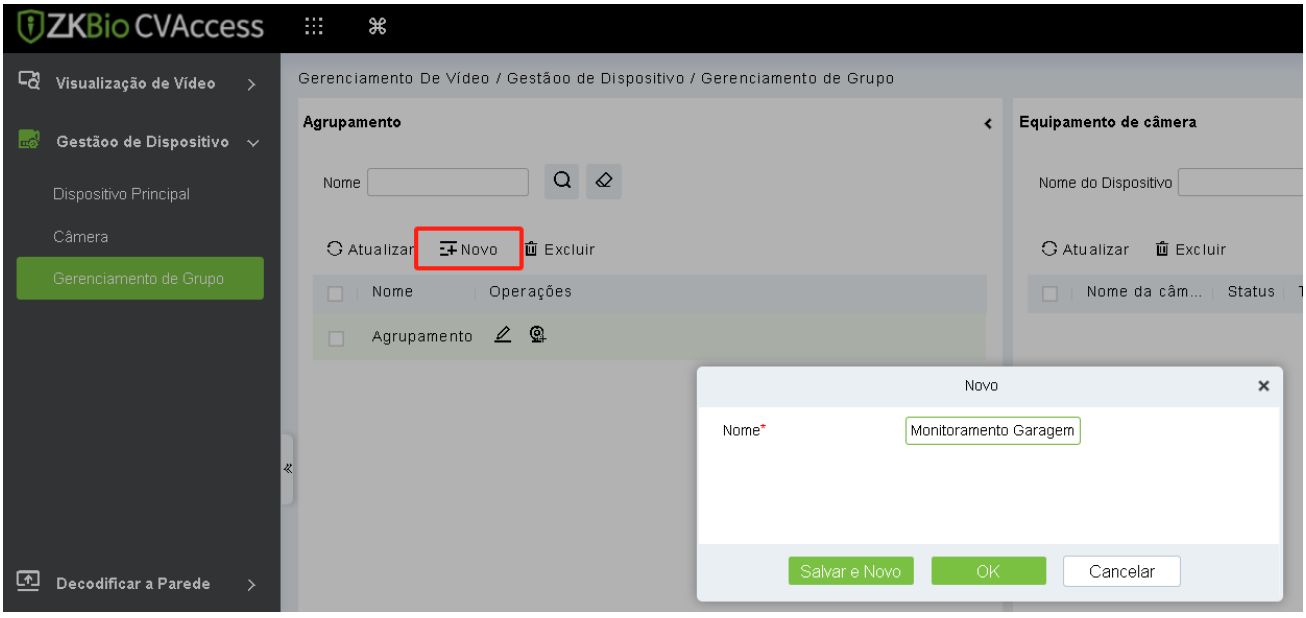
6.2.3 Gerenciamento de Grupos

Clique em **[Vigilância de Vídeo Inteligente] > [Gerenciamento de Dispositivos] > [Gerenciamento de Grupos].**



6.2.3.1 Novo

1. Clique em **[Vigilância de Vídeo Inteligente] > [Gerenciamento de Dispositivos] > [Gerenciamento de Grupos],** então clique em **[Novo].**



2. Clique em **[OK]** para salvar e sair.

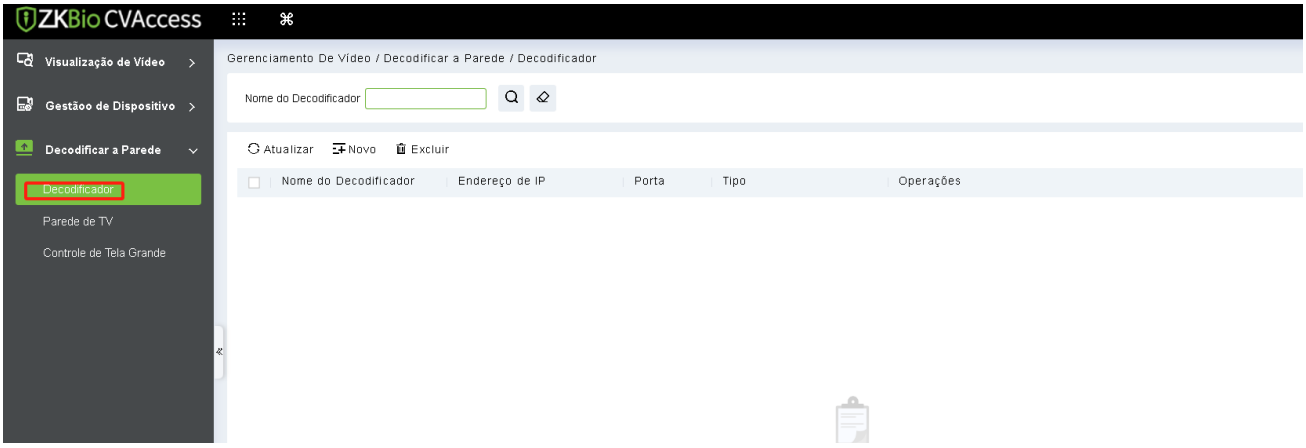
6.2.3.2 Excluir

Clique em **[Vigilância de Vídeo Inteligente] > [Gerenciamento de Dispositivos] > [Gerenciamento de Grupos],** depois clique em **[Excluir].**

6.3 Decodificação na Parede

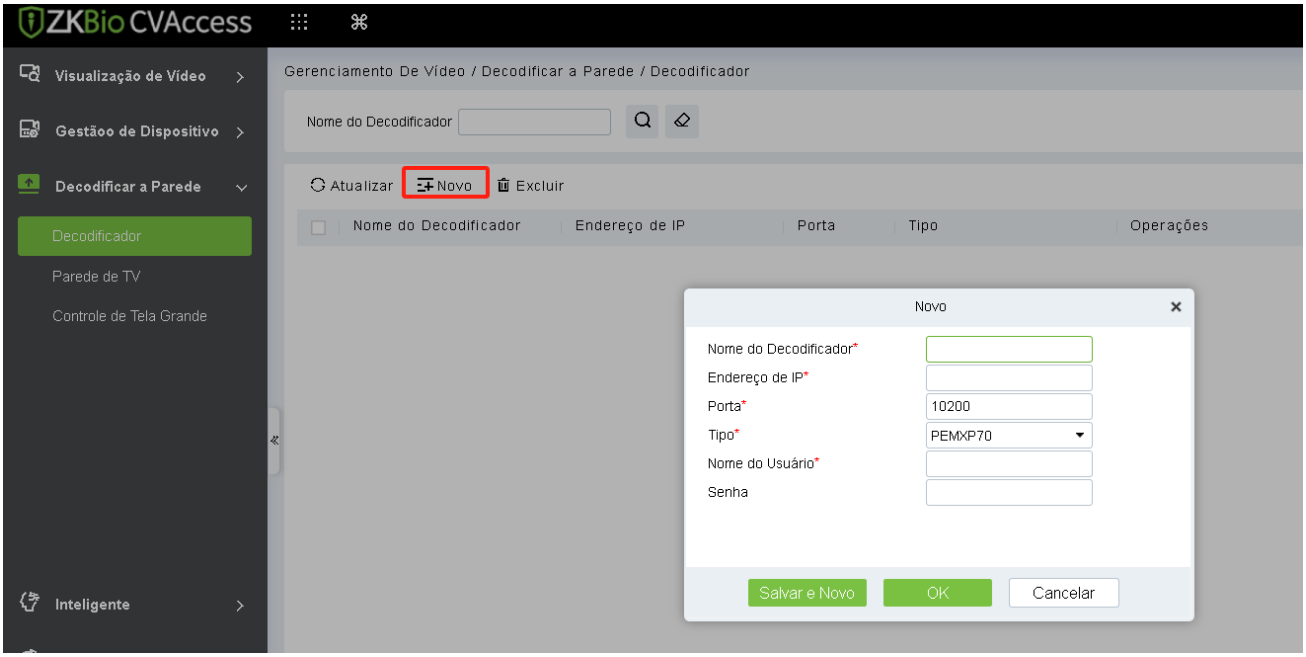
6.3.1 Decodificador

Clique em **[Smart Video Surveillance] > [Decodificação na parede] > [Decodificador].**



6.3.1.1 Novo (Adicionar Decodificador)

1. Clique em **[Novo].**



Descrição do Campo:

Nome do Decodificador: Nome personalizado do decodificador.

Endereço IP: Endereço IP do decodificador.

Porta: Porta padrão 10200.

Tipo: Selecione o modelo de dispositivo para acessar o decodificador. Suporta acesso ao decodificador PEMXP70 e DEC6109.

Nome de usuário: Insira o nome de usuário do negócio.

Senha: Insira a senha do negócio.

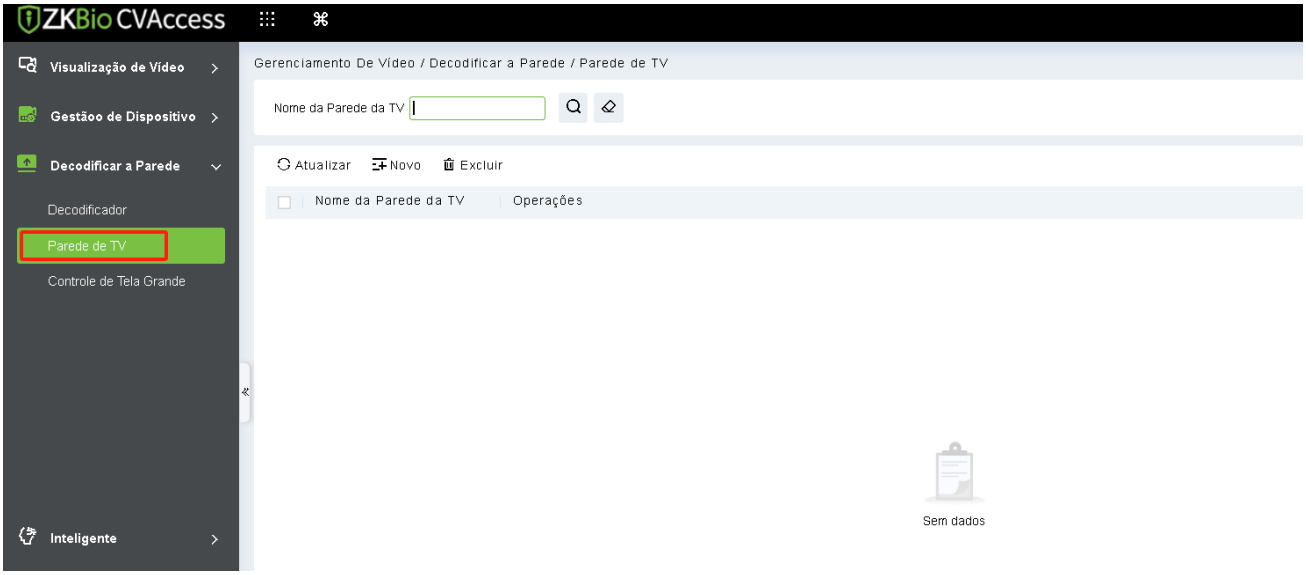
2. Clique em [OK] para salvar e sair, ou clique em [Salvar e Novo] para continuar.

6.3.1.2 Excluir

Clique em **[Smart Video Surveillance] > [Decodificação na parede] > [Decodificador],** e então clique em **[Excluir].**

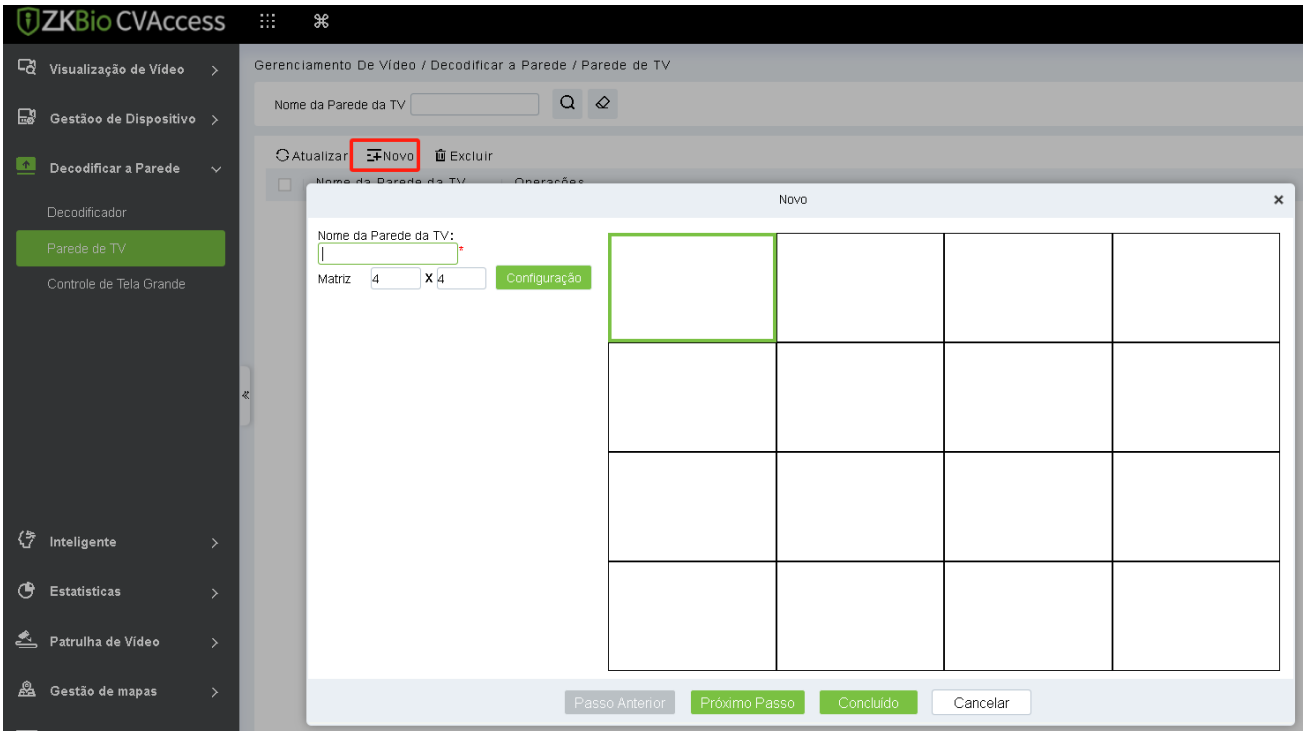
6.3.2 Parede de TV

Clique em **[Smart Video Surveillance] > [Decodificação na parede] > [Parede de TV].**



6.3.2.1 Novo (Criar Parede de TV)

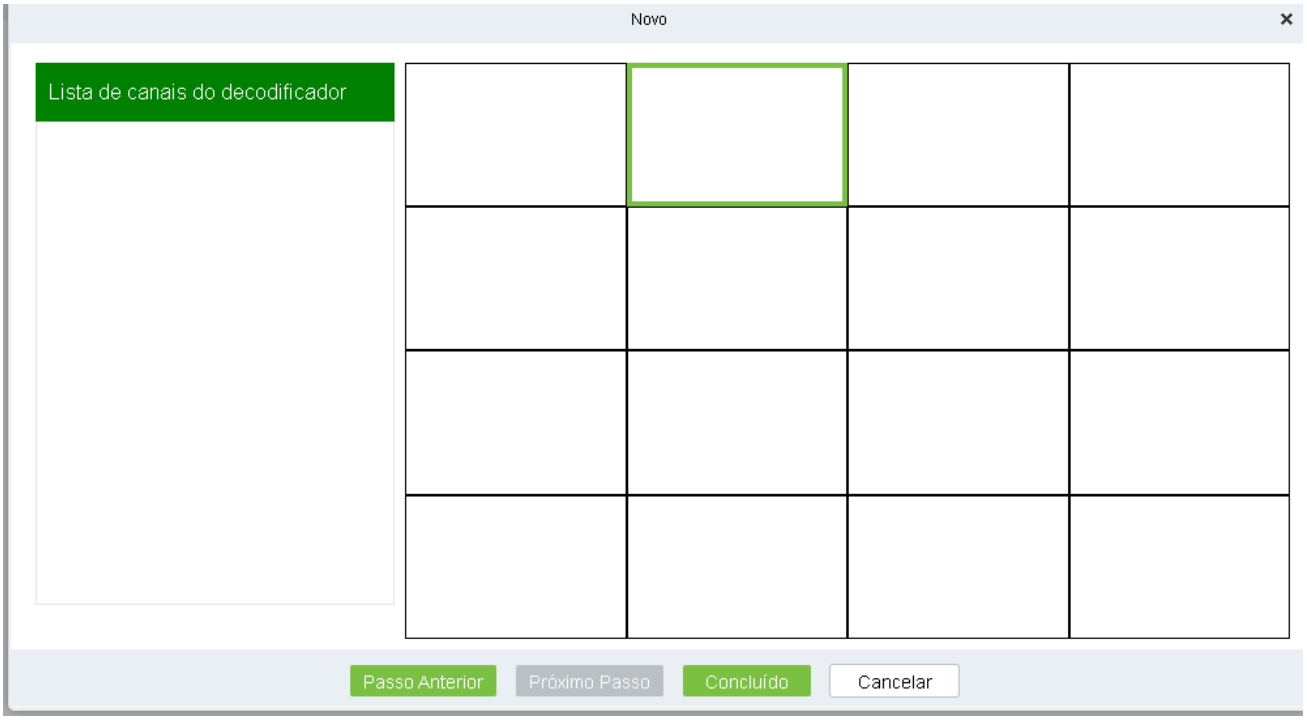
1. Clique **em [Smart Video Surveillance] > [Decodificação na parede] > [Parede de TV],** e então clique em [Novo (Criar Parede de TV)].



2. Insira um nome personalizado para a Parede de TV.
3. Na caixa de Configurações da Matriz, personalize o número de linhas e a lista de layouts de entrada, e clique em [Configurar] para aplicar o layout.

Observação: As configurações do painel de layout da matriz suportam no mínimo 1 * 1 e no máximo 8 * 8.

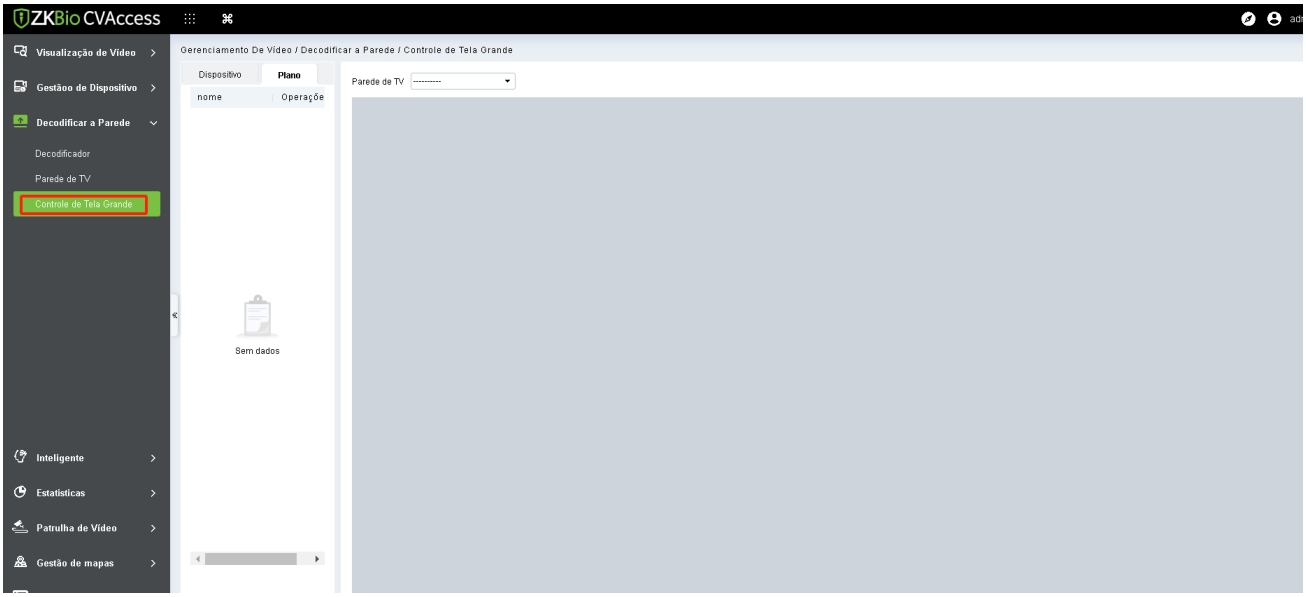
4. Clique em avançar para entrar na interface de vinculação do decodificador da parede de TV, como mostrado na figura abaixo.



5. Selecione o painel da parede de TV ao qual deseja adicionar um canal de decodificador e clique em **[Canal do Decodificador]** à esquerda para concluir a vinculação.
6. Clique em **[Concluir]** para terminar de adicionar a parede de TV.

6.3.3 Controle de Tela Grande

Clique em **[Smart Video Surveillance] > [Decodificação na parede] > [Controle de Tela Grande].**



Ícone	Parâmetro	Descrição
	Configuração de Alarme	Selecionar uma tela para mostrar os eventos de alarmes vinculados
	Pré-visualização de Vídeo	Visualizar a tela atual
	Coleção de Plano	Adicionar à lista de perfis de coleção
	Tela Mesclada	Mesclar várias telas dispersas em uma
	Tela Dividida	Separar as telas mescladas

	Janela Flutuante	Janela de tela flutuante
	Fim na Parede	Encerrar na parede
	1 Tela Dividida	1 Tela Dividida
	4 Telas Divididas	4 Telas Divididas
	8 Telas Divididas	8 Telas Divididas
	9 Telas Divididas	9 Telas Divididas
	16 Telas Divididas	16 Telas Divididas
	25 Telas Divididas	25 Telas Divididas

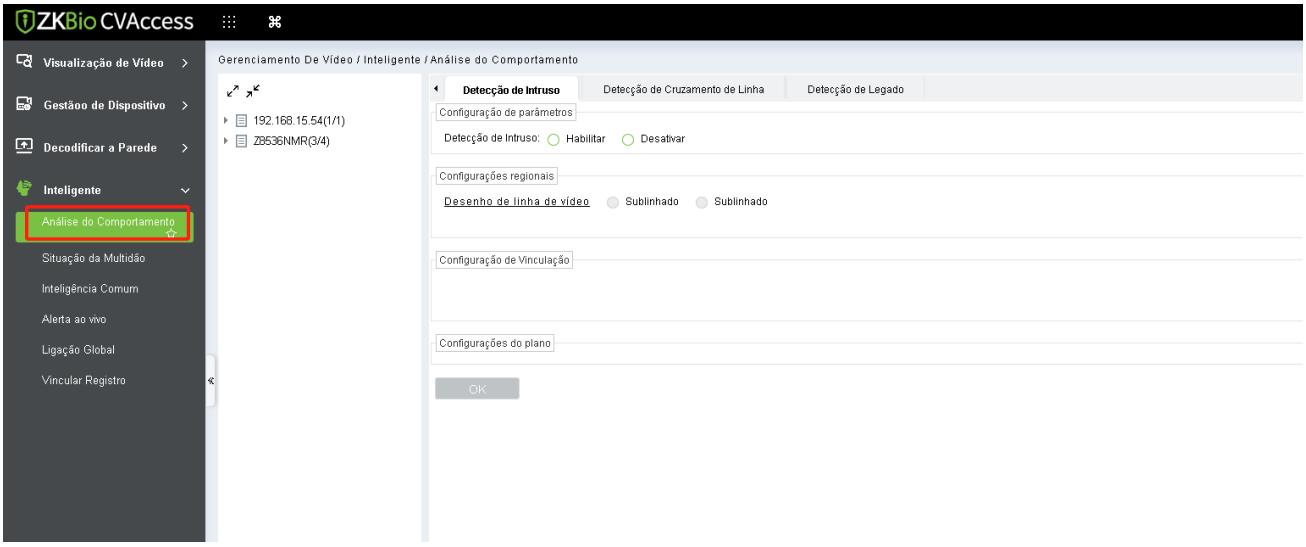
6.4 Inteligente

6.4.1 Análise Comportamental

Configuração de funções inteligentes para análise comportamental das câmeras front-end pela ZKBio CVAccess.

Observação: A interface padrão faz parte da funcionalidade do Holowits.

Clique em **[Smart Video Surveillance] > [Inteligente] > [Análise Comportamental].**



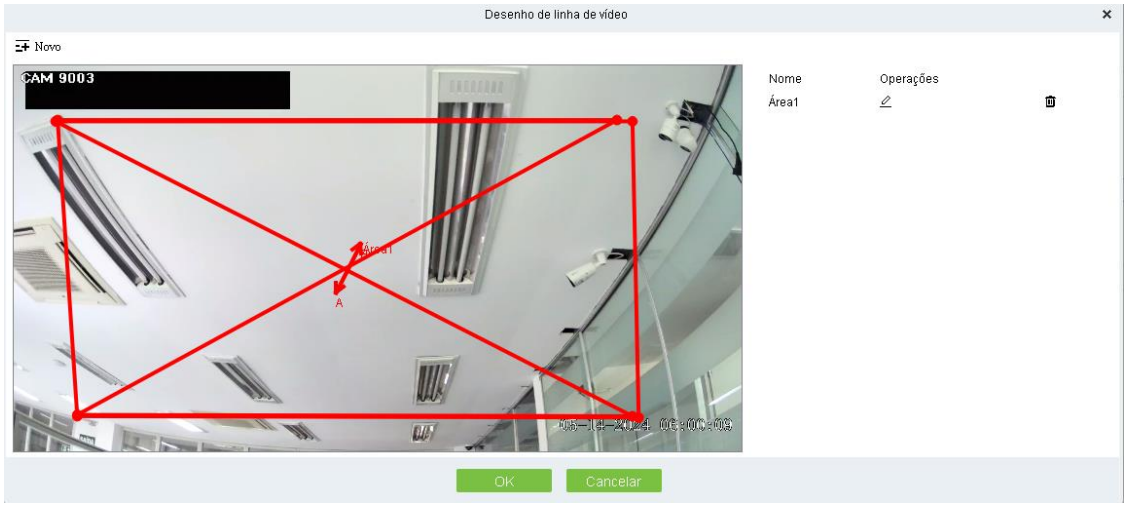
➢ Configuração de Parâmetros

Configure para ativar detecção de intrusão.

➢ Configurações Regionais

- **Cruzado:** Indica que uma linha está atualmente desenhada para esse recurso inteligente.
- **Não Riscado:** Indica que uma linha não está atualmente desenhada para esse recurso inteligente.

Clique em [Desenhar Ligação de Vídeo], desenhe a área de detecção.

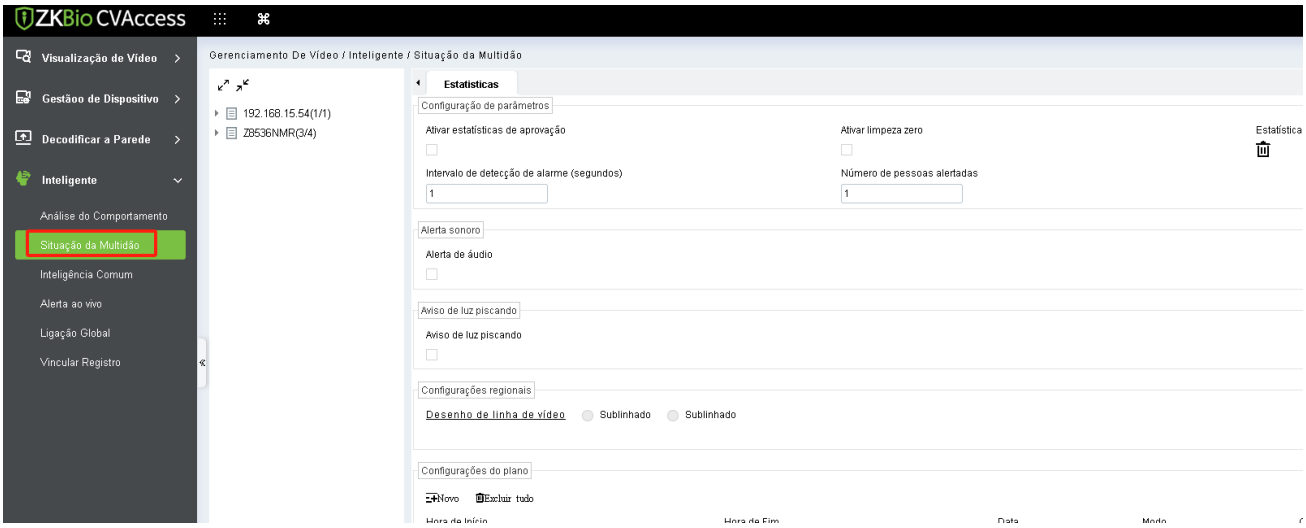


6.4.2 Situação de Multidão

Configuração de funções inteligentes para situação de multidão das câmeras front-end pela ZKBio CVAccess.

Observação: A interface padrão faz parte da funcionalidade do Holowits.

Clique em **[Smart Video Surveillance] > [Inteligente] > [Situação de Multidão].**



6.4.3 Inteligência Geral

Configuração de funções de inteligência geral das câmeras front-end pela ZKBio CVSecurity.

Observação: A interface padrão faz parte da funcionalidade do Holowits.

Clique em **[Smart Video Surveillance] > [Inteligente] > [Inteligência Geral].**

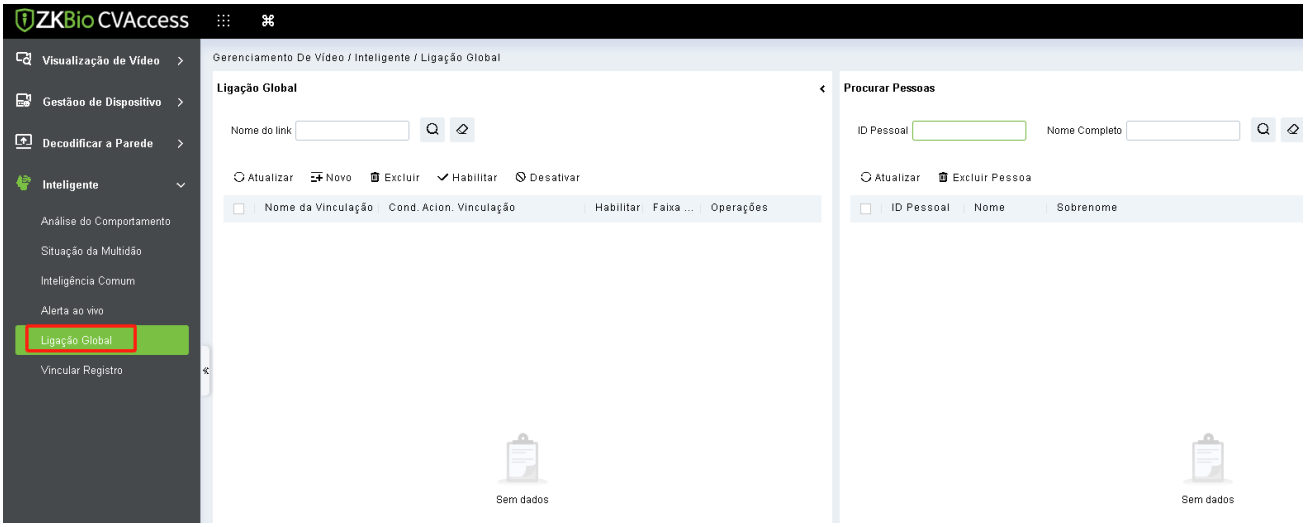
➢ Configuração de Parâmetros

- **Sensibilidade:** Sensibilidade de detecção.
- **Modo:**

1) Inteligente: Pode distinguir entre pessoas ou veículos.
2) Normal: Sem distinção entre pessoas e veículos.

6.4.4 Linkagem Global

Clique em **[Smart Video Surveillance] > [Inteligente] > [Linkagem Global].**



6.4.5 Registro de Link

Clique em **[Smart Video Surveillance] > [Inteligente] > [Registro de Link].**

➢ Limpar Todos os Dados

Clique em [Limpar Todos os Dados] para abrir um prompt e clique em **[OK]** para limpar todos os registros.

6.5 Estatísticas

6.5.1 Relatório de Alarme

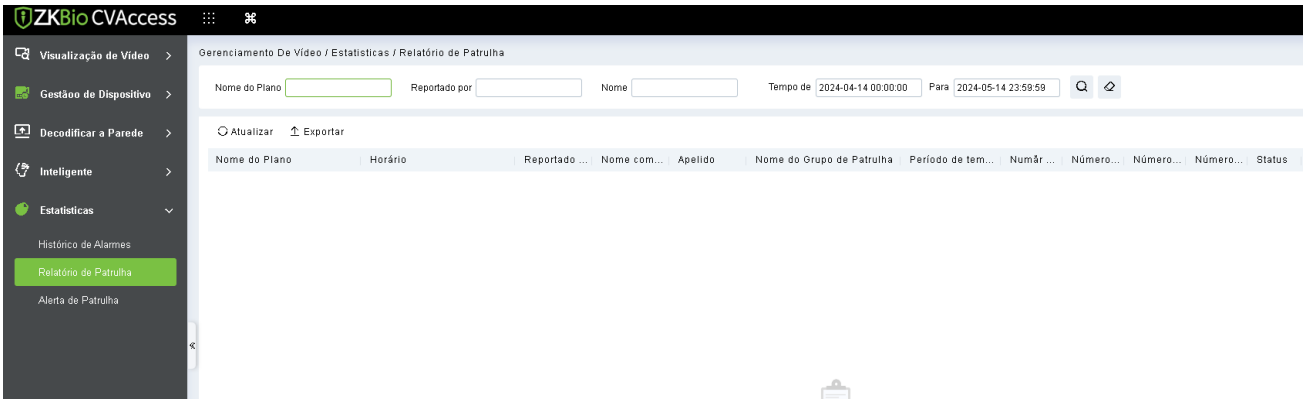
Neste módulo, você pode acessar os dados para o tipo de pessoal ou pessoa, pode selecionar o horário de início e término, o número de série do canal de vídeo e diferentes tipos de alarme para filtrar o relatório.

Clique em **[Smart Video Surveillance] > [Estatísticas] > [Relatório de Alarme].**

6.5.2 Relatório de Patrulha

Neste módulo, você pode acessar os dados para o tipo de pessoal ou pessoa como dd, aa, vip, ou VIP, lista de bloqueios, lista de permissões e Estranho para obter dados seguindo as opções.

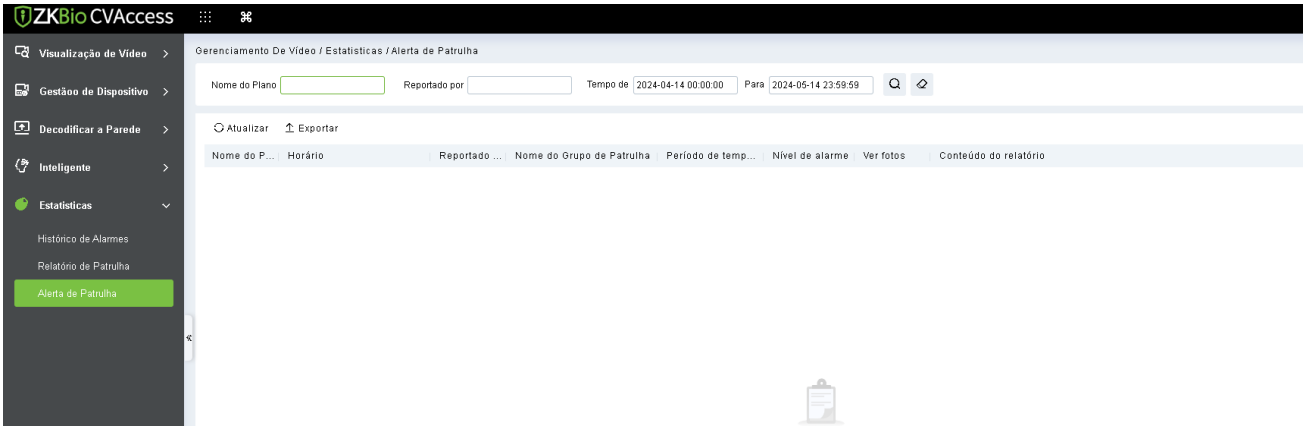
Clique em **[Smart Video Surveillance] > [Estatísticas] > [Relatório de Patrulha].**



6.5.3 Alarme de Patrulha

Neste módulo, você pode acessar os dados para o tipo de pessoal ou pessoa como dd, aa, vip, ou VIP, lista de bloqueios, lista de permissões e Estranho para obter dados seguindo as opções.

Clique em **[Smart Video Surveillance] > [Estatísticas] > [Alarme de Patrulha].**



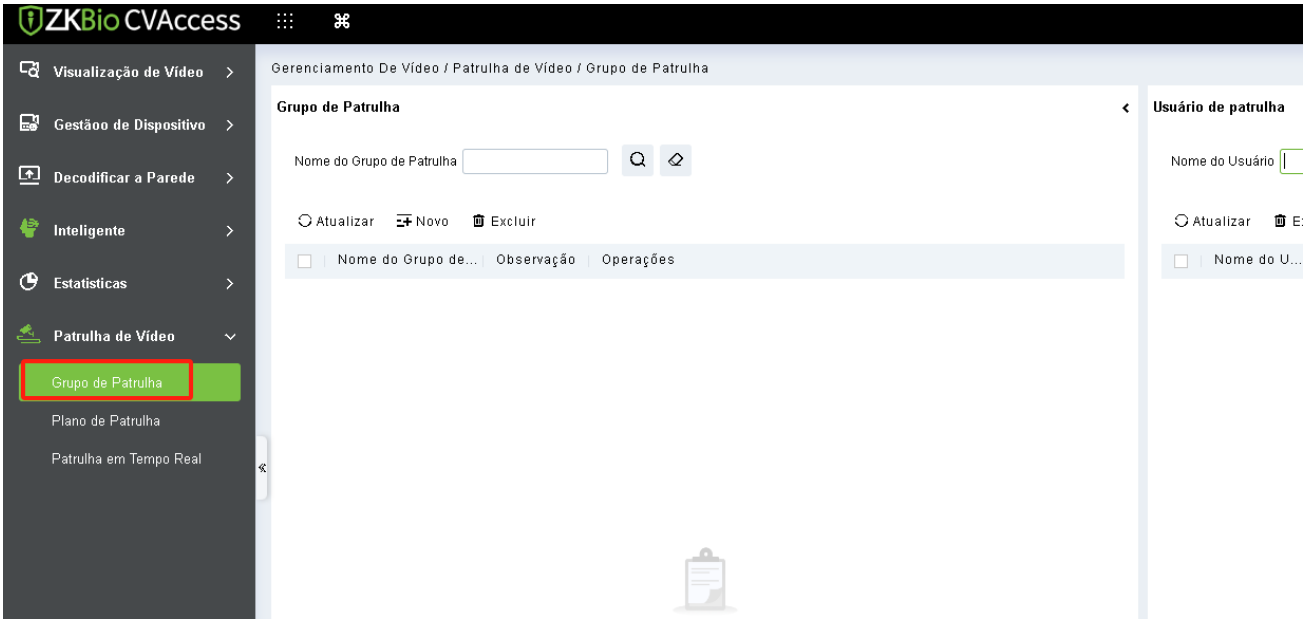
6.6 Patrulha de Vídeo

No caminho predefinido, você pode verificar a marcação do ponto por uma visualização em tempo real da câmera remotamente para alcançar a mesma tarefa de patrulha que o efeito de marcação tradicional.

6.6.1 Grupo de Patrulha

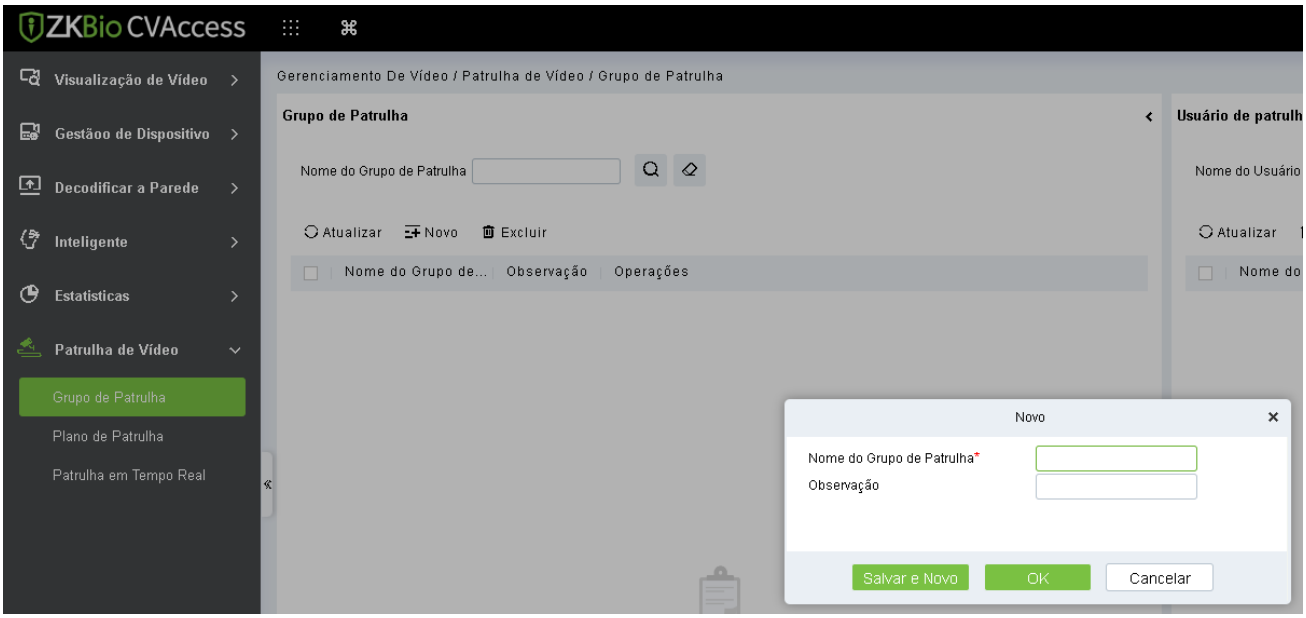
Crie um grupo de patrulha para adicionar pessoal de patrulha.

Clique em **[Smart Video Surveillance] > [Patrulha de Vídeo] > [Grupo de Patrulha].**



6.6.1.1 Adicionar Grupo de Patrulha

Clique em **[Novo].**

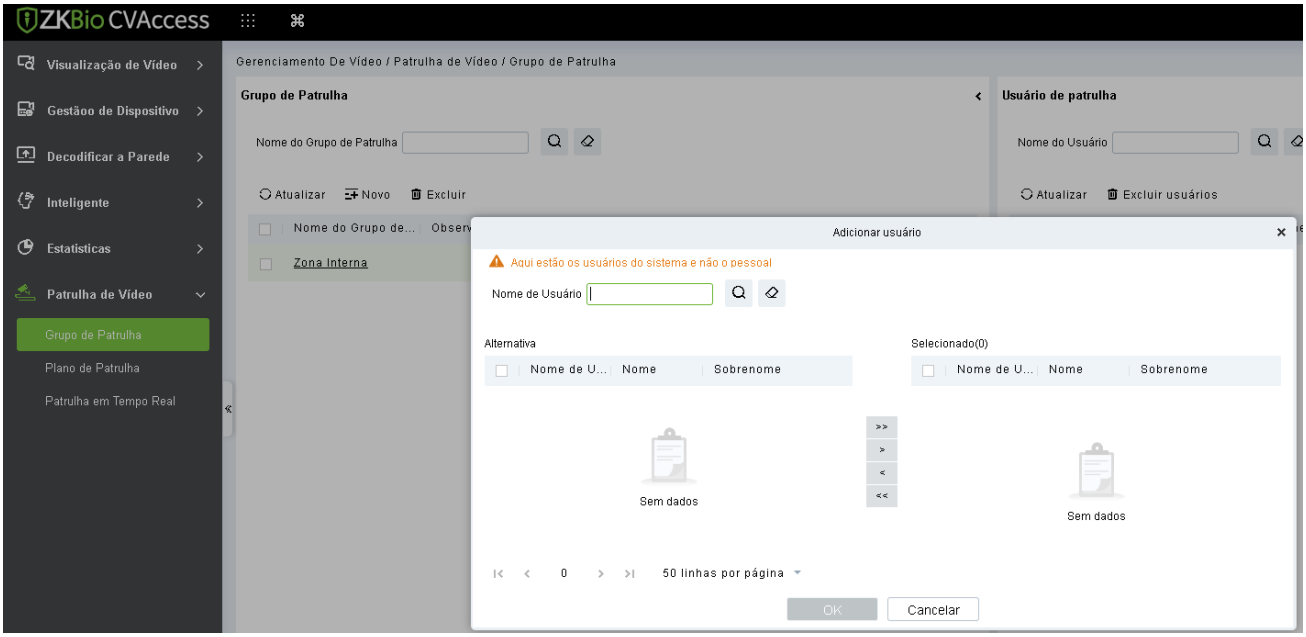


Descrição do Campo:

- **Nome do Grupo de Patrulha:** Digite o nome do grupo de patrulha para facilitar a pesquisa e gerenciamento não repetitivo.
- **Observações:** Notas de texto do grupo de patrulha.

6.6.1.2 Adicionar Usuário ao Grupo de Patrulha

Na lista de grupos de patrulha, clique no botão para inserir e selecionar para adicionar membros do grupo.



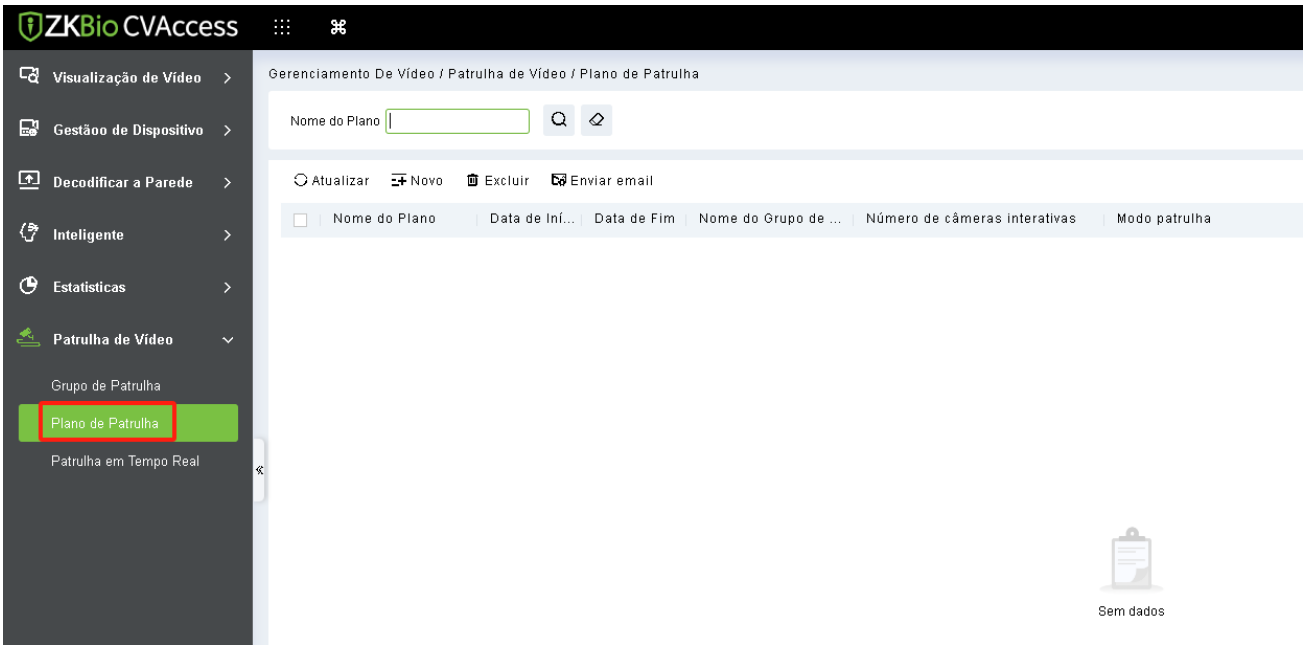
Selecione os usuários de patrulha necessários e clique no botão **[OK]** para completar a adição. Os usuários adicionados serão exibidos na lista de membros do grupo à direita.

Observação: Os usuários de patrulha são usuários do sistema. Para adicionar usuários ao sistema, consulte a adição de usuários.

6.6.2 Plano de Patrulha

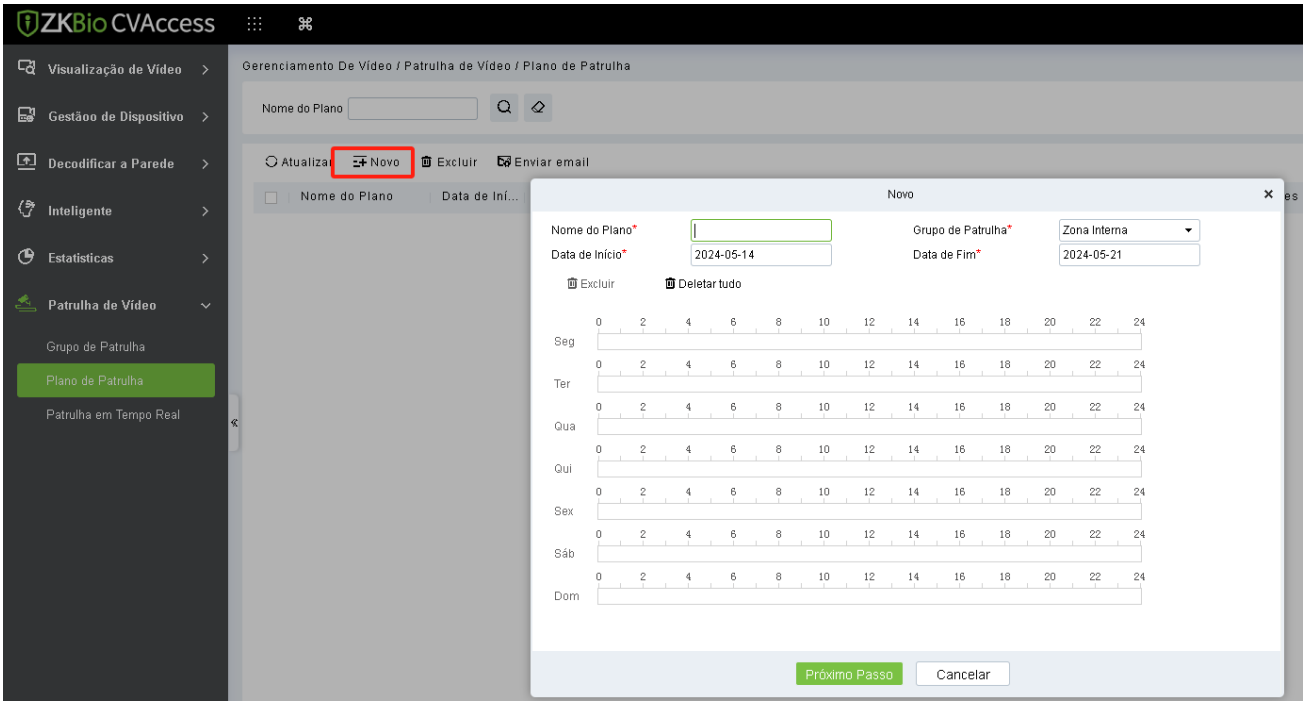
Defina um plano de patrulha para a equipe de patrulha.

Clique em **[Smart Video Surveillance]** > **[Patrulha de Vídeo]** > **[Plano de Patrulha].**



6.6.2.1 Adicionar Plano de Patrulha

1. Clique em **[Novo].**

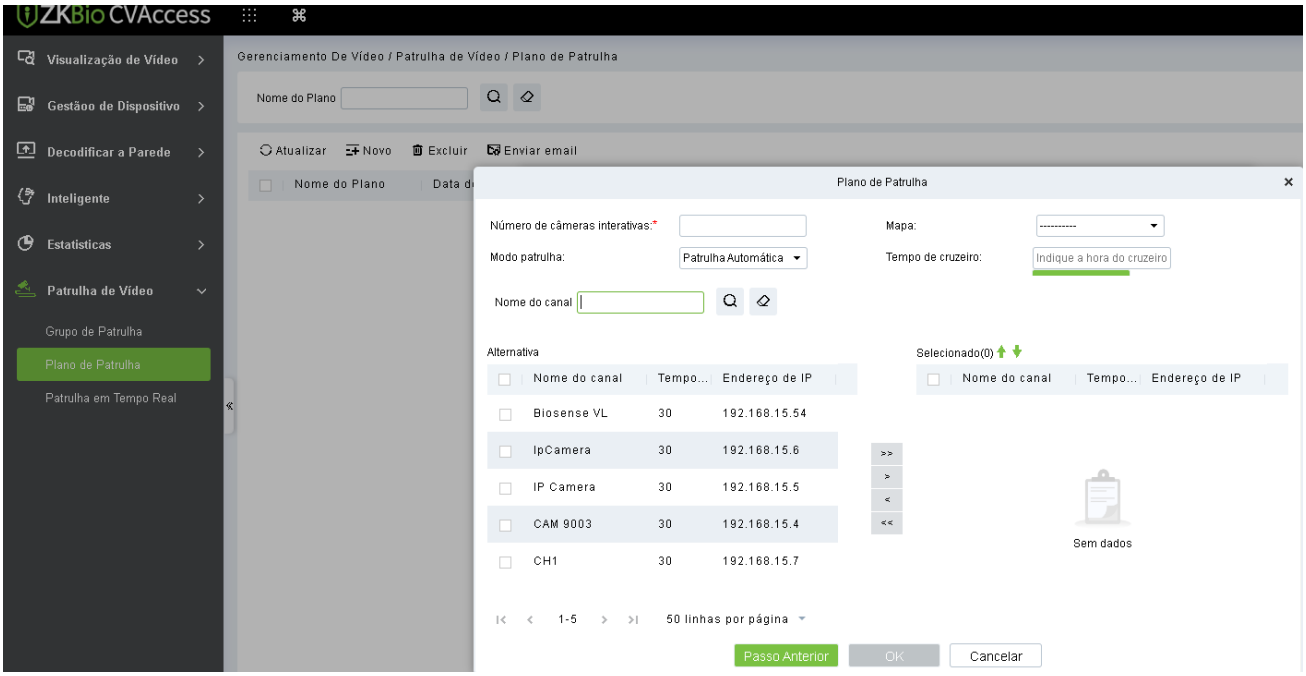


Descrição dos Campos:

- **Nome do Plano:** Dê um nome ao plano para facilitar a visualização e localização, não repetível.
- **Grupo de Patrulha:** Grupo de patrulha opcional criado.

- **Data de Início:** Defina a data de início da patrulha. A data de início não pode ser menor que a data de término.
- **Data de Término:** Defina a data de término da patrulha. A data de início não pode ser menor que a data de término.
- **Tempo de Patrulha:** Arraste a barra de tempo para selecionar o período que precisa ser patrulhado. Múltiplas cópias são suportadas.

2. Após editar esta página, clique em [Próximo] para entrar na interface de seleção de câmera.



Descrição dos Campos:

- **Número de Câmeras Interativas:** Defina o número de câmeras que precisam ser verificadas (por exemplo, "5" significa que a verificação deve ser concluída em 5 câmeras durante este plano de patrulha, esse número deve ser menor ou igual ao número de câmeras escolhidas)
- **Nome do Canal:** Pesquise o canal
- **Lista de Dispositivos:** Selecione o equipamento no mapa que precisa ser patrulhado. A lista de dispositivos mostra apenas os dispositivos que foram adicionados ao mapa atual, se desejar adicionar um dispositivo, vá para Adicionar Dispositivo
- **Mapa:** Selecione o mapa que precisa ser patrulhado.

Nota:

1) Você pode definir o tempo que precisa observar cada câmera clicando no tempo de patrulha, que é de 30 segundos por padrão.
2) A câmera usada no plano de patrulha precisa ser adicionada no centro do mapa.

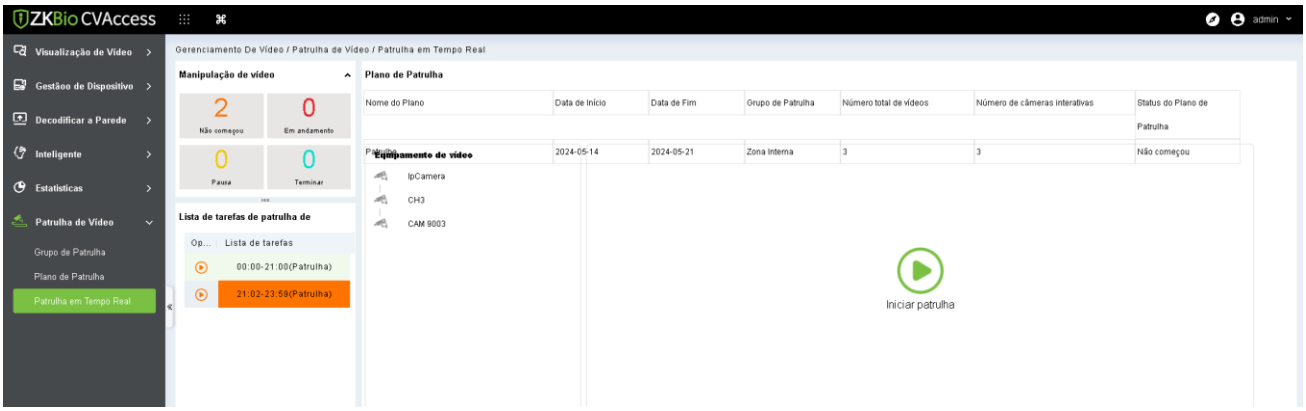
6.6.2.2 Excluir Plano de Patrulha

Selecione o plano de patrulha a ser excluído e clique no botão [Excluir].

Nota: Planos em andamento ou pausados não podem ser excluídos, por favor, conclua o plano primeiro.

6.6.3 Patrulha em Tempo Real

Clique em **[Vídeo Patrulha] > [Plano de Patrulha]**. As patrulhas online estão disponíveis apenas se o patrulheiro estiver logado no sistema.



➢ Operação de Vídeo

Visualize diferentes estados do plano de patrulha.

➢ Lista de Tarefas de Patrulha de Hoje

Exibindo o plano de patrulha, clique para patrulhar.

➢ Plano de Patrulha

Após clicar em [Iniciar Patrulha], a patrulha em vídeo começará. O mapa mostrará todas as câmeras na rota de patrulha, conforme mostrado na figura abaixo:

Nota:

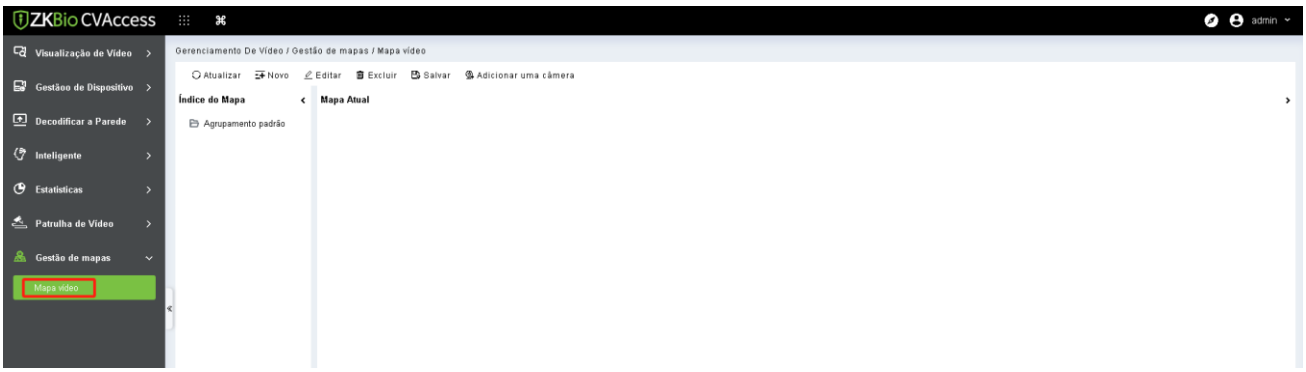
1) Você precisa adicionar uma câmera no centro do mapa antecipadamente.
2) Os pontos das câmeras na lista estão conectados no mapa para formar uma rota de patrulha.
3) Um ponto vermelho em uma câmera indica uma câmera em patrulha.

➢ Janela de Patrulha

Quando a câmera estiver em patrulha, a janela flutuante no mapa exibirá imagens em tempo real.

6.7 Gerenciamento de Mapas

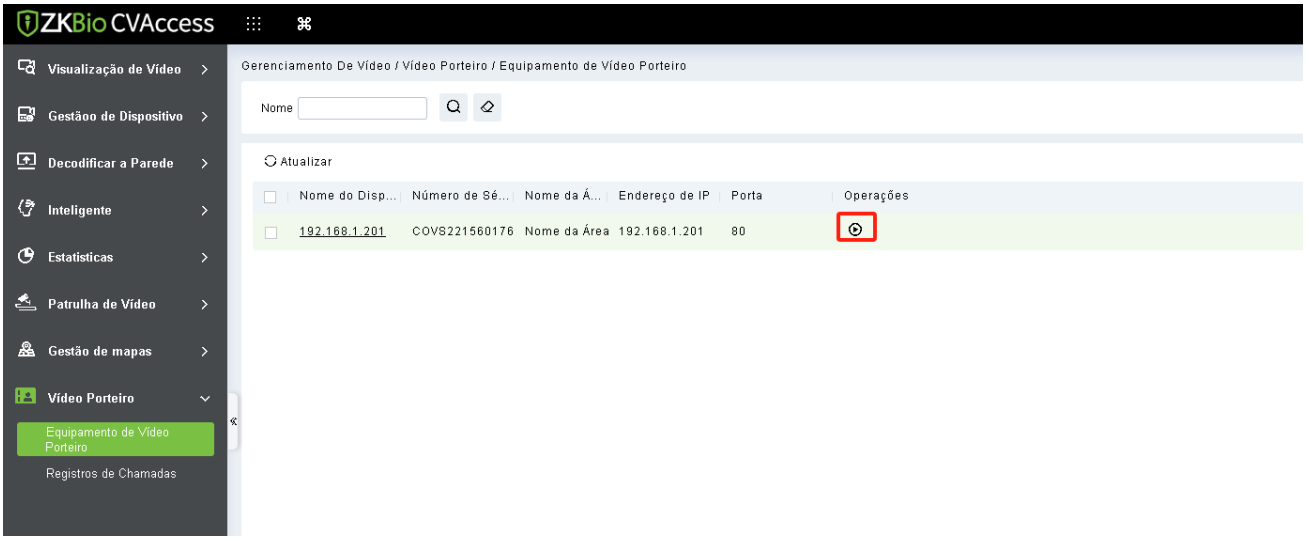
Clique em [**Smart Video Surveillance**] > [**Gerenciamento de Mapas**]. Clique em **[Novo]** para adicionar um E-mapa, em seguida, você pode clicar em **[Adicionar Câmera].** Adicione as câmeras ao mapa, depois ajuste a posição e **[Salvar posição].**



6.8 Intercomunicador de Vídeo

6.8.1 Dispositivo de Intercomunicador de Vídeo

1. Adicionar Dispositivos de Controle de Acesso. Vá para o Módulo de Controle de Acesso, pesquise e adicione dispositivos.
2. Após adicionar, o dispositivo será automaticamente adicionado a **[Smart Video Surveillance] > [Intercomunicador de Vídeo] > [Dispositivo de Intercomunicador de Vídeo],** e você pode fazer uma Prévia.



3. Quando alguém pressiona o botão da campainha no dispositivo, a plataforma automaticamente exibe a interface de chamada. Você pode clicar para atender.

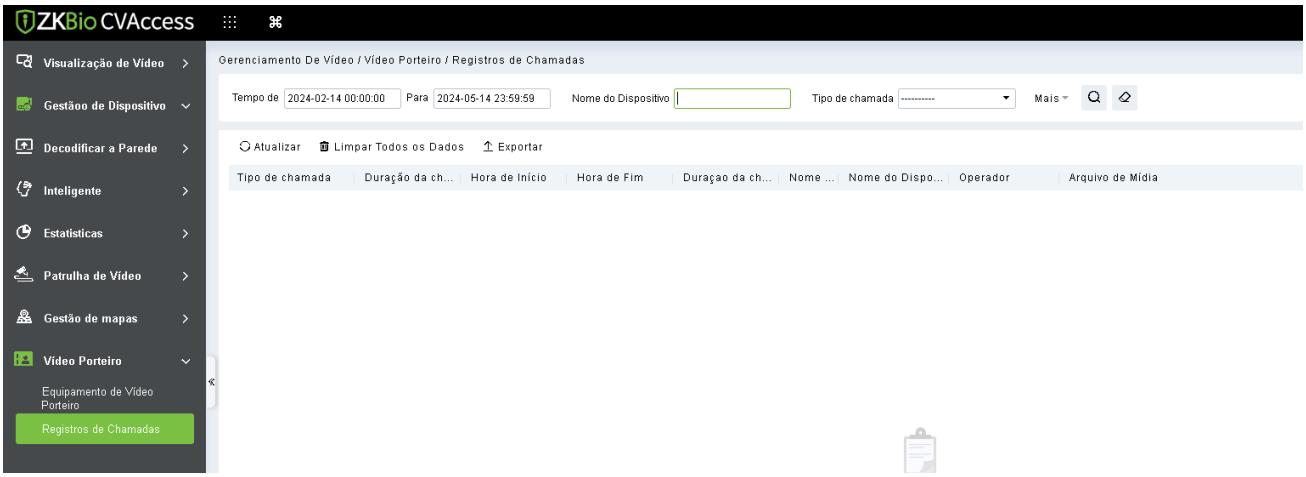
: Capturar uma captura de tela e aparecerá a notificação abaixo.

: Encerrar a chamada

: Abrir a porta.

6.8.2 Registros de Chamadas

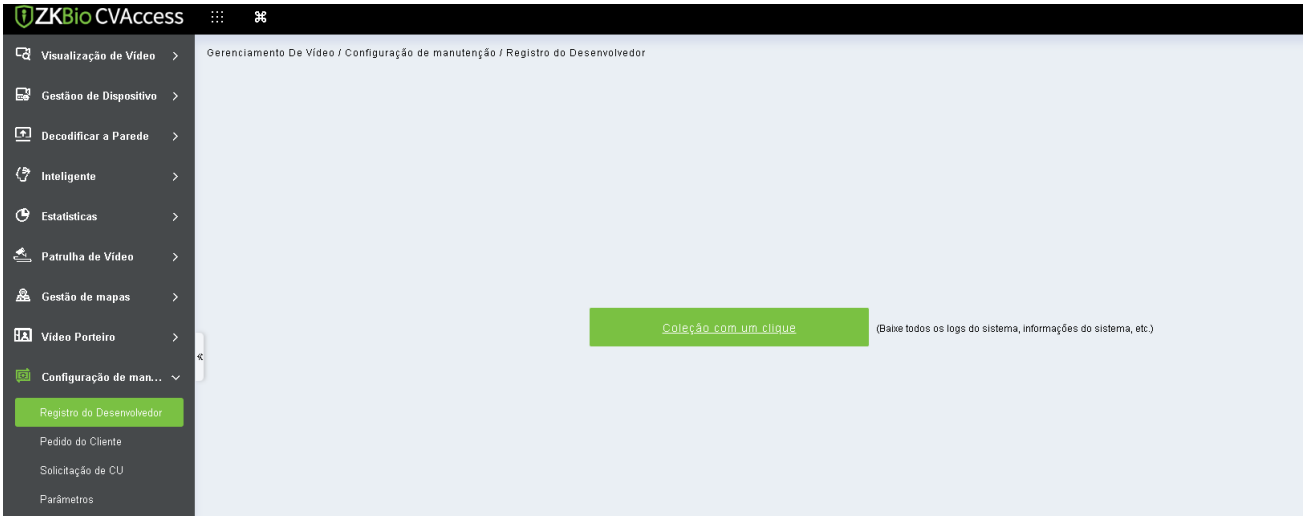
Clique em **[Smart Video Surveillance]** > **[Intercomunicador de Vídeo]** > **[Registros de Chamadas]**, você pode visualizar o relatório e ver um registro de todas as respostas, você pode exportar os relatórios via excel/pdf/CVS/txt.



6.9 Configuração de Manutenção

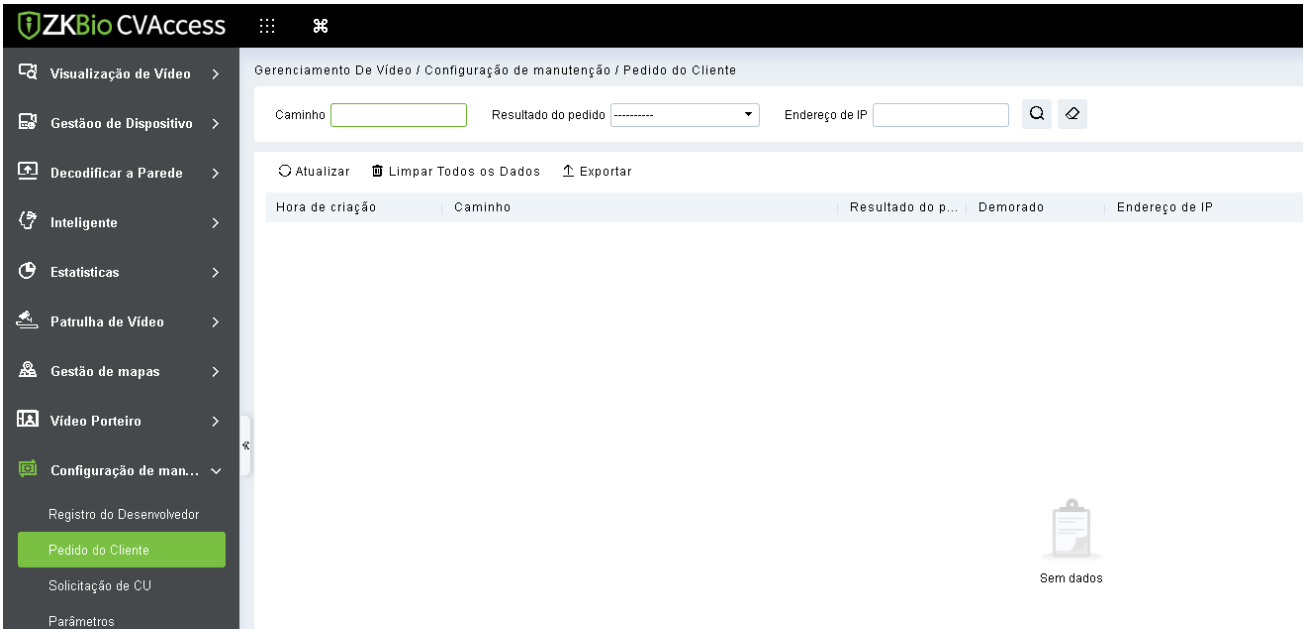
6.9.1 Log do Desenvolvedor

Clique em **[Smart Video Surveillance]** > **[Configuração de Manutenção]** > **[Log do Desenvolvedor]**, em seguida, clique em **[Coleta em Um Clique]** para baixar todos os logs do sistema e informações do sistema.



6.9.2 Log de Solicitações do Cliente

Clique em **[Smart Video Surveillance] > [Configuração de Manutenção] > [Log de Solicitações do Cliente].**



➢ Limpar Todos os Dados

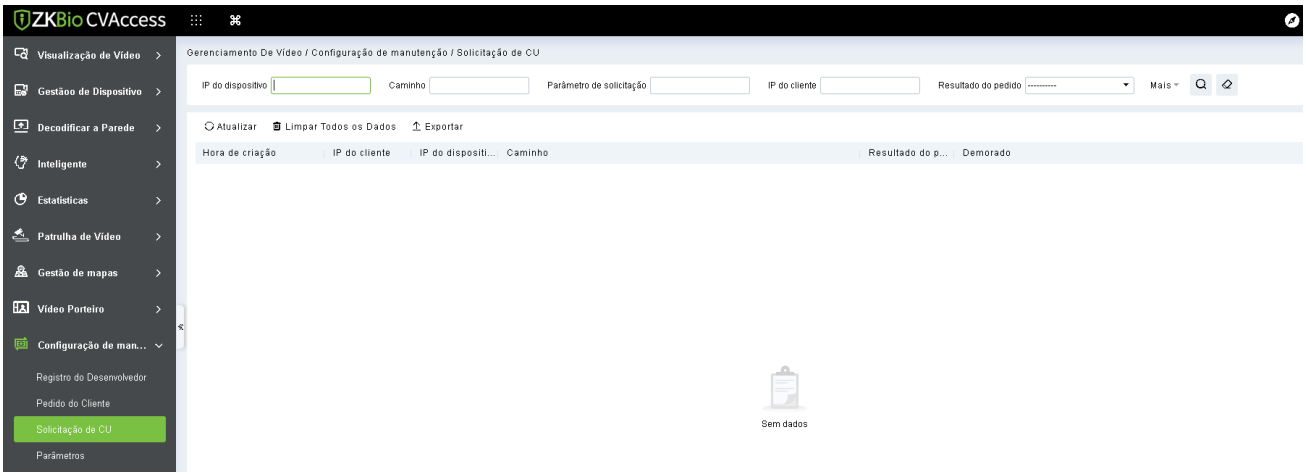
Clique **em [Limpar Todos os Dados]** para abrir o prompt e clique em **[OK]** para limpar todas as operações de dados.

➢ Exportar

Exportar informações de pessoal selecionadas na área; você pode exportar em formato Excel, PDF, CSV.

6.9.3 Solicitação de CU

Clique em **[Smart Video Surveillance] > [Configuração de Manutenção] > [Solicitação de CU].**



➢ Limpar Todos os Dados

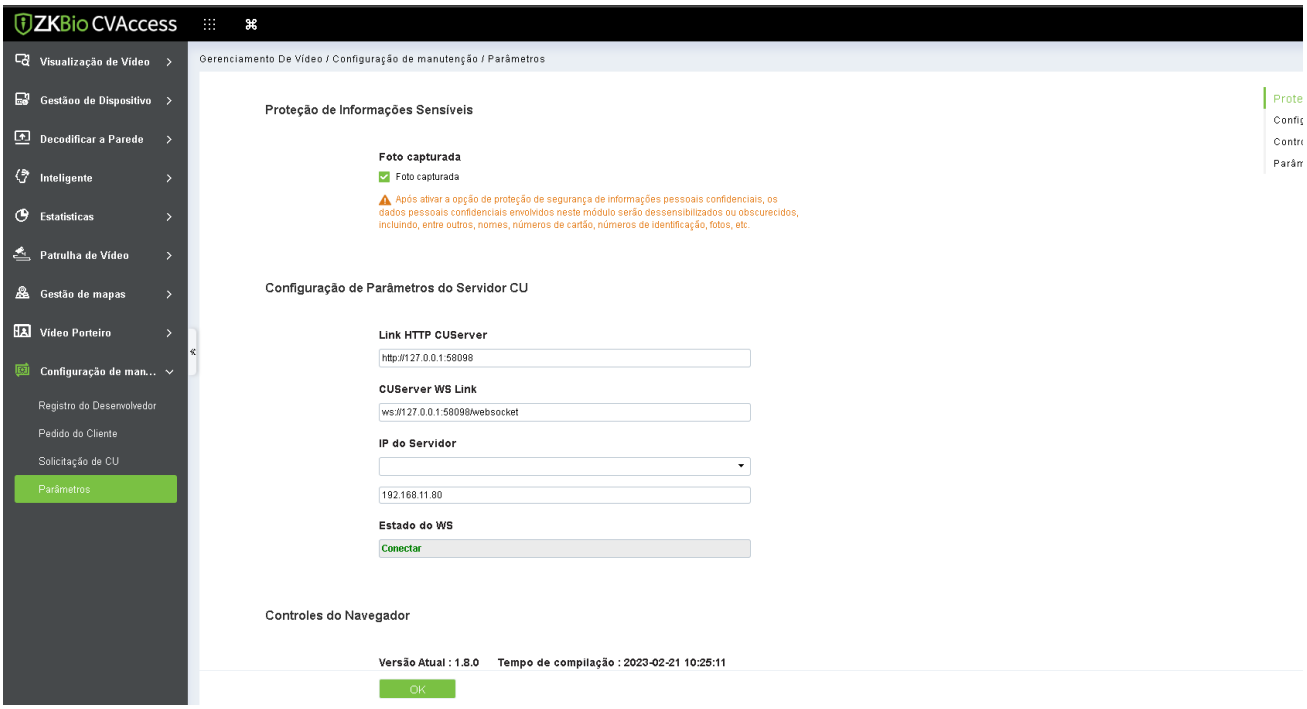
Clique em **[Limpar Todos os Dados]** para abrir o prompt e clique em **[OK]** para limpar todas as operações de dados.

➢ Exportar

Exportar informações de pessoal selecionadas na área; você pode exportar em formato Excel, PDF, CS

6.9.4 Parâmetros

Clique em [**Smart Video Surveillance] > [Configuração de Manutenção] > [Parâmetros].** Configure todas as configurações e depois clique em **[OK].**

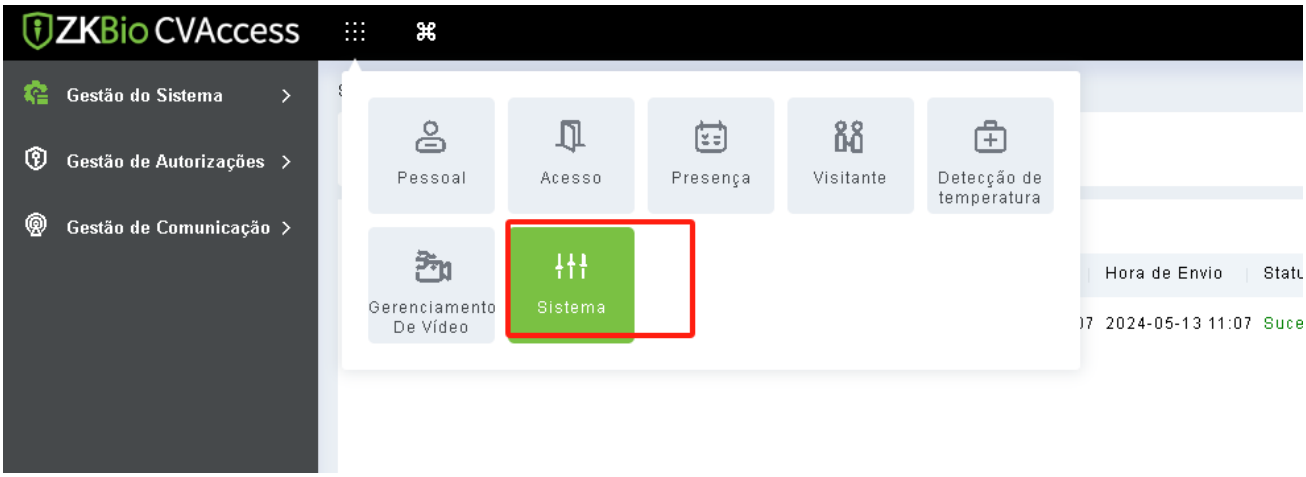


Descrição dos Campos:

- **Configurações de Parâmetros do Servidor CU:** Configure o URL HTTP do servidor CU e o URL WS e insira o endereço IP do servidor para visualizar o estado do WS.
- **Controles do Navegador:** Configure o local de armazenamento de arquivos e altere e restaure o caminho.
- **Configurações de Parâmetros de Log:** Configure o log de depuração e o log de acesso e selecione Sim/Não.

7 Sistema

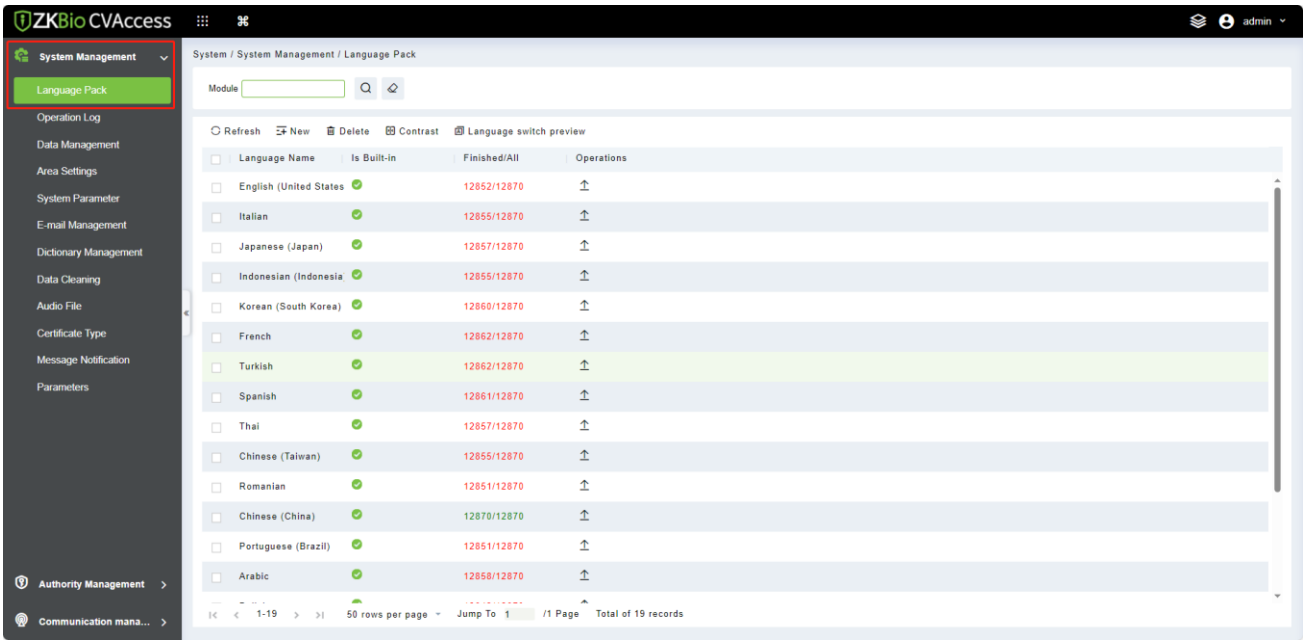
As configurações do sistema incluem principalmente atribuir usuários do sistema (como usuário de gerenciamento da empresa, administrador e administrador de controle de acesso) e configurar os papéis dos módulos correspondentes, gerenciar o banco de dados, configurar parâmetros do sistema e visualizar logs de operação, etc.



7.1 Gerenciamento de Sistema

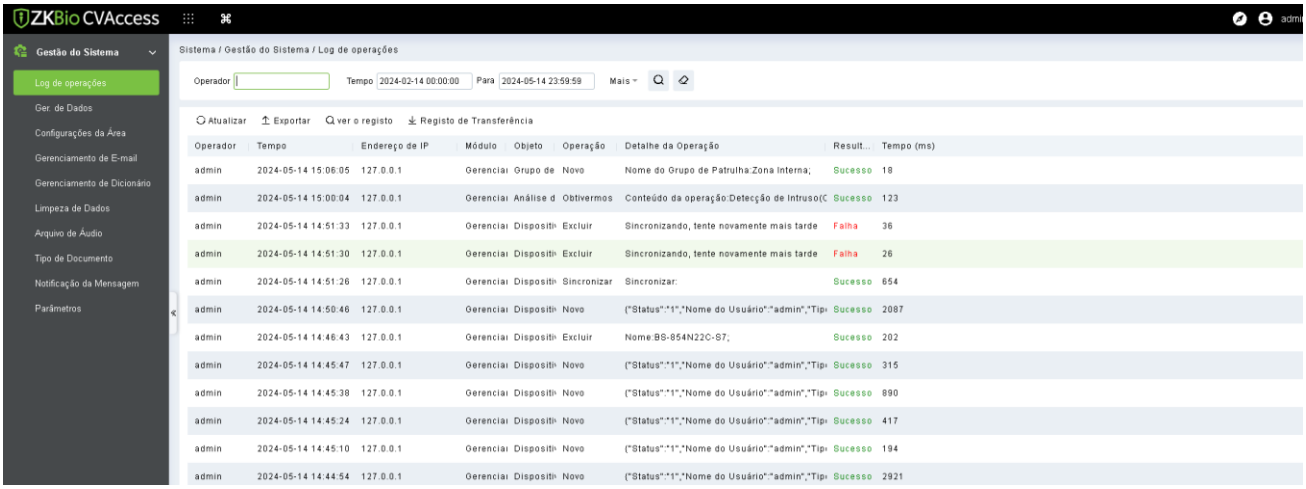
7.1.1 Pacote de Idiomas

Clique em **[Sistema]** > **[Gerenciamento de Sistema]** > **[Pacote de Idiomas].**



7.1.2 Logs de Operação

Clique em **[Sistema]** > **[Gerenciamento de Sistema]** > **[Log de Operação].**



Todos os logs de operações são exibidos nesta página. Você pode consultar logs específicos por condições.

➢ **Exportar**

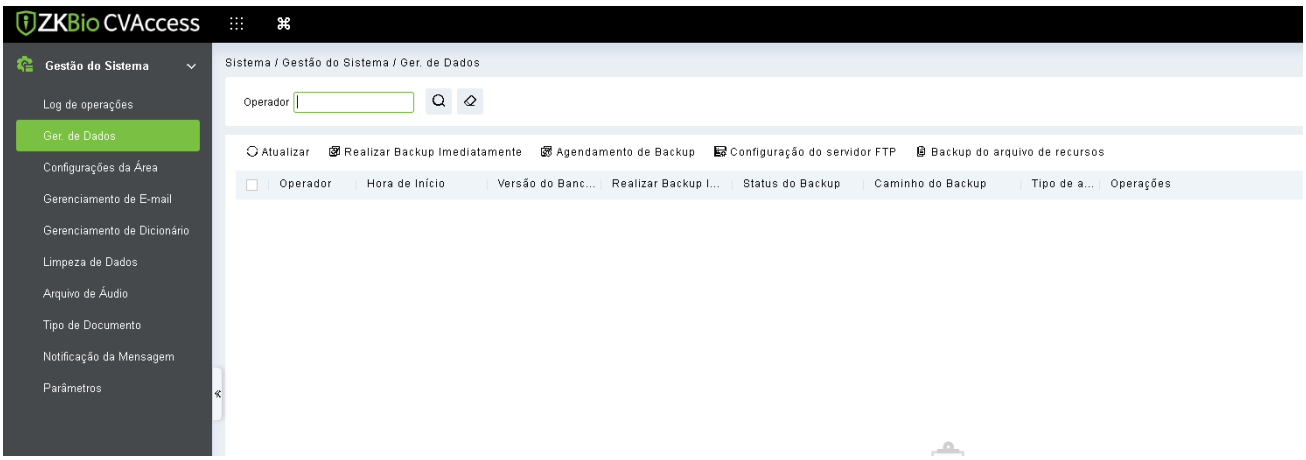
Você pode exportar dados selecionados em formato Excel, PDF e CSV.

Operation Log

Operation User	Operation Time	Operation IP	Module	Operating Object	Operation Type	Operation Content	Result	Elapsed Time (Milliseconds)
admin	2018-12-28 02:41:46	172.31.1.10	Access	Access Rights By Personnel	Export	Export	0	15
admin	2018-12-28 02:41:45	172.31.1.10	Access	Access Rights By Personnel	Export	Export	0	13
admin	2018-12-28 02:41:43	172.31.1.10	System	User	User Login	User Login:admin;	0	0
admin	2018-12-28 02:36:19	172.31.1.10	Access	Access Rights By Door	Export	Export	0	16
admin	2018-12-28 02:36:18	172.31.1.10	Access	Access Rights By Door	Export	Export	0	19
admin	2018-12-28 02:28:10	172.31.1.10	Access	All Exception Events	Export	Export Failed	1	20016
admin	2018-12-28 02:28:11	172.31.1.10	Access	All Exception Events	Export	Export	0	1234
admin	2018-12-28 02:22:07	172.31.1.10	Access	Last Known Position	Export	Export	0	15
admin	2018-12-28 02:22:06	172.31.1.10	Access	Last Known Position	Export	Export	0	26
admin	2018-12-28 02:14:15	172.31.1.10	Access	All Transactions	Export	Export Failed	1	42014
admin	2018-12-28 02:14:19	172.31.1.10	Access	All Transactions	Export	Export	0	4970

7.1.3 Gerenciamento de Banco de Dados

Clique em **[Sistema] > [Gerenciamento de Sistema] > [Gerenciamento de Banco de Dados].**



O histórico de logs de operações de backup do banco de dados é exibido nesta página. Você pode atualizar, fazer backup e programar o backup do banco de dados conforme necessário.

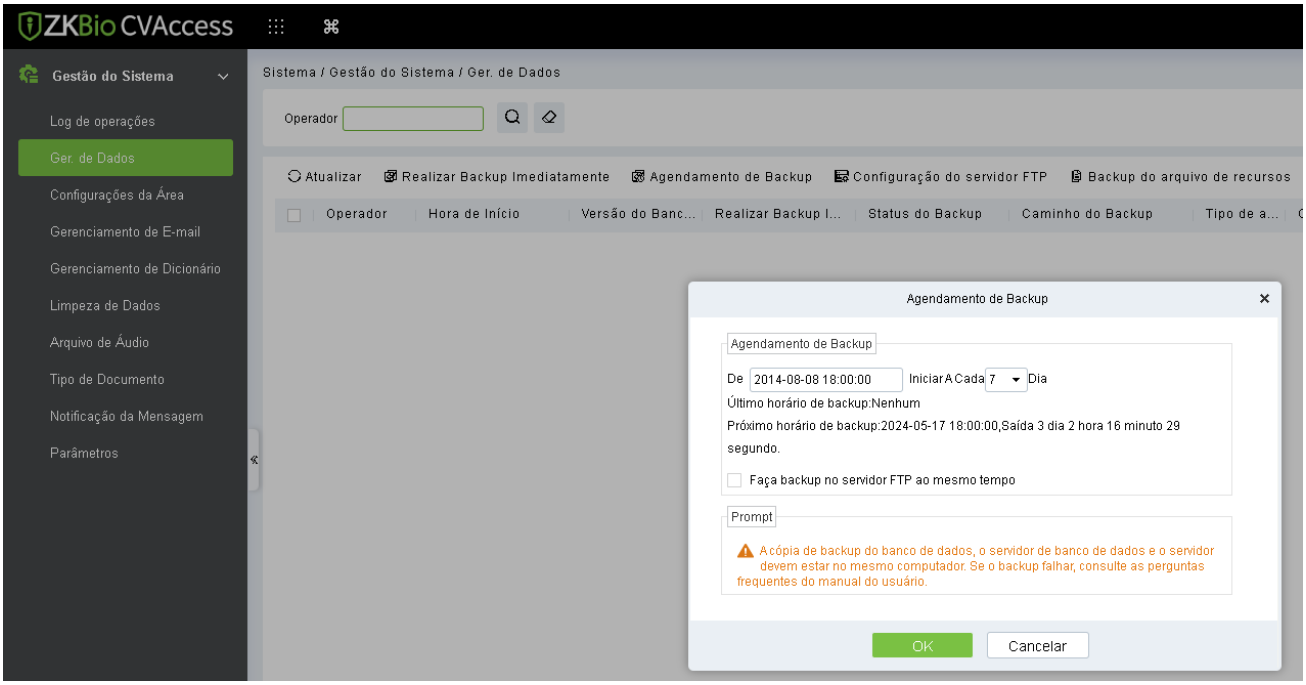
➢ Backup Imediato

Faça o backup do banco de dados no caminho definido na instalação agora mesmo.

Nota: O caminho de backup padrão para o sistema é o caminho selecionado durante a instalação do software. Para mais detalhes, consulte o Guia de Instalação do ZKBio CVAccess.

➢ Programar Backup

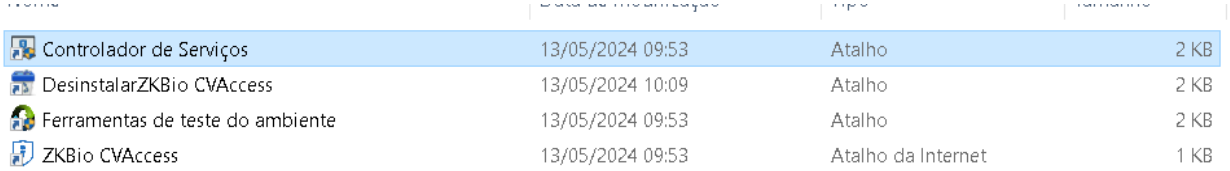
Clique em [Backup Programado].

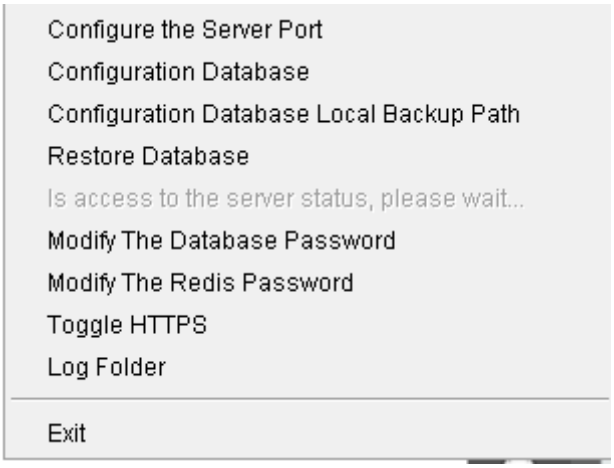


Defina o horário de início, o intervalo entre dois backups automáticos e clique em [OK].

➢ Restaurar Banco de Dados

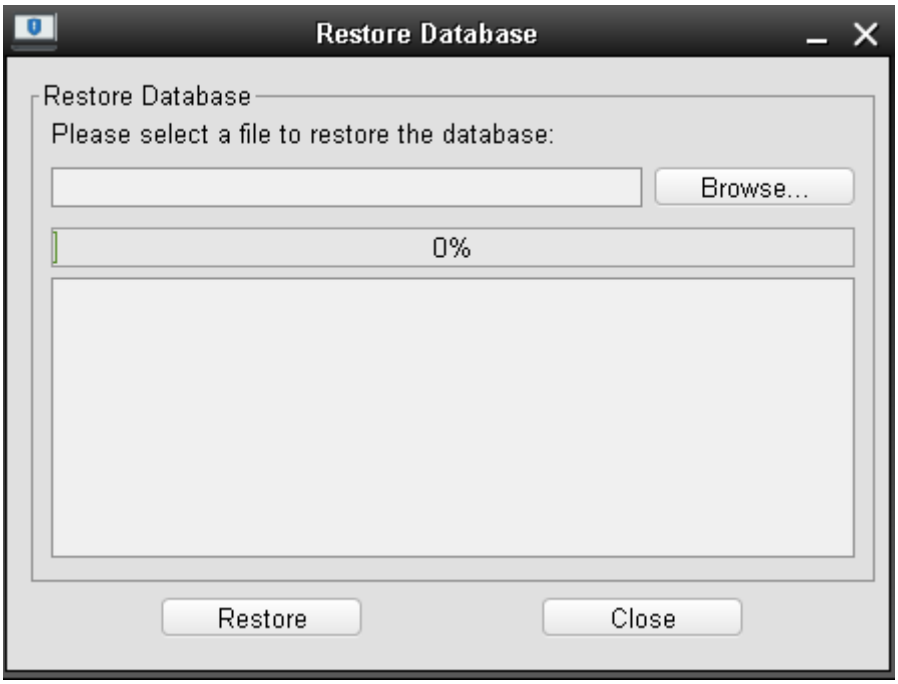
1. Clique no menu iniciar do PC > [Todos os Programas] > [ZKBio CVAccess] > Em seguida, execute o "Controlador de Serviços", e você pode encontrar o ícone do "Controlador de Serviços" na barra de tarefas como a seguir, clique com o botão direito do mouse nesse ícone e, em seguida, clique em "Restaurar Banco de Dados".





2. Na janela pop-up, clique em [Procurar] para escolher o arquivo de backup para restaurar o banco de dados.

Nota: Antes de restaurar um banco de dados, é recomendável fazer o backup do banco de dados atual para evitar a perda de dados.



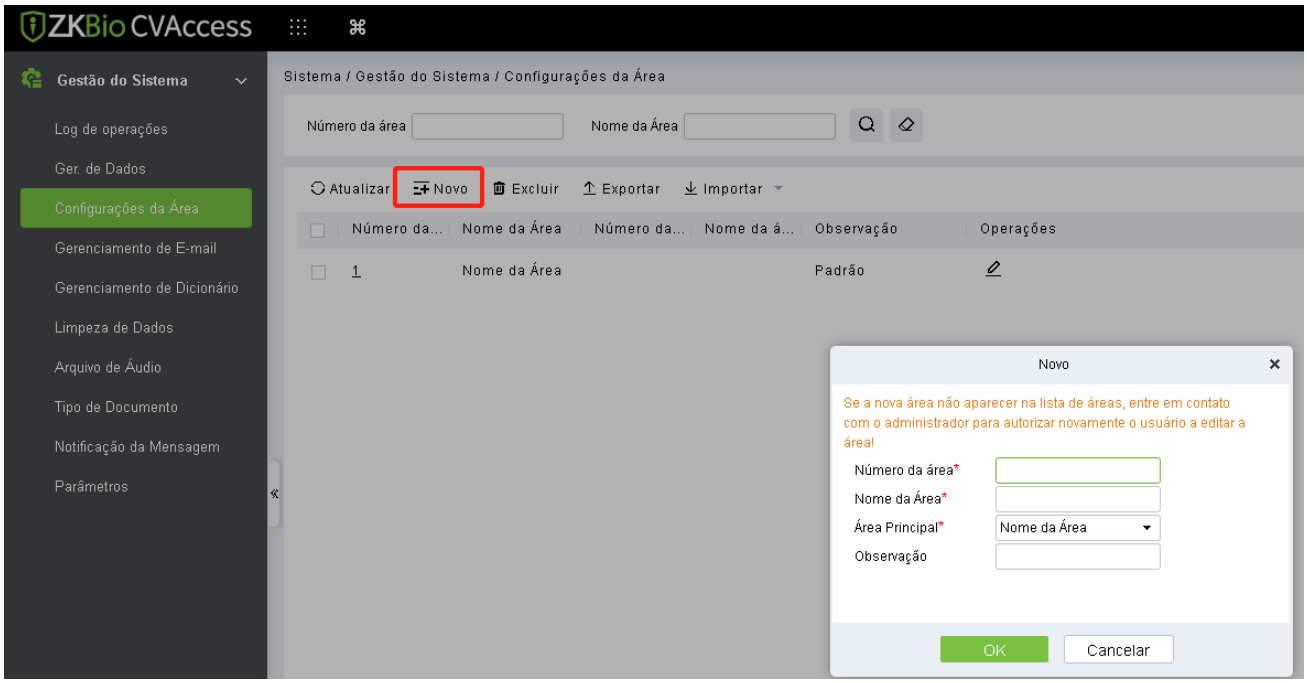
7.1.4 Configurações de Área

A área é um conceito espacial que permite ao usuário gerenciar dispositivos em uma área específica. Após a configuração da área, os dispositivos (portas) podem ser filtrados por área durante o monitoramento em tempo real.

Clique em **[Sistema] > [Gerenciamento de Sistema] > [Configurações de Área].** O sistema, por padrão, tem uma área chamada "Nome da Área" e numerada "1".

➢ **Adicionar uma Área**

1. Clique em [Nova].



Os campos são os seguintes:

- **Número da Área:** Deve ser único.
- **Nome da Área:** Qualquer caractere com comprimento inferior a 30.
- **Área Pai:** Determine a estrutura de área do sistema.

2. Clique em **[OK]** para concluir a adição.

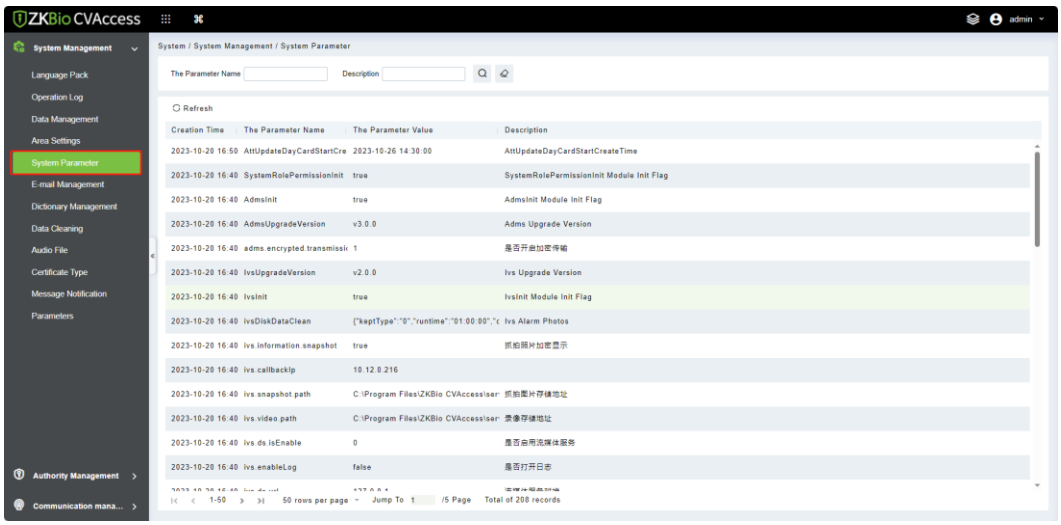
➢ Editar/Excluir uma Área

Clique em **[Editar] ou [Excluir]** conforme necessário.

7.1.5 Parâmetro do Sistema

Essa função é usada para visualizar os parâmetros que foram criados.

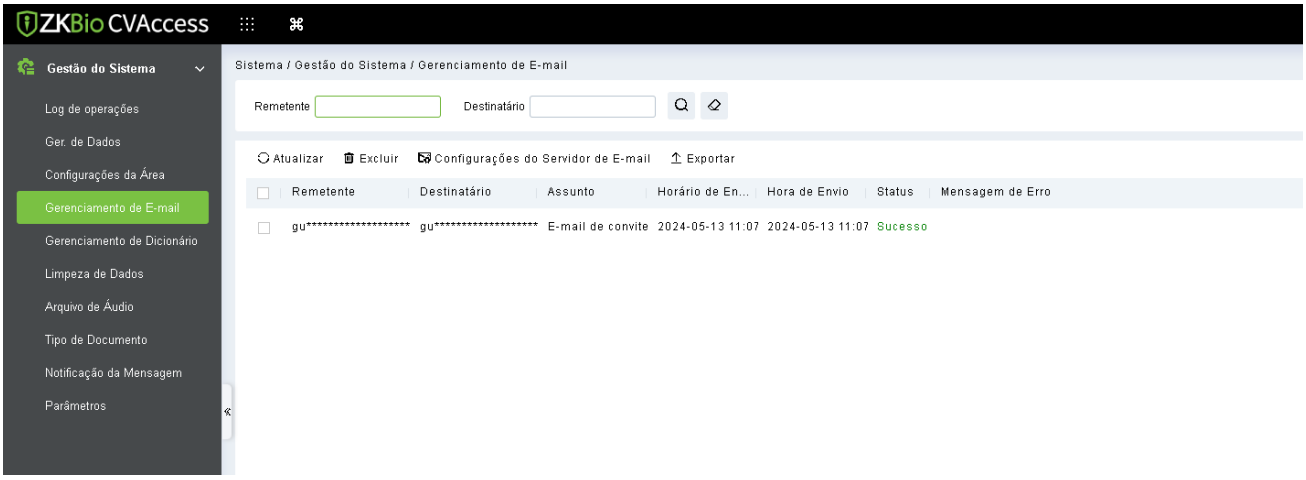
Clique em **[Sistema] > [Gerenciamento de Sistema] > [Parâmetro do Sistema].**



7.1.6 Gerenciamento de E-mail

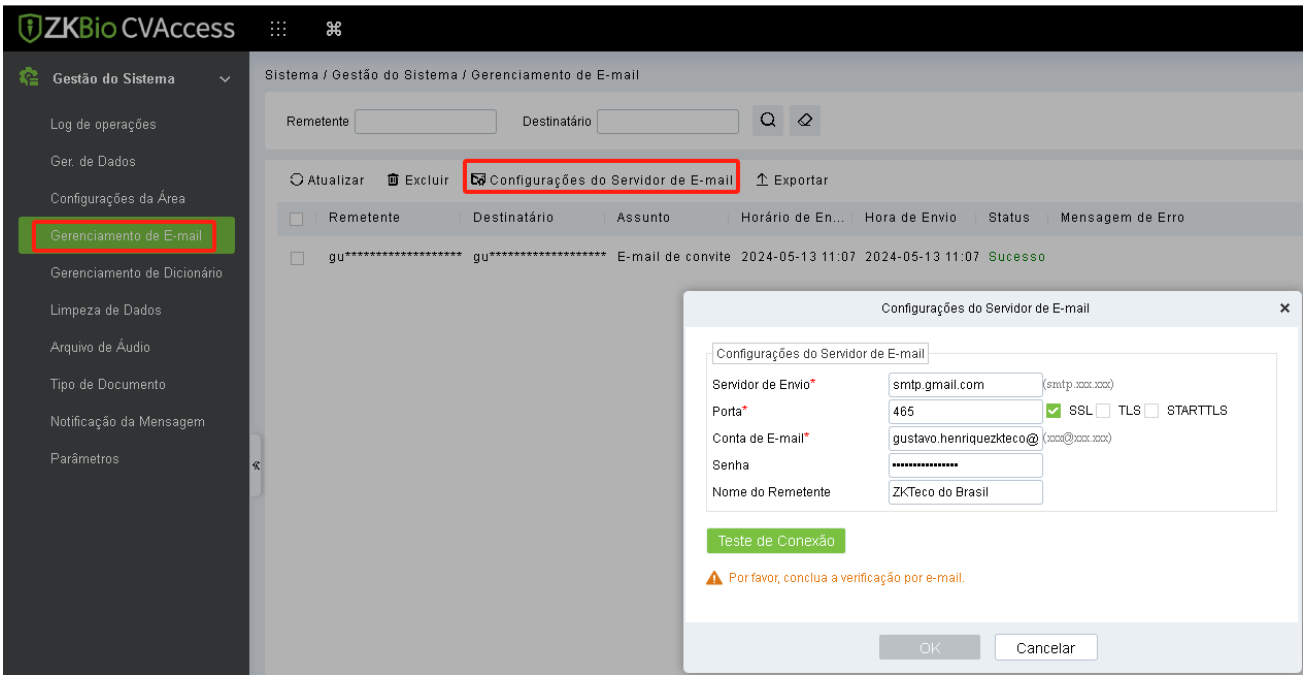
Configure as informações do servidor de envio de e-mails. O e-mail do destinatário deve ser configurado em Linkage.

Clique em **[Sistema] > [Gerenciamento de Sistema] > [Gerenciamento de E-mail].**



➢ Configurações do Servidor de Envio de E-mails

Clique em **[Configurações do Servidor de Envio de E-mails].**

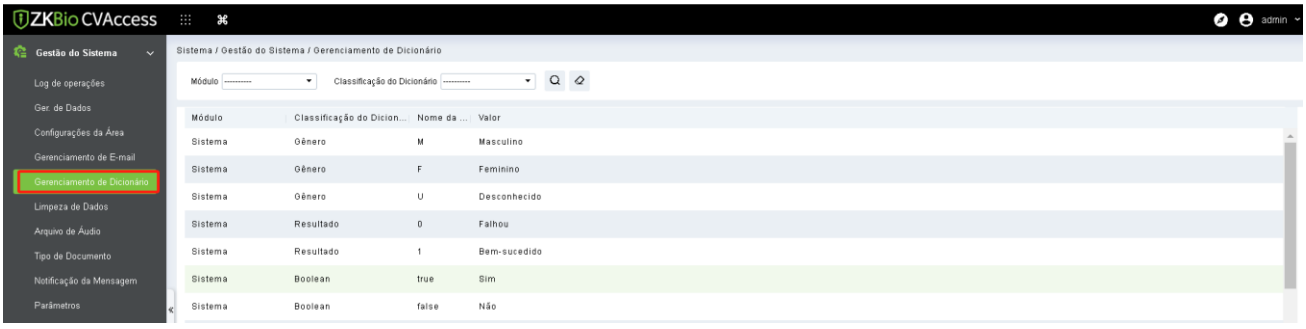


Nota: O nome de domínio do endereço de e-mail e do servidor de envio de e-mails deve ser idêntico. Por exemplo, se o endereço de e-mail for: test@gmail.com, então o servidor de envio de e-mails deve ser: smtp.gmail.com.

7.1.7 Gerenciamento de Dicionário

Função de gerenciamento de dicionário de dados, os usuários podem encontrar o significado do código de erro e verificar erros do software.

Clique em **[Sistema] > [Gerenciamento de Sistema] > [Gerenciamento de Dicionário].**



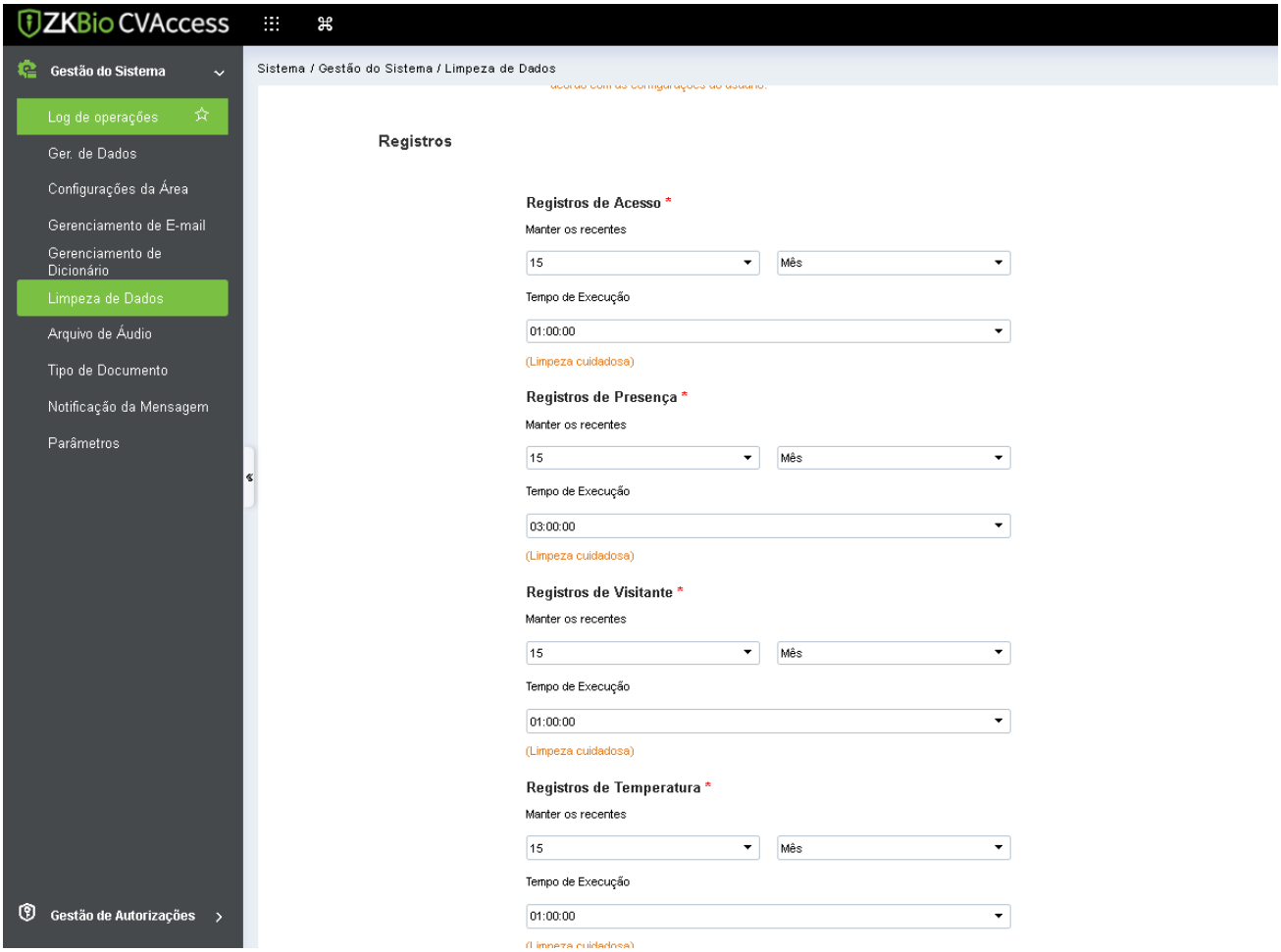
7.1.8 Limpeza de Dados

As configurações de tempo de limpeza de dados estão disponíveis para definir. O volume de dados aumenta com o uso do sistema. Para economizar espaço de armazenamento nos discos, você precisa limpar periodicamente os dados antigos gerados pelo sistema.

Clique em **[Sistema] > [Gerenciamento de Sistema] > [Limpeza de Dados].**

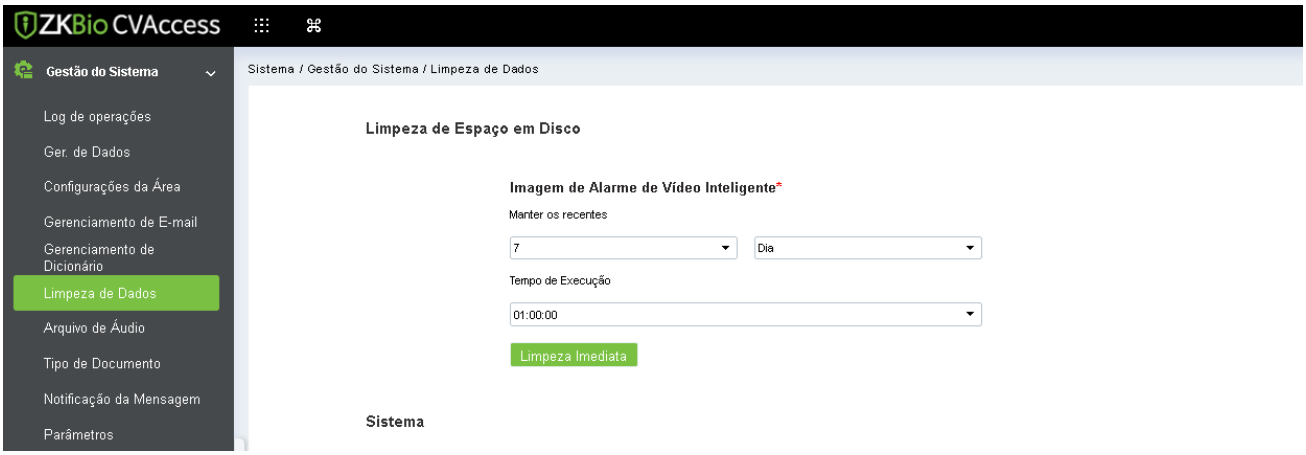
7.1.8.1 Registro

Esta opção ajuda a definir a frequência de retenção dos dados recentes da transação de acesso, transação de presença, transações de elevador e transações de visitantes, etc.



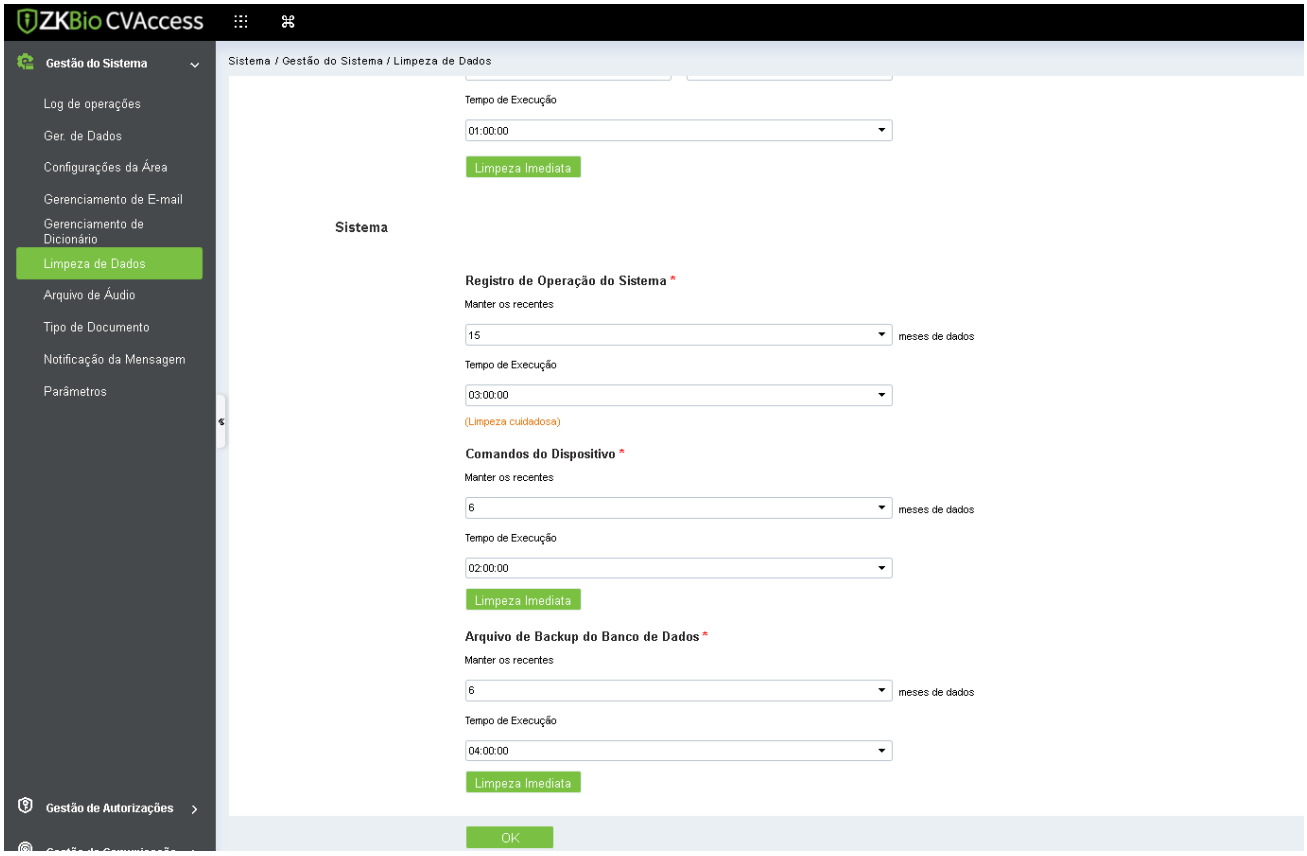
7.1.8.2 Limpeza de Espaço em Disco

Nesta opção, você pode definir a frequência de retenção dos dados recentes e também limpar os dados dos dias selecionados.



7.1.8.3 Sistema

Esta opção ajuda a limpar o log de operações do sistema, comandos de dispositivos e arquivos de backup do banco de dados.



7.1.9 Arquivo de Áudio

Clique em **[Sistema]** > **[Gerenciamento de Sistema]** > **[Arquivo de Áudio].**

➢ **Novo**

1. Clique em **[Novo].**

Os campos são os seguintes:

- **Alias do Arquivo (Nome):** Digite o nome do arquivo. Qualquer caractere, até 30 caracteres.
- **Tamanho:** Após o upload do arquivo, o tamanho do arquivo é gerado automaticamente.
- **Sufixo:** Após o upload do arquivo, o sufixo do arquivo é gerado automaticamente.

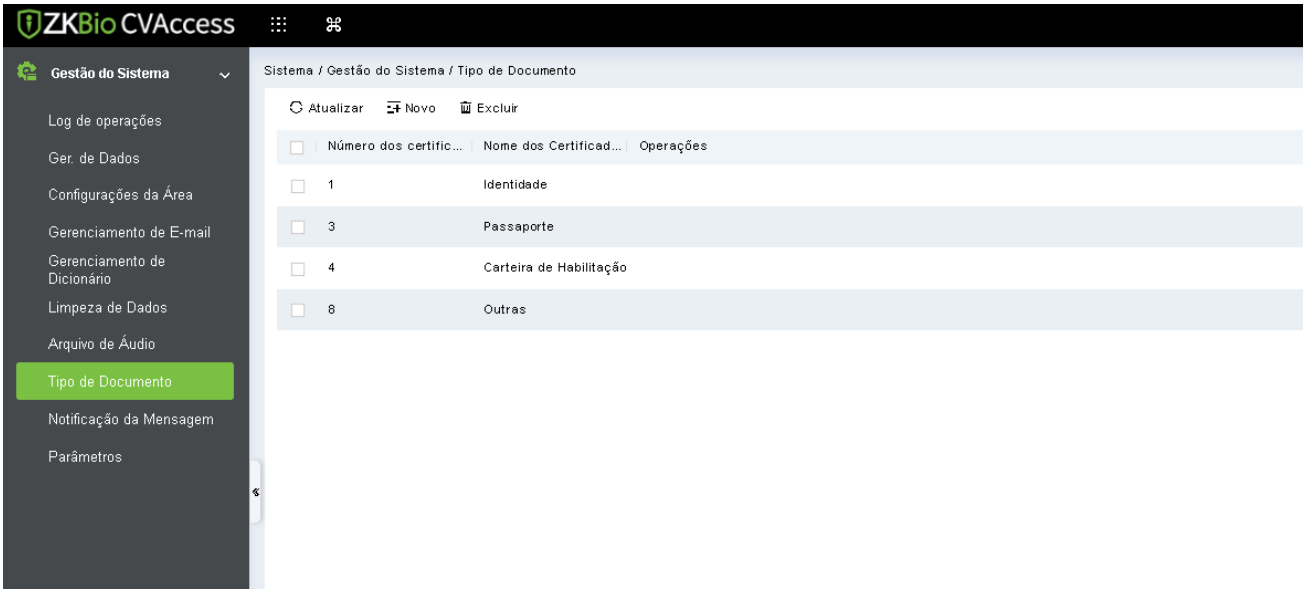
Clique em [OK] para concluir a adição.

Nota: Você pode fazer upload de um som do seu computador. O arquivo deve estar no formato wav ou mp3 e não deve exceder 10MB.

7.1.10 Tipo de Certificado

O sistema inicializa 9 tipos de certificados. O usuário pode adicionar o tipo de certificado necessário para registro de pessoal e visitantes.

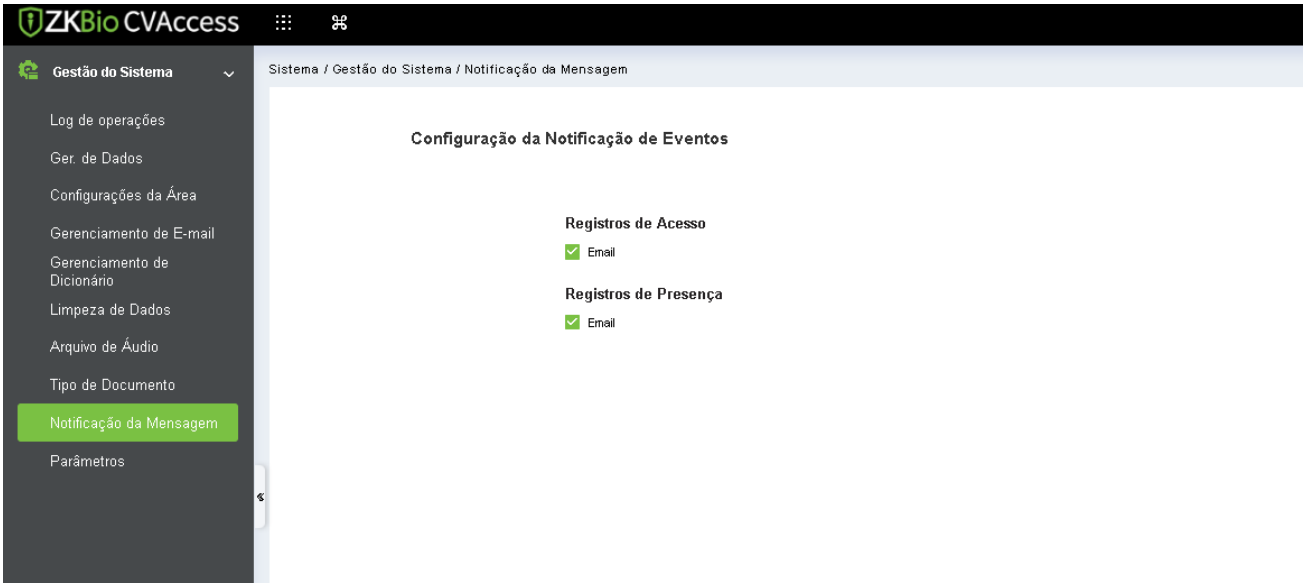
Clique em **[Sistema] > [Gerenciamento de Sistema] > [Tipo de Certificado].**



7.1.11 Notificação de Mensagem

Esta função é usada para abrir/fechar a notificação de eventos de acesso e transação de presença.

Clique em **[Sistema] > [Gerenciamento de Sistema] > [Notificação de Mensagem].**

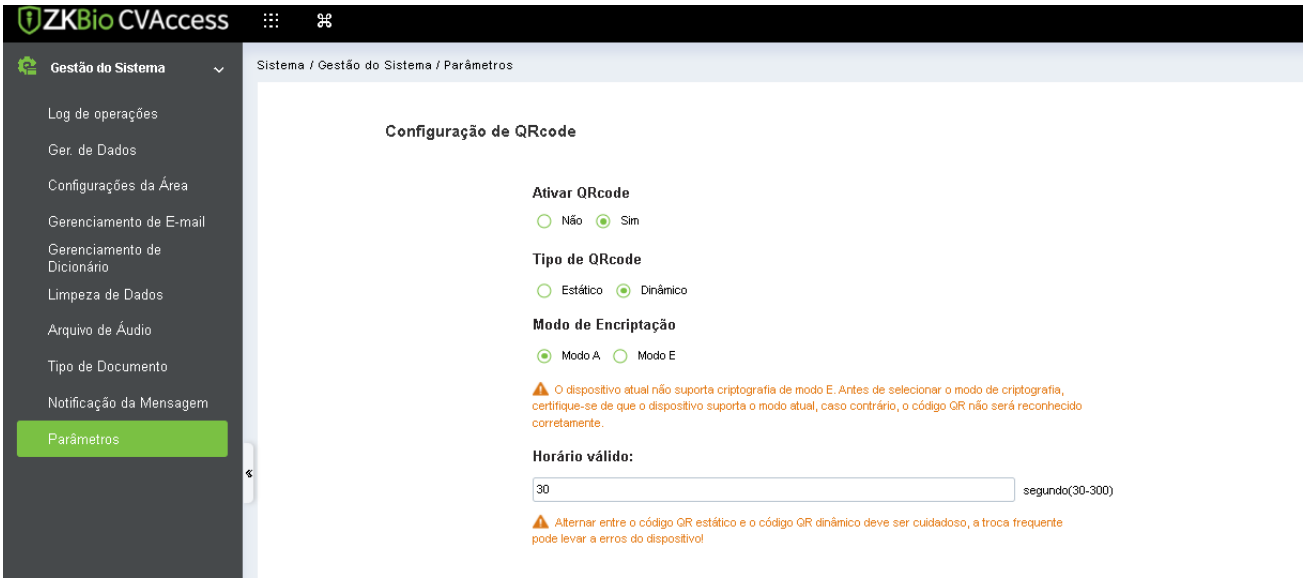


7.1.12 Parâmetros

Clique em **[Sistema] > [Gerenciamento de Sistema] > [Parâmetros].**

7.1.12.1 Configuração de QR Code

1. Ative o QR code, selecione "SIM" ou "NÃO" para Ativar o QR code.
2. Ative o QR code Se SIM, selecione "SIM > Estático". Ele fixará as informações do QR da mesma maneira para o resto do tempo.
3. Ative o QR code Se SIM, selecione "SIM > Dinâmico > Tempo de Validade". Ele gerará um novo QR code a cada 30 segundos.

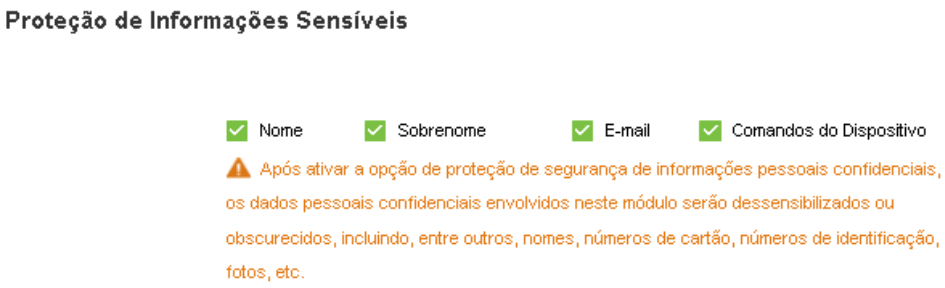


7.1.12.2 Marca d'água em Vídeo

Esta opção ajuda você a adicionar marca d'água e título aos seus vídeos.

7.1.12.3 Proteção de Informações Sensíveis Pessoais

Após ativar a opção de proteção de segurança de informações pessoais sensíveis, os dados pessoais sensíveis envolvidos neste módulo serão desidentificados ou obscurecidos, incluindo, mas não se limitando a nomes, números de cartão, números de identificação, fotos, etc.



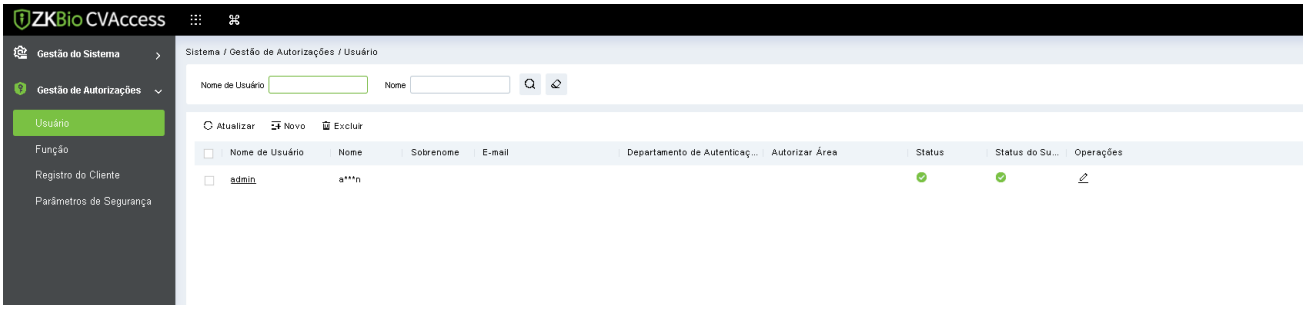
7.1.13 Política de Privacidade

Clique em [Visualizar] para ver a política de privacidade.

7.2 Gerenciamento de Autoridade

7.2.1 Usuário

Adicione novos usuários e implemente níveis para o usuário no sistema. Clique em **[Sistema] > [Gerenciamento de Autoridade] > [Usuário].**



➢ **Novo**

1. Clique em **[Sistema] > [Gerenciamento de Autoridade] > [Usuário] > [Novo].**

Os campos são os seguintes:

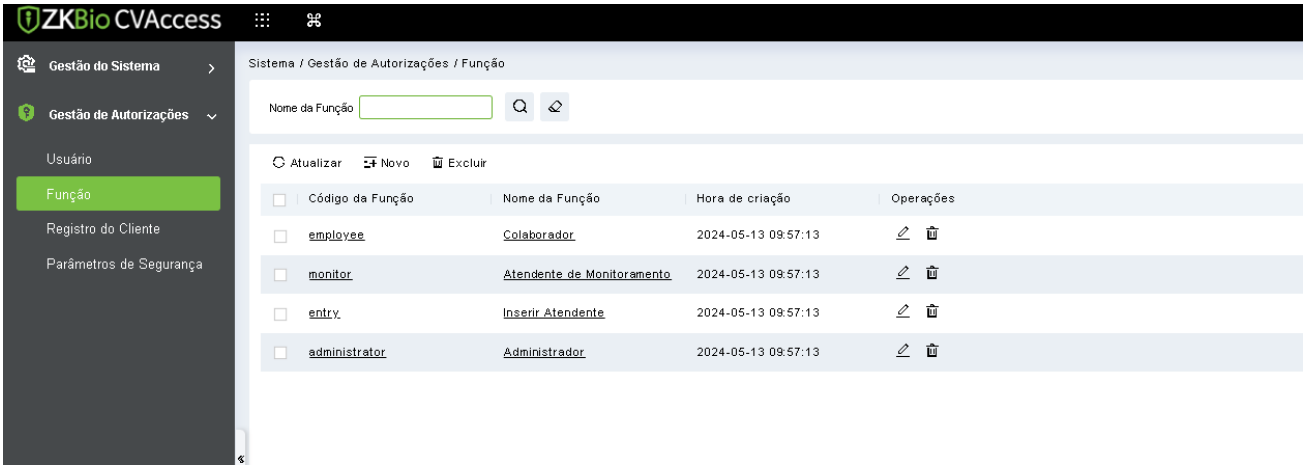
- **Nome de Usuário:** Qualquer caractere com comprimento de até 30 caracteres.
- **Senha:** O comprimento deve ser superior a 4 dígitos e inferior a 18 dígitos. A senha padrão é 111111.
- **Estado:** Ative ou desative o usuário para operar o sistema.
- **Estado de Super Usuário:** Ative ou desative o usuário para ter os níveis de super usuário.
- **Função:** Você precisa definir a função conforme explicado em Função.
- **Departamento Autorizado:** Se nenhum departamento for selecionado, o usuário terá todos os direitos do departamento por padrão.
- **Área Autorizada**: Nenhuma área selecionada significa que o usuário possui todos os direitos da área por padrão.
- **Email:** Digite seu email no formato correto.
- **Primeiro Nome:** Digite suas iniciais.

2. Após editar, clique em **[OK]** para completar a adição do usuário, e o usuário será mostrado na lista.

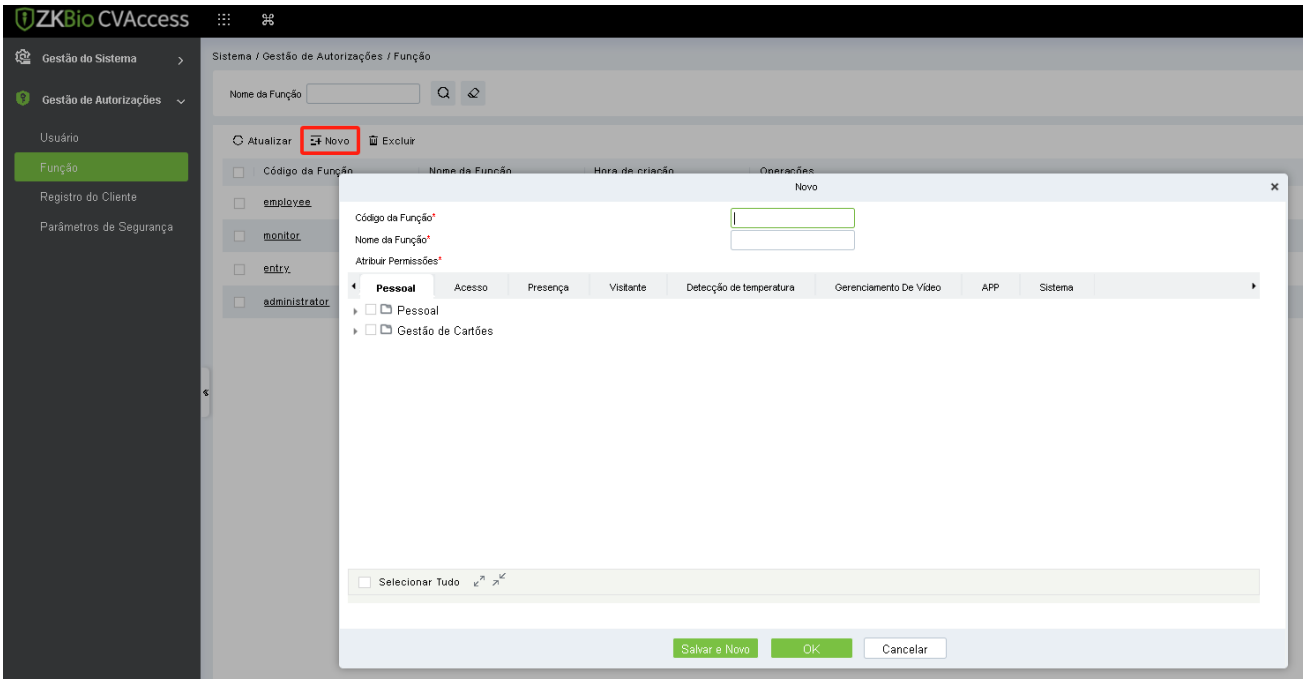
7.2.2 Função

Ao usar o sistema, o super usuário precisa atribuir diferentes níveis a novos usuários. Para evitar configurar usuários um por um, você pode definir funções com níveis específicos no gerenciamento de funções e atribuir funções apropriadas aos usuários ao adicioná-los. Um super usuário tem todos os níveis, pode atribuir direitos a novos usuários e definir funções correspondentes (níveis) de acordo com os requisitos.

1. Clique em **[Sistema] > [Gerenciamento de Autoridade] > [Função].**



2. Clique em **[Sistema] > [Gerenciamento de Autoridade] > [Função] > [Novo]**. 2. Defina o nome e atribua permissões para a função.

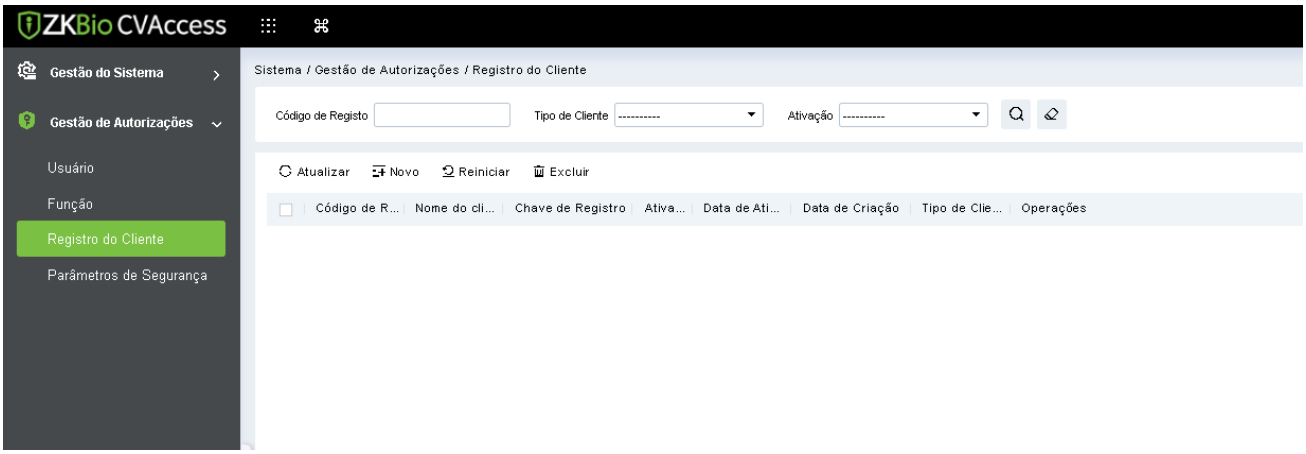


3. Clique em **[OK]** para salvar.

7.2.3 Registro do Cliente

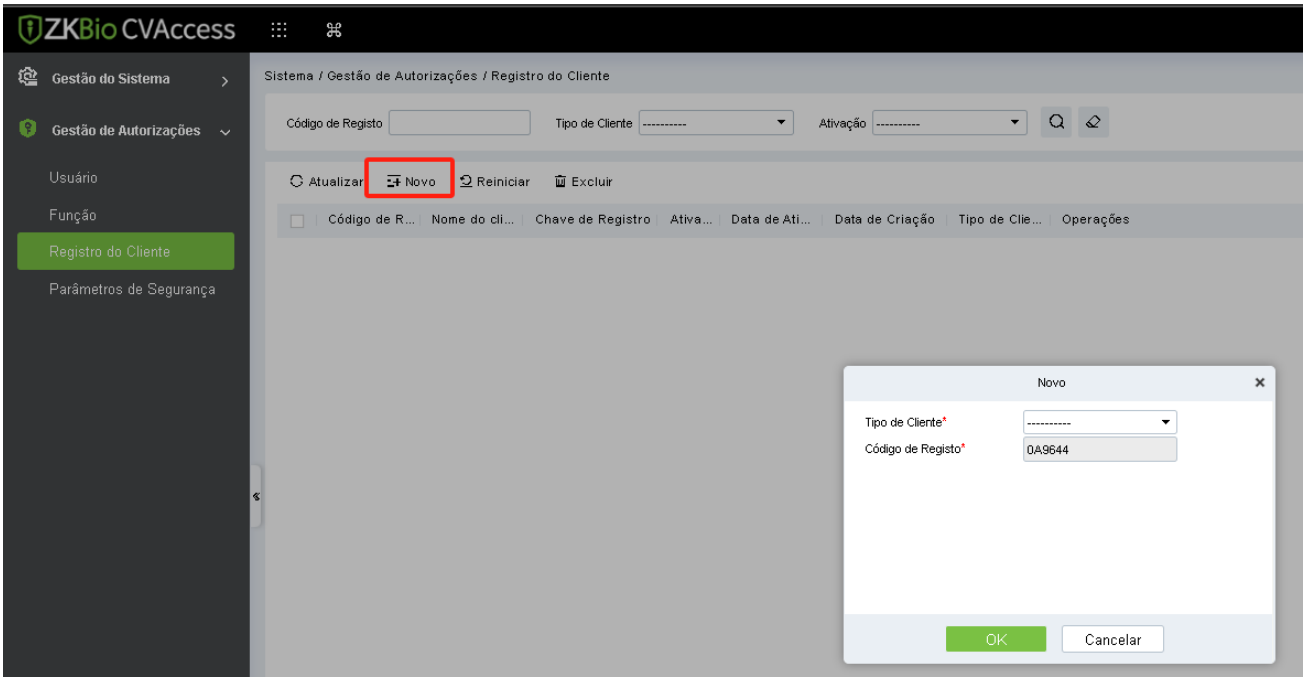
Você pode adicionar tipos de clientes para o sistema e gerar códigos de registro para registros de clientes de cada função do módulo. O número de clientes permitidos é controlado pelo número de pontos permitidos.

Clique em **[Sistema] > [Gerenciamento de Autoridade] > [Registro de Cliente].**



➢ Novo

1. Clique em **[Novo].**



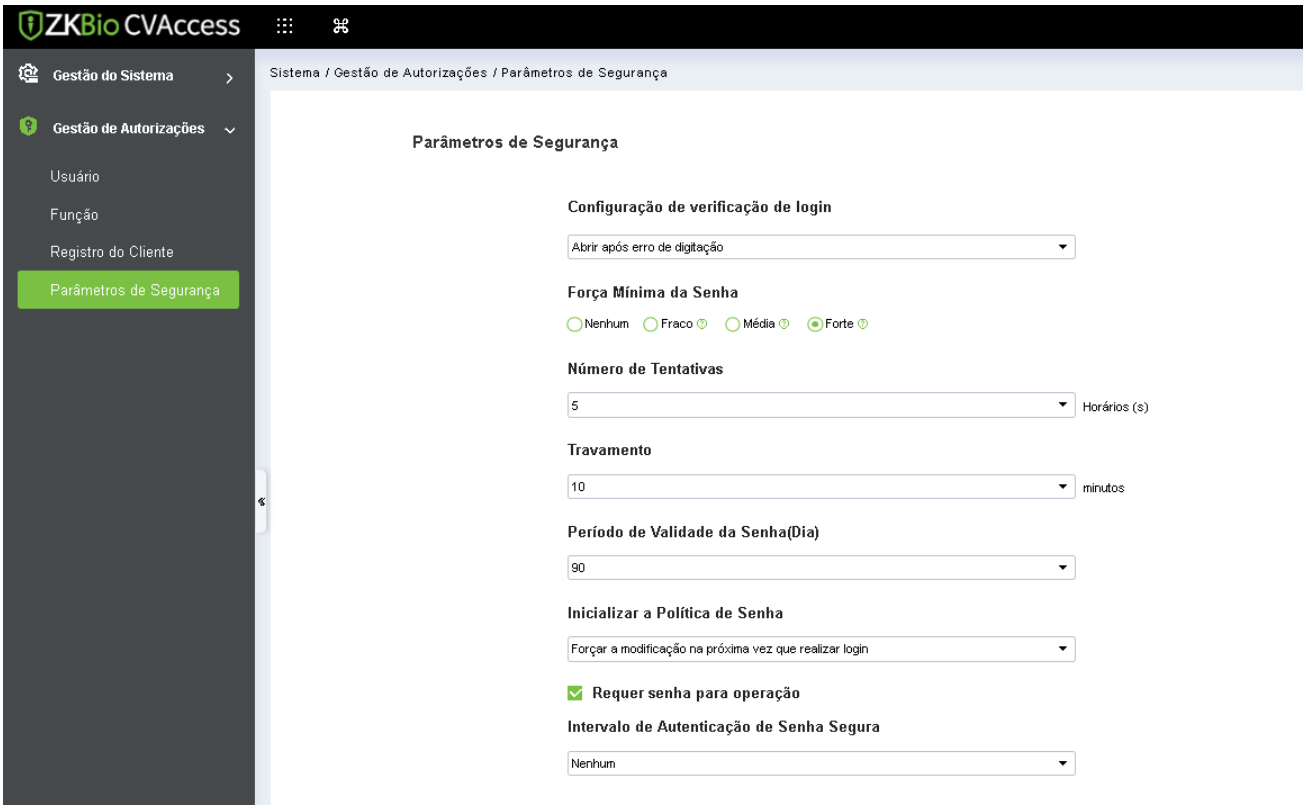
Os campos são os seguintes:

- **Tipo de Cliente:** O valor pode ser Cliente de Aplicativo, OCR-Pessoal, OCR-Visitante, Leitor de ID-Pessoal, Leitor de ID-Visitante ou Visitante de Assinatura, Impressão de Cartão-Pessoal, Impressão de Cartão-Visitante.
- **Código de Registro:** O código de registro para Cliente de Aplicativo é usado em Configurações de Rede na página de login do aplicativo e o código para Impressão de Cartão-Pessoal é usado em Configurações de Parâmetros > Registro de Cliente. Apenas os novos códigos de registro adicionados no servidor são autorizados e um código de registro pode ser usado por apenas um cliente.

2. Clique em **[OK]** para finalizar a adição.

7.2.4 Parâmetros de Segurança

Clique em **[Sistema]** > **[Gerenciamento de Autoridade]** > **[Parâmetros de Segurança].**



➢ Configuração de Código de Verificação de Login

Inclui Nenhum, sempre solicitar código de verificação, Solicitar após inserir um erro.

- **Não abrir código de verificação:** O sistema não permite código de verificação
- **Abrir código de verificação:** Os usuários devem preencher o código de verificação ao fazer login no software.
- **Abrir após inserir erro:** O sistema exibirá uma caixa de verificação após preencher o Nome de Usuário e senha incorretos.

➢ Configuração de Força de Senha

- **Fraco:** As senhas que podem ser usadas devem conter pelo menos 8 caracteres e conter pelo menos 2 dos seguintes tipos: números, letras minúsculas, letras maiúsculas e caracteres especiais.
- **Médio:** As senhas que podem ser usadas devem conter pelo menos 8 caracteres e conter pelo menos 2 dos seguintes tipos: números, letras minúsculas, letras maiúsculas e caracteres especiais, bem como números e letras minúsculas ou apenas números e letras maiúsculas.

- **Forte:** As senhas que podem ser usadas devem conter pelo menos 8 caracteres e conter pelo menos 3 dos seguintes tipos: números, letras minúsculas, letras maiúsculas e caracteres especiais.

➢ **Conta Será Bloqueada**

A conta será bloqueada se o usuário falhar ao fazer login no sistema de acordo com a configuração do software. Por exemplo, se o sistema permitir que o usuário preencha o nome de usuário e senha errados por 2 vezes. O sistema será bloqueado por 10 minutos após exceder 2 vezes de operação.

➢ **Validade da Senha (dias)**

Os usuários podem definir a validade como 30 dias, 60 dias ou permanente. Se a senha expirar, o usuário não poderá fazer login no sistema.

➢ **Modificação de Senha**

Existem 2 opções que o usuário pode definir. Não é obrigatório e forçado a modificar na próxima vez que você fizer login.

- **Não é obrigatório:** O sistema não precisa modificar a senha inicial.
- **Forçado a modificar na próxima vez que você fizer login:** É obrigatório modificar a senha inicial após o segundo login.

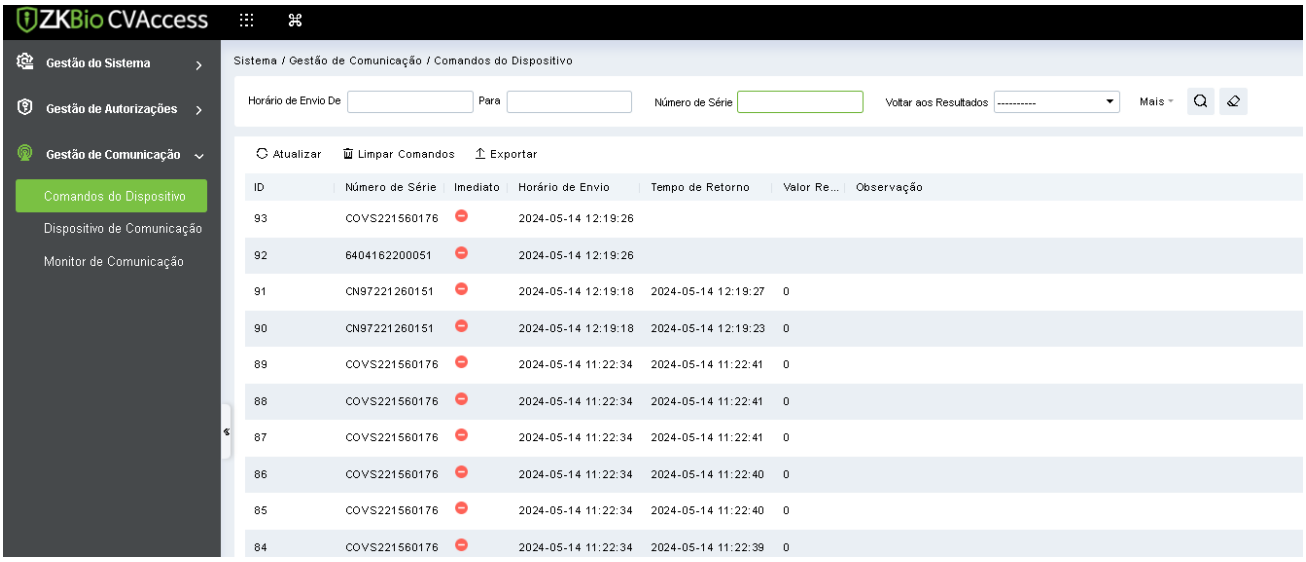
➢ **Intervalo de Autenticação de Senha Segura**

Intervalo mínimo de autenticação de senha.

7.3 Gerenciamento de Comunicação

7.3.1 Comandos do Dispositivo

Clique em **[Sistema]** > **[Comunicação]** > **[Comandos do Dispositivo],** as listas de comandos serão exibidas.



Se o valor retornado for igual ou superior a 0, o comando foi emitido com sucesso. Se o valor retornado for menor que 0, o comando falhou.

- **Limpar Comandos**

Limpar a lista de comandos.

- **Exportar**

Exportar a lista de comandos para o host local. Você pode exportar para um arquivo Excel. Veja a figura a seguir.

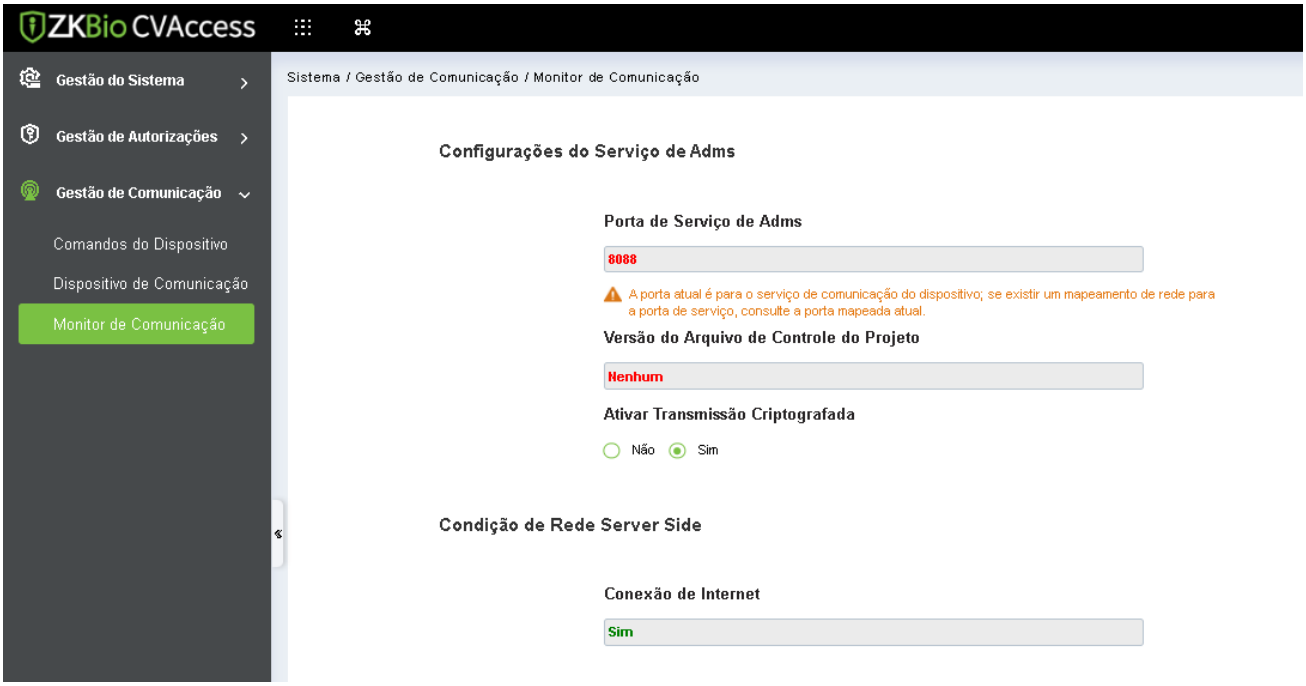
			Device Commands			
ID	Serial Number	Content	Immediately Cmd	Submit Time	Return Time	Returned Value
1504	20100501999	DATA UPDATE userauthorize Pin=2AuthorizeTimezoneId=1AuthorizeDoorId=1 Pin=1AuthorizeTimezoneId=1AuthorizeDoorId=1 ...	false	2017-12-18 10:51:15	2017-12-18 10:51:21	0

7.3.2 Dispositivo de Comunicação

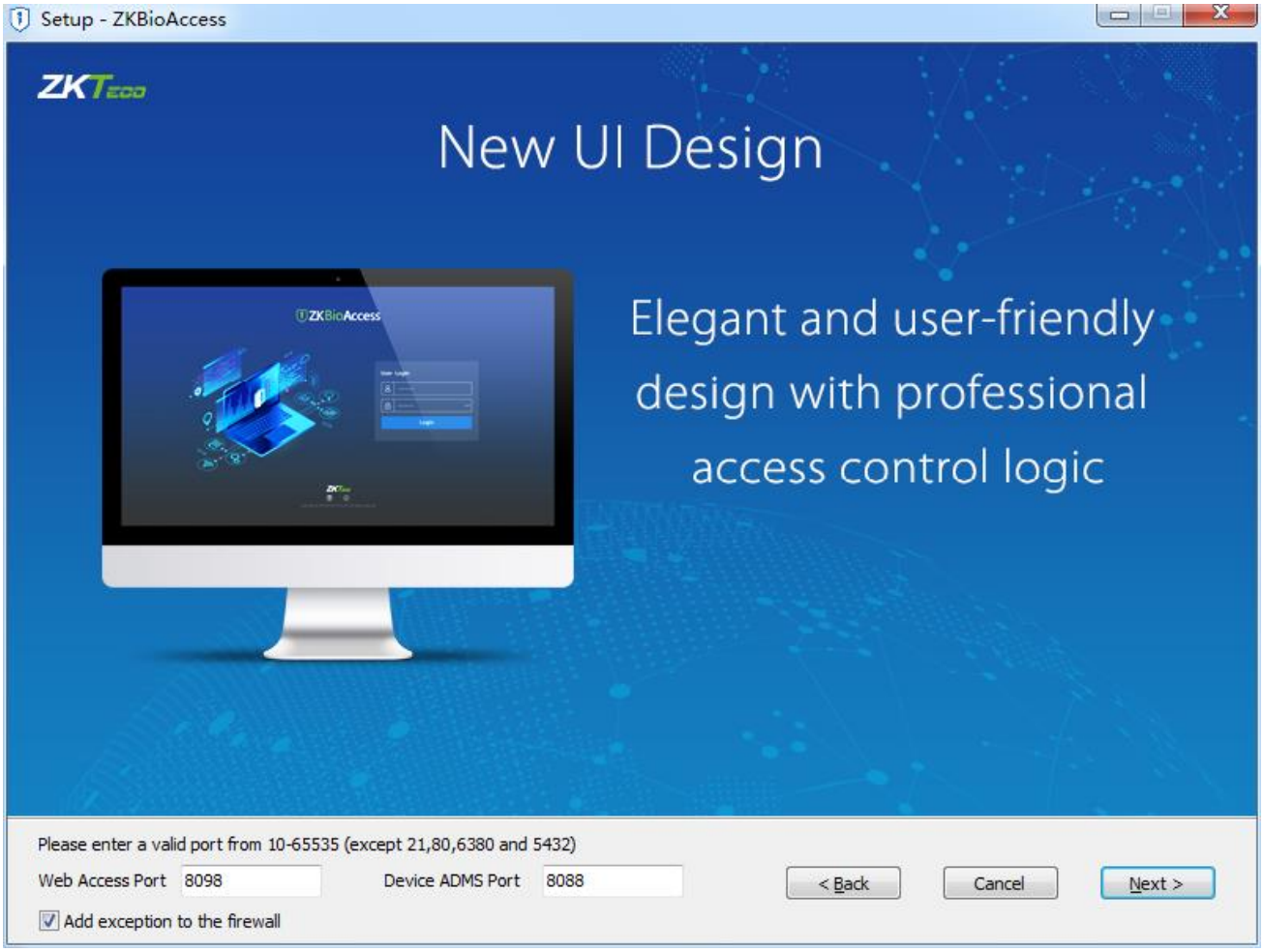
Clique em **[Sistema] > [Comunicação] > [Dispositivo de Comunicação],** você pode visualizar todas as informações do equipamento e comunicação no sistema. Informações detalhadas como módulo acessado, número de série, versão do firmware, endereço IP, status de comunicação e execução de comandos podem ser visualizadas.

7.3.3 Monitor de Comunicação

Clique em **[Sistema]** > **[Comunicação]** > **[Monitor de Comunicação],** a porta de serviço do dispositivo e seus detalhes serão exibidos:



Nota: Ao instalar o ZKBio CVAccess, você precisa inserir o número da porta corretamente.



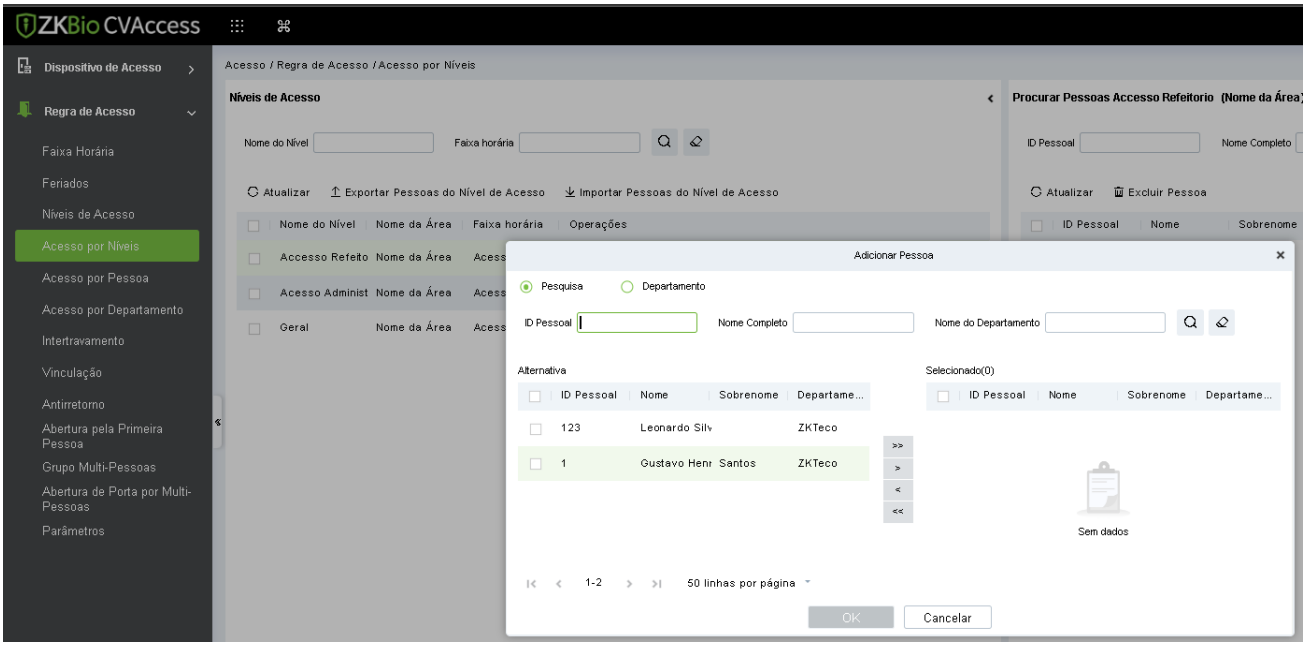
A porta ADMS é usado para se conectar ao dispositivo e a porta de acesso web é usado para acessar o site.

8 Apêndices

8.1 Operações Comuns

➢ Selecionar Pessoal

A página de pessoal selecionado no sistema é como segue:

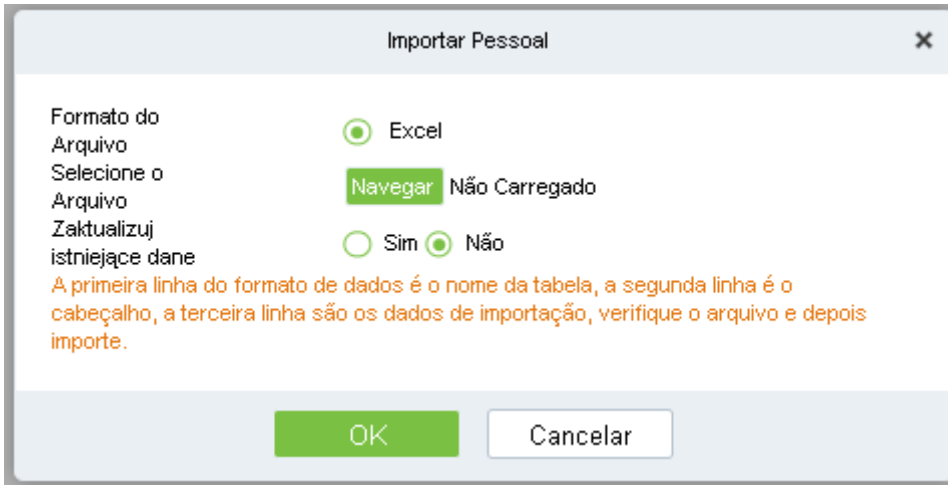


Clique para mover o pessoal selecionado para as listas selecionadas. Se desejar cancelar o movimento, clique

➢ Importar (tome a importação de lista de pessoal como exemplo)

Se houver um arquivo de pessoal em seu computador, você pode importá-lo para o sistema.

1. Clique em [Importar]:



Os campos são os seguintes:

Arquivo de Destino: Escolha o arquivo a ser importado.

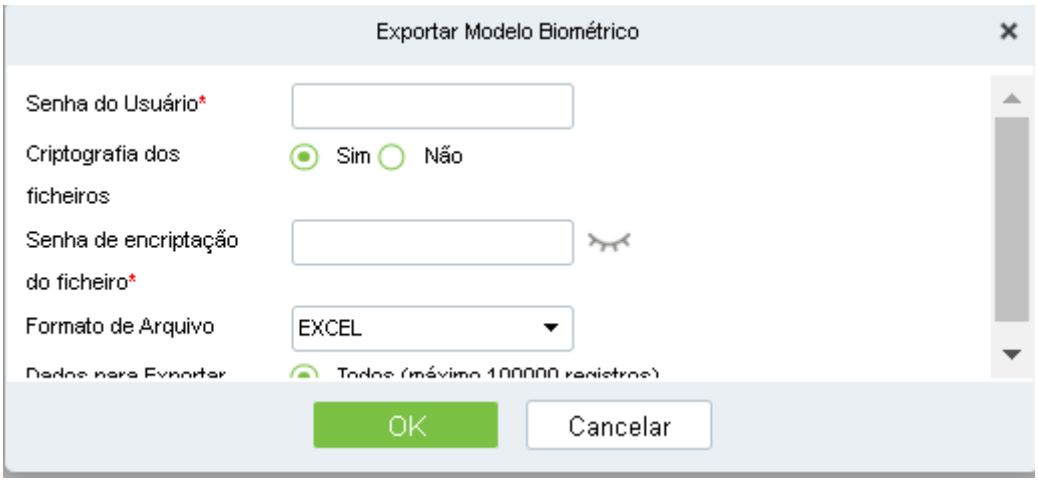
2. Clique em **[OK],** Os dados são importados com sucesso.

Notas:

1) Ao importar a tabela de departamento, o nome do departamento e o número do departamento não devem estar vazios, o departamento pai pode estar vazio. O número duplicado não afeta a operação, pode ser modificado manualmente.
2) Ao importar uma tabela pessoal, um número de pessoal é necessário. Se o número de pessoal já existir no banco de dados, ele não será importado.

➢ **Exportar (tome a exportação de lista de pessoal como exemplo)**

1) Clique em [Exportar]:



2) Selecione o formato do arquivo e o modo de exportação a serem exportados. Clique em [OK].
3) Você pode visualizar o arquivo em seu disco local.

Nota: Por padrão, são permitidos 10000 registros para exportação, você pode inserir manualmente conforme necessário.

8.2 Tipo de Evento de Acesso

➢ **Eventos Normais**

- **Abertura Normal por Cartão:** No modo de verificação [Apenas Cartão], a pessoa com níveis de abertura de porta insere o cartão em um período de tempo válido, abre a porta e aciona o evento normal.
- **Abertura Normal por Impressão Digital:** No modo de verificação [Apenas Impressão Digital] ou [Cartão ou Impressão Digital], a pessoa com níveis de abertura de porta pressiona a impressão digital em um período de tempo válido, a porta é aberta e aciona o evento normal.
- **Abertura por Cartão e Impressão Digital:** No modo de verificação [Cartão e Impressão Digital], a pessoa com permissão de abertura, insere o cartão e pressiona a impressão digital no período de tempo válido, a porta é aberta e aciona o evento normal.

- **Botão de Saída Aberto:** Pressione o botão de saída para abrir a porta dentro do período de tempo válido e acionar este evento normal.
- **Acionar o botão de saída (travado):** Indica o evento normal acionado ao pressionar o botão de saída quando este está travado.
- **Punção durante o Horário Normal de Abertura:** No período de abertura normal (definir período normal de abertura para uma única porta ou para a primeira pessoa normalmente aberta), ou através da operação de abertura normal remota, a pessoa com permissão de abertura de porta insere o cartão eficaz na porta aberta para acionar este evento normal.
- **Pressione a Impressão Digital durante o Horário Normal de Abertura:** No período de abertura normal (definir período normal de abertura para uma única porta ou para a primeira pessoa normalmente aberta), ou através da operação de abertura normal remota, a pessoa com permissão de abertura de porta pressiona a impressão digital eficaz na porta aberta para acionar este evento normal.
- **Primeira Pessoa Normalmente Aberta (Punção de Cartão):** No modo de verificação [Apenas Cartão], a pessoa com permissão para primeira pessoa normalmente aberta, punção no período de tempo de primeira pessoa normalmente aberta (a porta está fechada) e aciona o evento normal.
- **Primeira Pessoa Normalmente Aberta (Pressione a Impressão Digital):** No modo de verificação [Apenas Impressão Digital] ou [Cartão mais Impressão Digital], a pessoa com permissão para primeira pessoa normalmente aberta, pressione a impressão digital no período de tempo de primeira pessoa normalmente aberta (a porta está fechada) e acione o evento normal.
- **Primeira Pessoa Normalmente Aberta (Cartão mais Impressão Digital):** No modo de verificação [Cartão mais Impressão Digital], a pessoa com permissão para primeira pessoa normalmente aberta, punção no cartão e pressione a impressão digital no período de tempo de primeira pessoa normalmente aberta (a porta está fechada) e acione o evento normal.
- **Horário Normal de Abertura Concluído:** Após o término do horário normal de abertura, a porta se fechará automaticamente.
- **Abertura Normal Remota:** Ao definir o estado da porta para abertura normal na operação de abertura remota, este evento normal é acionado.
- **Cancelar Abertura Normal:** Ao punir o cartão válido ou usar a função de abertura remota para cancelar o estado de abertura normal da porta atual, este evento normal é acionado.
- **Desativar o Horário de Passagem Intradia:** Estado normal de abertura interno, punção do cartão eficaz por cinco vezes (deve ser o mesmo usuário), ou selecione [Desativar o Horário de Passagem Intradia] no fechamento remoto.
- **Modo de Passagem Intradia Habilitado:** Se a zona de tempo do modo de passagem intradia estiver desativada, insira o cartão eficaz por cinco vezes (deve ser o mesmo usuário), ou selecione [Habilitar Modo de Passagem Intradia] na operação de abertura remota, e este evento normal será acionado.
- **Abertura de Porta Multiusuário (Punção):** No modo de verificação [Apenas Cartão], a combinação Multiusuário pode ser usada para abrir a porta. Após o último cartão ser verificado, o sistema aciona este evento normal.

- **Abertura de Porta Multiusuário (Pressione a Impressão Digital):** No modo de verificação [Apenas Impressão Digital] ou [Cartão mais Impressão Digital], a combinação Multiusuário pode ser usada para abrir a porta. Após a última impressão digital ser verificada, o sistema aciona este evento normal.
- **Abertura de Porta Multiusuário (Cartão mais Impressão Digital):** No modo de verificação [Cartão mais Impressão Digital], a combinação Multiusuário pode ser usada para abrir a porta. Após o último cartão mais impressão digital ser verificado, o sistema aciona este evento normal.
- **Abertura de Porta por Senha de Emergência:** A senha de emergência (também conhecida como super senha) definida para a porta atual pode ser usada para abrir a porta. Este evento normal será acionado após a verificação da senha de emergência.
- **Abertura de Porta durante o Horário Normal de Abertura:** Se a porta atual estiver definida com um período normal de abertura, a porta se abrirá automaticamente após o término do horário de início definido, e este evento normal será acionado.
- **Disparo de Evento de Vinculação:** Após a configuração de vinculação entrar em vigor, este evento normal será acionado.
- **Cancelar Alarme:** Quando o usuário cancela com sucesso o alarme da porta correspondente, este evento normal será acionado.
- **Abertura Remota:** Quando o usuário abre uma porta por [Abertura Remota] com sucesso, este evento normal será acionado.
- **Fechamento Remoto:** Quando o usuário fecha uma porta por [Fechamento Remoto] com sucesso, este evento normal será acionado.
- **Abrir Saída Auxiliar:** Na configuração de vinculação, se o usuário selecionar Saída Auxiliar para Ponto de Saída, selecionar Abrir para Tipo de Ação, este evento normal será acionado quando a configuração de vinculação entrar em vigor.
- **Fechar Saída Auxiliar:** Na configuração de vinculação, se o usuário selecionar Saída Auxiliar para Ponto de Saída, selecionar Fechar para Tipo de Ação, ou fechar a saída auxiliar aberta por [Configuração de Porta] > [Fechar Saída Auxiliar], este evento normal será acionado.
- **Porta Aberta Corretamente:** Quando o sensor da porta detecta que a porta foi aberta corretamente, acionando este evento normal.
- **Porta Fechada Corretamente:** Quando o sensor da porta detecta que a porta foi fechada corretamente, acionando este evento normal.
- **Ponto de Entrada Auxiliar Desconectado:** Será acionado quando o ponto de entrada auxiliar estiver desconectado.
- **Ponto de Entrada Auxiliar Curto:** Quando houver curto-circuito no ponto de entrada auxiliar, acione este evento normal.
- **Início do Dispositivo:** Será acionado se o dispositivo for iniciado (Este evento dos dispositivos PULL não aparecerá no monitoramento em tempo real e só pode ser visualizado nos registros de eventos dos relatórios).

➢ **Eventos Anormais**

- **Intervalo de Punção Muito Curto:** Quando o intervalo entre duas punções é menor que o intervalo de tempo definido, este evento anormal será acionado.
- **Intervalo de Pressão de Impressão Digital Muito Curto:** Quando o intervalo entre duas pressões de impressão digital é menor que o intervalo de tempo definido, este evento anormal será acionado.
- **Zona de Tempo Inativa da Porta (Cartão de Punção):** No modo de verificação [Apenas Cartão], se o usuário com permissão de abertura da porta punção, mas não durante o período de tempo efetivo da porta, este evento anormal será acionado.
- **Zona de Tempo Inativa da Porta (Pressione a Impressão Digital):** Se o usuário com permissão de abertura da porta pressionar a impressão digital, mas não durante o período de tempo efetivo da porta, este evento anormal será acionado.
- **Zona de Tempo Inativa da Porta (Botão de Saída):** Se o usuário com permissão de abertura da porta pressionar o botão de saída, mas não durante um período de tempo efetivo, este evento anormal será acionado.
- **Zona de Tempo Ilegal:** Se o usuário com a permissão de abrir a porta punção durante a zona de tempo inválida, este evento anormal será acionado.
- **Acesso Ilegal:** Se o cartão registrado sem permissão da porta atual for punção para abrir a porta, este evento anormal será acionado.
- **Anti-Retrocesso:** Quando o anti-retrocesso entra em vigor, este evento anormal será acionado.
- **Intertravamento:** Quando as regras de intertravamento entram em vigor, este evento anormal será acionado.
- **Verificação Multiusuário (Punção):** Quando a combinação Multiusuário abre a porta, a verificação do cartão antes do último (verificado ou não), este evento anormal será acionado.
- **Verificação Multiusuário (Pressione a Impressão Digital):** No modo de verificação [Apenas Impressão Digital] ou [Cartão ou Impressão Digital], quando a combinação Multiusuário abre a porta, a verificação da impressão digital antes do último (verificado ou não), este evento anormal será acionado.
- **Cartão Não Registrado:** Se o cartão atual não estiver registrado no sistema, este evento anormal será acionado.
- **Impressão Digital Não Registrada:** Se a impressão digital atual não estiver registrada ou estiver registrada, mas não sincronizada com o sistema, este evento anormal será acionado.
- **Tempo Limite de Abertura de Porta:** Se a porta não for fechada dentro do tempo de atraso especificado após a abertura, então o sensor detecta e aciona este evento anormal.
- **Cartão Expirado:** Se a pessoa com o nível de acesso à porta punção após o tempo efetivo do controle de acesso e não pode ser verificada, este evento anormal será acionado.
- **Impressão Digital Expirada: Se** a pessoa com a permissão de acesso à porta pressionar a impressão digital após o tempo efetivo do controle de acesso e não puder ser verificada, este evento anormal será acionado.
- **Erro de Senha:** Se estiver usando o modo de verificação [Cartão mais Senha], senha de duress ou senha de emergência para abrir a porta, este evento anormal será acionado.

- **Falha ao Fechar a Porta durante o Horário Normal de Abertura:** Se a porta atual estiver no estado de abertura normal, mas o usuário não puder fechá-la por [Fechamento Remoto], este evento anormal será acionado.
- **Erro de Modo de Verificação:** Se o modo de abertura de porta do usuário for inconsistente com o definido para a porta atual,
- **Erro de Verificação Multiusuário:** Quando a combinação Multiusuário abre a porta, a verificação falha e aciona este evento anormal.

➢ **Eventos de Alarme**

- **Abertura de Porta por Senha de Coação:** Use a senha de coação da porta atual para verificação com sucesso e acione este evento de alarme.
- **Abertura de Porta por Impressão Digital de Coação:** Use a impressão digital de coação da porta atual para verificação com sucesso e acione este evento de alarme.
- **Alarme de Abertura de Porta por Coação:** Use a senha de coação ou a impressão digital de coação definida para a porta atual para verificação com sucesso e acione este evento de alarme.
- **Aberto Acidentalmente:** Exceto por todos os eventos normais, se o sensor da porta detectar que a porta está aberta, este evento de alarme será acionado.
- **Tempo Limite de Abertura da Porta:** Este evento de alarme é acionado quando a porta aberta não é trancada no tempo de fechamento da porta.
- **Alarme de Resistência a Manipulações:** Este evento de alarme será acionado quando o dispositivo AIO for manipulado.
- **Falha na Conexão com o Servidor:** Este evento de alarme será acionado quando o dispositivo estiver desconectado do servidor.
- **Queda de Energia Principal:** Eventos de controlador da série Inbio5, queda de energia externa.
- **Queda de Energia da Bateria:** Evento de controlador da série Inbio5, queda de energia da bateria interna.
- **Alarme de Cartão Inválido:** Evento de alarme acionado quando cinco cartões inválidos são passados consecutivamente.

Notas: O usuário pode personalizar o nível de cada evento (Normal, Anormal e Alarme).

8.3 Perguntas Frequentes

Q: Como usar um emissor de cartões?
R: Conecte o emissor de cartões ao PC através da porta USB e clique em emissão individual de cartão ou emissão em lote. Mova o cursor para a caixa de entrada do número do cartão e passe o cartão no emissor de cartões; o número do cartão será mostrado automaticamente na caixa de entrada.

Q: Qual é a utilidade da configuração de papéis?

R: A configuração de papéis tem as seguintes utilidades: 1. Definir um nível unificado para o mesmo tipo de usuários recém-adicionados, basta selecionar este papel ao adicionar usuários; 2. Ao configurar lembretes do sistema e determinar quais papéis podem ser visualizados.

Q: Como operar se eu quiser configurar contas para todos os funcionários do Departamento Financeiro da Empresa?
R: Primeiro, crie um novo papel nas configurações do sistema e configure as funções a serem usadas para este papel. Em seguida, adicione um usuário, configure as informações do usuário e selecione o papel do usuário, assim adicionando uma nova conta. Para outras contas, faça o mesmo.

Q: No Windows Server 2003, por que o navegador IE exibe erro ao acessar o sistema e como resolver?
R: Esse problema ocorre porque o Server 2003 possui configurações de [Opção de Configuração de Segurança]. Para acessar o sistema, configure-o da seguinte forma: clique em Iniciar – Painel de Controle – Adicionar ou Remover Programas, selecione [Adicionar e remover componentes do Windows] na interface e clique na opção [Configuração Avançada de Segurança do Internet Explorer], desmarque a caixa de seleção. Em seguida, clique em [Avançar] para removê-lo do sistema. Abra novamente o sistema e o navegador acessará o sistema corretamente.

Q: Se o backup ou a restauração do banco de dados falhar, qual pode ser o motivo?
R: Backup falha: Verifique as variáveis de ambiente do sistema, vá em Propriedades > Avançado para definir as variáveis de ambiente como
"C:\Program Files\ZKBio CVAccess\Main Resource\postgresql\bin:"
"C:\Program Files" é o caminho de instalação do sistema, você pode modificar conforme sua situação real.
Restauração falha: Existem várias razões: a versão do sistema é muito alta ou muito baixa, ou o banco de dados está danificado, você precisa seguir as instruções para alterar a versão do sistema ou reparar o sistema, reinstalar o banco de dados.

8.4 ACORDO DE LICENÇA DE USUÁRIO FINAL

Informações importantes - leia atentamente:
Este Acordo de Licença de Usuário Final ("EULA") é um acordo legal entre Sketch e você (individualmente ou como uma entidade única). **O PRODUTO DE SOFTWARE** inclui o aplicativo de software, mídia associada, materiais impressos e documentação online ou eletrônica. Ao instalar, copiar ou usar o Produto de Software, você concorda em estar vinculado aos termos deste EULA. Se você não concordar com os termos deste EULA, não instale ou use o Produto de Software.

LICENÇA DO PRODUTO DE SOFTWARE

O Produto de Software é protegido por leis de direitos autorais, acordos internacionais de direitos autorais, bem como outras leis e acordos de propriedade intelectual. O Produto de Software é licenciado e não pode ser vendido por terceiros.

1. **OUTORGA DE LICENÇA**

Este EULA concede a você os seguintes direitos:

Instalação e Uso: Você pode instalar o software em um número ilimitado de sistemas.
Replicação e Distribuição: Você pode distribuir o software para um número ilimitado de sistemas; desde que cada cópia seja verdadeira e completa, incluindo todos os avisos de direitos autorais e marcas registradas, e seja acompanhada por uma cópia deste EULA. O Produto de Software pode ser distribuído como um produto independente ou pode ser incluído em seu próprio produto.

2. **DESCRIÇÃO DE OUTROS DIREITOS E LIMITAÇÕES**

Limitações sobre Desmontagem, Decompilação e Desmontagem

Você não pode desmontar, descompilar ou desmontar o Produto de Software, exceto e somente na medida em que tal atividade seja expressamente permitida por lei aplicável, não obstante esta limitação.

Separação de Componentes

O produto de software é licenciado como um único produto. Seus componentes não podem ser separados para uso em mais de um sistema.

Transferência de Software

Você pode transferir permanentemente sua propriedade, desde que o destinatário concorde com os termos deste EULA.

Rescisão

Sem prejuízo de quaisquer outros direitos, a ZKTeco pode rescindir este EULA se você não cumprir os termos e condições deste EULA. Nesse caso, você deve destruir todas as cópias do Produto de Software e todos os seus componentes.

Distribuição

O Produto de Software não pode ser vendido ou incluído em um produto ou pacote que pretenda receber benefícios através da inclusão do Produto de Software. O Produto de Software pode ser incluído em pacotes ou produtos gratuitos ou sem fins lucrativos.

3. DIREITOS AUTORAIS

Todos os títulos e direitos autorais no Produto de Software (incluindo, mas não se limitando a imagens, fotografias, animações, vídeo, áudio, música, texto e applets incorporados no Produto de Software), os materiais impressos acompanhantes e quaisquer cópias do Produto de Software são de propriedade da ZKTeco. O Produto de Software é protegido por leis de direitos autorais e acordos internacionais. Portanto, você deve tratar o Produto de Software como qualquer outro material protegido por direitos autorais, exceto que você pode instalar o Produto de Software em um único sistema, desde que mantenha o original exclusivamente para fins de backup ou arquivamento.

GARANTIA LIMITADA

A ZKTeco expressamente renuncia qualquer garantia para o Produto de Software. O Produto de Software e qualquer documentação relacionada são fornecidos "como estão", sem garantia de qualquer tipo, expressa ou implícita, incluindo, sem limitação, as garantias implícitas de comercialização, adequação a uma finalidade específica ou não infração. Todo o risco decorrente do uso ou desempenho do Produto de Software permanece com você.

SEM RESPONSABILIDADE POR DANOS

Em nenhum caso, a ZKTeco será responsável por quaisquer danos (incluindo, sem limitação, danos por perda de lucros comerciais, interrupção de negócios, perda de informações comerciais ou qualquer outro prejuízo pecuniário) decorrentes do uso ou incapacidade de uso deste produto, mesmo que a ZKTeco tenha sido avisada da possibilidade de tais danos.

Reconhecimento do Acordo

Li e entendi cuidadosamente este Acordo, a Declaração de Política de Privacidade da ZKTeco Ltda.
Se VOCÊ ACEITAR os termos deste Acordo:
Eu reconheço e entendo que, ao aceitar este acordo, devo cumprir os termos e condições para usar o Produto de Software e garantir um funcionamento adequado. Também reconheço que a ZKTeco pode rescindir o Contrato de Licença se eu não cumprir os termos e condições.

SE VOCÊ NÃO ACEITAR os termos deste Acordo.

Eu reconheço e entendo que, ao recusar aceitar estes termos, rejeitei este acordo de licença e, portanto, não tenho o direito legal de instalar, usar ou copiar este Produto ou o Software Licenciado que ele incorpora.

Telefone: (31) 3055-3530
Endereço: Rodovia MG-010, KM 26
Loteamento 12 - Bairro Angicos
Vespasiano - MG - CEP: 33.206-240
www.zkteco.com.br