

Manual detalhado do JNAccess

Operação configuração e administração de todos os módulos

Versão 0.3.15

Revisão de 09 de outubro de 2026

Guia para administradores gestores e operadores

Procedimentos de cadastros e acesso, integração JC-013, reconhecimento facial, LPR, garagem, refeitório, manutenção e rotinas do servidor.

Inclui seleção das portas habilitadas em Ponto de acesso e popup de porta aberta com desativação individual.

Sumário

1 Como usar este manual	4
2 Instalação e atualização	5
3 Sessão e acesso ao painel	6
4 Operadores permissões e notificações	7
5 Pessoas e credenciais	8
6 Visitantes e QR temporário	10
7 Pré cadastro e convites	11
8 Empresas e vagas	12
9 Departamentos e grupos	13
10 Áreas e ocupação lógica	14
11 Horários de acesso	15
12 Regras de acesso	16
13 Dispositivos e controladores	17
14 Placa Valle JC 013 e porta aberta	20
15 Monitoramento e abertura manual	22
16 Ocupação e presença	23
17 Relatórios e auditoria	24
18 Reconhecimento facial por câmera IP	26
19 LPR e leitura de placas	29
20 Monitor de Eventos LPR	31

21	Garagem cobranças e recebimentos	32
22	Refeitório e alimentação	35
23	Manutenção e saúde dos ativos	40
24	Lista de restrição	42
25	LGPD e privacidade	43
26	Licenciamento	44
27	Relatórios automáticos	45
28	Launcher backup e restauração	46
29	Aplicativo móvel de cadastros	47
30	Rotinas recomendadas e implantação	48
31	Solução de problemas por módulo	49
32	Referência de telas e revisão do manual	51

1 Como usar este manual

Este manual orienta administradores, gestores e operadores no uso do JNAccess. Abrange os módulos disponíveis na distribuição 0.3.15, atualizada em 09 de outubro de 2026, incluindo a JC-013 e a seleção das portas habilitadas no campo Ponto de acesso do reconhecimento facial.

Use o sumário do PDF para localizar um módulo. Os exemplos são fictícios e não contêm senhas, chaves de câmeras ou dados pessoais da instalação. Os menus e botões dependem das permissões do operador; as rotas são caminhos dentro do endereço do servidor.

Preparação da operação

1. Servidor instalado, licença válida e endereço de acesso definido.
2. Operadores com permissões adequadas às suas tarefas.
3. Áreas, horários e regras cadastrados para os acessos.
4. Equipamentos e câmeras comunicando e configurados para a finalidade correta.
5. Pessoas e visitantes com credenciais válidas; vagas e benefícios configurados quando usados.
6. Backup e procedimentos de correção conhecidos pela equipe.

Cadastrar uma pessoa não concede acesso por si só. A liberação depende de regras, validade, credencial e configuração do ponto. Um comando aceito pelo equipamento não comprova que a pessoa passou nem que a porta abriu fisicamente.

Vocabulário inicial

Termo	Uso no sistema
Pessoa	Cadastro de usuário com acesso regular.
Visitante	Cadastro temporário com fim de validade.
Operador	Usuário que entra no painel.
Área	Local de origem ou destino de uma passagem.
Porta	Ponto lógico do equipamento associado a áreas.
Relé	Saída física de abertura, como S1 a S6 na JC-013.
Sensor	Entrada que informa estado da porta, como A1 a A6.
Regra	Associação de pessoas ou grupos, horários e áreas.
Online	Equipamento consulta o servidor para decidir o acesso.
Standalone	Equipamento decide usando dados locais.
Somente leitura	Sistema acompanha sem assumir gerenciamento.
Template facial	Representação biométrica processada para câmeras IP.

O refeitório usa configuração própria, separada do acesso geral. O manual descreve recursos implementados, mas não afirma que todos os equipamentos e serviços externos já estejam instalados ou ligados. Confira conexão, direção e funcionamento físico na implantação.

2 Instalação e atualização

Escolher o executável

Arquivo	Finalidade
Setup Completo 0.3.15	Instalação de um novo servidor com os componentes completos.
Atualizacao 0.3.15	Atualização de uma instalação existente conforme o assistente.

Os executáveis 0.3.15 gerados em 09 de outubro de 2026 incluem a JC-013, o popup de porta aberta e a seleção de portas habilitadas em Ponto de acesso. O nome inclui versão e horário de geração.

Instalar um servidor

1. Use uma conta Windows autorizada a instalar serviços.
2. Execute o instalador completo e acompanhe o assistente.
3. Confira pasta, parâmetros do servidor e componentes. Anote a pasta escolhida.
4. Defina um endereço de rede estável para os demais computadores.
5. Conclua e use Abrir no navegador no Launcher.
6. Faça o login, troque a senha quando solicitado e confira a licença.
7. Configure cadastros, áreas, regras e equipamentos antes de operar.

Use a porta e o endereço exibidos pelo Launcher. Instalações podem usar portas diferentes; localhost só aponta para o próprio computador. Para uso em rede, informe o IP ou nome do servidor.

Atualizar

1. Gere e confira um backup; guarde também configuração e arquivos externos relevantes.
2. Informe à operação a janela de manutenção, pois o serviço pode reiniciar.
3. Execute o atualizador e selecione a pasta da instalação existente.
4. Aguarde o fim do assistente.
5. Abra o sistema e atualize o navegador; use Ctrl e F5 se a tela antiga persistir.
6. Confira login, licença, cadastros, monitoramento e comunicação.
7. Confira câmeras, portas, vagas, benefícios e integrações dos módulos utilizados.

Não restaure um banco antigo apenas porque a tela mudou. Confira primeiro versão, endereço e serviço. Uma restauração substitui dados e requer uma rotina de manutenção.

Endereço e HTTPS

Use o HTTPS da instalação para os recursos que exigem conexão segura, incluindo aplicativo e captura no navegador. Confie no certificado pelo procedimento do administrador. O equipamento online precisa alcançar o endereço de comunicação do JNAccess; após troca de IP, use o reapontamento em Dispositivos.

A URL pública de pagamento ou convite pode ser diferente da URL interna. Cadastrar um endereço local não o torna acessível pela internet.

3 Sessão e acesso ao painel

Entrar e sair

1. Abra o endereço do servidor ou use o Launcher.
2. Informe usuário e senha e clique em Entrar.
3. Defina a nova senha se o sistema solicitar.
4. Confira o operador no rodapé do menu.
5. Ao terminar, clique em Sair, especialmente em computador compartilhado.

Manter conectado prolonga a sessão nesse computador. Utilize somente quando a conta e a máquina estiverem sob seu controle. Se a sessão expirar, faça novo login.

Trocar usuário e senha

Trocar usuário permite assumir outra conta e preservar a autoria das ações. A nova conta pode ser direcionada a outra tela conforme suas permissões. Use o nome do usuário no rodapé para acessar a troca de senha.

Em caso de esquecimento, solicite redefinição ao administrador. A conta pode exigir uma senha nova no próximo login.

Menu ausente

Confira conta, recarga da página e permissão Ver do módulo. Alguns módulos são exclusivos do administrador, e algumas abas dependem de permissões próprias. Não compartilhe a conta de outro operador para contornar uma restrição.

4 Operadores permissões e notificações

Onde acessar: Sistema → Operadores e Sistema → Permissões.

Cadastrar operador

1. Como administrador, adicione um usuário em Operadores.
2. Informe Usuário, Nome, Perfil e senha inicial.
3. Marque Ativo, salve e oriente o primeiro acesso.
4. Abra Permissões e ajuste os módulos e ações necessários.

Admin tem acesso total. Operador e Portaria podem usar o padrão do perfil ou uma configuração personalizada. A própria conta administrativa não pode ser desativada ou rebaixada por essa rotina.

Configurar permissões

1. Selecione o operador.
2. Marque Ver, Inserir, Alterar e Excluir conforme a tarefa.
3. Use os atalhos de perfil e confira o resultado.
4. Salve; peça ao usuário para entrar ou recarregar.
5. Confira uma consulta e uma ação permitida.

Ação	Efeito típico
Ver	Exibe menu e permite consulta.
Inserir	Cadastro e importação quando oferecidos.
Alterar	Edição; no monitor também abertura e exceção.
Excluir	Remoção quando existe e não há vínculo impeditivo.

Marcar uma ação pressupõe Ver. Restaurar padrão desfaz a personalização. Operadores, Permissões, Licenciamento e Relatórios automáticos possuem acesso administrativo. Refeitório e biometria têm permissões próprias por aba e ação.

Permissões para JC 013 e facial

Alterar Dispositivos permite configurar canais e desabilitar permanentemente o alerta de porta aberta. Acionamento no monitor exige a ação correspondente do Monitoramento. Cadastro de templates exige Biometria facial, além do acesso ao cadastro da pessoa. Alterar câmeras e consultar eventos também são permissões distintas.

Notificações

Confira os canais configurados, retenção e resumo disponíveis na área de notificações. Enviar teste verifica o canal. Webhook, Telegram e e-mail dependem da configuração técnica da instalação.

Eventos de equipamento offline, retorno, exceção e acesso podem gerar notificações. O popup de porta aberta depende do sensor e do alerta do canal. Use a Auditoria para conferir operador, data e ação.

5 Pessoas e credenciais

Busque por nome, matrícula, CPF ou cartão; filtre por situação. A coluna **Credenciais** mostra cartões e face; **Último acesso** mostra a última passagem.

Cadastrar ou editar

Clique em **+ Adicionar** ou no nome da pessoa.

Aba Dados

- **Nome completo** (obrigatório), **CPF** (validado), **Matrícula**, **E-mail**, **Telefone**.
- **Válido de / Válido até**: período em que o acesso vale (opcional para pessoas).
- **Observações**.
- **Inativo**: continua listada, mas não entra.
- **Contingência**: fica gravada no equipamento mesmo no modo online — entra se o servidor cair.
- **Lista de exceção**: sempre bloqueada e gera alarme.

Aba Grupos — marque os departamentos/grupos. É por eles que as regras dão acesso.

Aba Cartões / QR — adicione cartões de proximidade (formato 123,45678 ou número) ou gere um QR Code.

Aba Veículo — cadastre placa, tipo, marca, modelo e cor. Uma placa não pode pertencer simultaneamente a duas pessoas. A quantidade e o responsável pelas vagas são definidos na aba Vagas.

Aba Face

- **Enviar arquivo**: foto frontal, bem iluminada, rosto centralizado, JPG/PNG até 2 MB.
- **Capturar pela câmera do...**: escolha o iDFace e clique em **Capturar**; fique de frente para o equipamento a ~50 cm (ele conta 3 s e tira a foto; aguarda até 45 s).

Depois de salvar pessoas, fotos, cartões ou regras, o servidor agenda automaticamente o envio aos equipamentos habilitados e gerenciados. Se houver falha, a pendência permanece no banco e será tentada novamente. Em **Dispositivos**, acompanhe o último envio, a pendência e eventuais erros.

Enviar dados continua disponível para uma tentativa manual. Salvar não significa que o equipamento já recebeu a alteração.

Otimização automática das fotos: novas fotos e substituições enviadas pelo cadastro web, aplicativo e convites podem ser reduzidas pelo servidor, mantendo a proporção e sem ampliar a imagem. Quando a conversão reduz o arquivo, utiliza JPEG com qualidade 85 e até 1024 pixels no maior lado. JPEGs já dimensionados e corretamente orientados são preservados. Fotos já cadastradas, importações em lote e imagens recebidas diretamente do equipamento não são recomprimidas por essa rotina. O limite de envio continua sendo 2 MB. A redução de tamanho não corrige uma foto desfocada; confira a imagem e teste o reconhecimento no equipamento.

Biometria das câmeras IP

A foto do cadastro e a face enviada a um iDFace não criam automaticamente o template das câmeras IP. Na aba Face, use Biometria facial — câmeras IP e escolha Enviar arquivo, Usar a foto do cadastro ou Capturar. Aguarde a situação válida. O capítulo Reconhecimento facial detalha esse processamento.

Vagas

Na aba Vagas escolha Esta pessoa para cota própria ou Empresa para cota compartilhada. Visitantes também podem usar Pessoa responsável. Confira ocupação antes de trocar vínculos.

Importação em lote

1. Baixe o modelo da tela de importação de Pessoas.
2. Preencha conforme as instruções; nome é obrigatório e visitante precisa de fim de validade.
3. Use Pré-visualizar e confira erros, duplicidades, grupos e cartões.
4. Corrija e confirme.
5. Confira os cadastros e o envio em Dispositivos.

Para carga com fotos, use a rotina apropriada do Launcher e confira pasta e arquivos. O nome de uma foto em uma planilha não comprova que a imagem foi incorporada.

Conferência antes de liberar

Verifique situação, validade, grupos, regra e credencial. Garagem também exige vaga e veículo conforme o uso; refeitório exige benefício; câmeras IP exigem template válido e serviço facial. Confira último envio se um leitor não recebeu a alteração.

6 Visitantes e QR temporário

Onde acessar: Cadastros → Visitantes.

Cadastrar uma visita

1. Pesquise o documento ou nome para evitar duplicidade.
2. Adicione o visitante e informe identificação e contato.
3. Defina início e fim da validade.
4. Associe empresa visitada ou anfitrião conforme a ficha.
5. Selecione os grupos e confira regra para área e horário.
6. Cadastre cartão, QR, face do leitor ou biometria da câmera IP.
7. Se houver garagem, escolha Empresa ou Pessoa responsável na aba Vagas.
8. Salve e confira situação e período.

Empresa visitada não escolhe automaticamente quem fornece a vaga. Cadastro temporário não ignora restrição, validade, regra ou cota.

QR de acesso

Na aba Cartões / QR, use a geração disponível. Para QR de 24 horas, confira início e fim e confirme a emissão. O leitor precisa estar configurado para interpretar essa credencial. As regras de acesso continuam valendo.

Antes de entregar, confira pessoa, período e local. Se a leitura resultar em Não identificado, confira credencial, validade, sincronização e configuração do equipamento.

Encerrar e corrigir

Edite a validade ou situação para encerrar a visita. Corrija presença em Relatórios → Status atual somente após conferir a saída real. Com veículo dentro, trate a ocupação antes de remover vínculos.

Restrição de visitante

VISITANTE NÃO AUTORIZADO À ENTRADA pode indicar restrição por CPF ou RG. O motivo detalhado depende de permissão específica. Encaminhe ao responsável; trocar nome ou criar outra ficha não resolve uma restrição ativa.

7 Pré cadastro e convites

O visitante preenche os próprios dados e tira a selfie pelo celular **antes de chegar**; a portaria só aprova.

1. **+ Novo convite**: informe (opcional) o nome, a **validade do link**, o **início e o fim da visita**, anfitrião, empresa visitada, uma observação e os **grupos aplicados na aprovação** (são eles que darão acesso — ex.: "Visitantes Bloco A").
2. Envie o link por **WhatsApp, E-mail** ou **Copiar link**.
3. O visitante abre o link no celular, preenche nome, CPF, contato, tira a **selfie** e aceita o termo de consentimento (LGPD).
4. O convite vai para **Para aprovar** e a portaria recebe um aviso na tela. Confira a foto e clique em **Aprovar** (cria o visitante com a validade da visita) ou **Recusar** (apaga os dados enviados).
5. Aprovado, o visitante pode receber um **passe com QR Code** (botão **Passe**), válido só no período da visita.

O link é de uso único e expira na data definida. **Cancelar** invalida um convite ainda não preenchido.

Conferir após aprovação

Abra o cadastro aprovado e confira grupos, validade, credencial e estacionamento. Enviar o formulário não equivale à aprovação. Uma selfie de convite também precisa de processamento próprio para ser utilizada pelas câmeras IP.

O link deve ser alcançável pelo visitante. Use o endereço externo autorizado para convites fora da rede. Cancele links e pedidos que não serão utilizados.

8 Empresas e vagas

Onde acessar: Cadastros → Empresas.

Cadastro

1. Pesquise antes de criar.
2. Informe Nome, Sala e CNPJ quando aplicável.
3. Defina Quantidade de vagas se não usar numeração.
4. Configure exceção de anti-dupla entrada somente se necessária.
5. Salve e confira os vínculos das pessoas.

Sala aparece junto à empresa nos relatórios. Vínculo empresarial e responsabilidade pela vaga precisam ser conferidos separadamente no cadastro da pessoa.

Vagas numeradas

Na edição, use Vagas numeradas e informe posições separadas por vírgula ou faixa, como 15-18. Preencha garagem, sala e observação e clique em Adicionar vagas. Cada número pertence a uma empresa. O total passa a refletir a lista.

A numeração organiza as vagas; a autorização utiliza a cota compartilhada e não reserva uma posição para cada placa.

Importar Excel

1. Selecione o arquivo em Importar empresas e vagas.
2. Use Posição e Empresa ou Nome para contagem; preencha opcionais conforme o formato.
3. Pré-visualize empresas e alterações.
4. Corrija antes de confirmar.
5. Confira totais e transferências.

As vagas das empresas da carga são substituídas pelas da planilha. Uma posição de outra empresa pode ser transferida. Confira esse efeito antes de importar.

Compartilhar cota

Na aba Vagas, selecione Empresa como responsável. Pessoas e visitantes vinculados compartilham seu limite. O visitante também pode usar a cota própria de uma pessoa. Quem usa cota empresarial não fornece automaticamente uma cota pessoal.

Com cinco vagas, três veículos de pessoas e dois de visitantes dentro, a próxima entrada é negada até uma saída. O cadastro não reserva antecipadamente uma vaga.

Vínculos com veículos dentro são protegidos. Antes de trocar responsável ou reduzir cota, confira a ocupação real e corrija os registros quando necessário.

9 Departamentos e grupos

Onde acessar: Cadastros → Departamentos e grupos.

Grupos organizam a concessão de regras para várias pessoas. Departamentos representam a estrutura da instituição; empresas possuem tela própria.

1. Pesquise antes de criar.
2. Escolha Tipo e Nome.
3. Configure Desativar anti-dupla entrada para este grupo somente quando necessário.
4. Salve e associe as pessoas pela aba Grupos ou pela gestão de membros.
5. Inclua o grupo em uma regra com áreas e horários.

Ao alterar grupos, confira as regras recebidas e o envio aos dispositivos. Grupo sem regra não concede entrada. A exceção de anti-dupla entrada não ignora validade, restrição, horário ou cota.

10 Áreas e ocupação lógica

- **Nome** e tipo: **Área externa** representa a rua — quem entra nela deixa de contar como presente.
- **Anti-dupla entrada**: bloqueia quem tenta entrar de novo sem ter saído.
- **Capacidade** (opcional): lotação máxima (modo online).

Configurar e conferir

1. Crie a área externa da rua ou saída.
2. Cadastre áreas internas com nomes claros.
3. Defina capacidade onde haverá contagem controlada.
4. Escolha anti-dupla entrada conforme o processo.
5. Vincule origem e destino nas portas.
6. Selecione as áreas nas regras.

Destino é o local para onde a pessoa vai após a passagem. Áreas invertidas causam presença e sentido incorretos. O sensor de porta aberta não altera sozinho a localização da pessoa.

11 Horários de acesso

Cada horário tem uma ou mais **faixas**: dias da semana + hora inicial e final. Faixas em que o fim é menor que o início atravessam a meia-noite (ex.: 22:00 até 06:00). Uma regra **sem horário** vale **sempre**.

Criar um horário

1. Adicione e dê um nome claro.
2. Inclua faixas, dias e Início e Fim.
3. Confira a faixa noturna se atravessar a meia-noite.
4. Salve e vincule à regra.
5. Confira o resultado por meio das regras e eventos.

Horário sem regra não muda o acesso. Regra sem horário vale continuamente. Horários de refeição são configurados no próprio Refeitório.

12 Regras de acesso

Onde acessar: Acesso → Regras de acesso.

Assistente de configuração

1. Em Nova regra, informe Nome, Prioridade e situação habilitada.
2. Em Quem, escolha pessoas e grupos.
3. Em Quando, selecione horários; nenhum significa funcionamento contínuo.
4. Em Onde, escolha áreas.
5. Revise o resumo e conclua.

A prioridade maior é avaliada primeiro. Exemplo: crie Administrativo diurno ligando o grupo Administrativo ao horário de segunda a sexta e à área Recepção. A porta deve ligar Rua à Recepção, e a pessoa deve pertencer ao grupo e ter credencial válida.

Condições de acesso

Identificação, situação ativa, exceção/restrição, validade, sentido, área, anti-dupla entrada, regra, horário e capacidade podem impedir a entrada. Garagem pode verificar vagas e financeiro. Facial verifica também template, similaridade e câmera. O motivo registrado mostra qual condição impediu o evento.

Depois de alterar

Confira cadastros afetados e sincronização. Equipamentos standalone precisam receber os dados aplicáveis; verificações do servidor precisam de comunicação. Desabilitar uma regra pode retirar acesso de vários grupos.

Regra geral de acesso não concede benefício de refeição.

13 Dispositivos e controladores

Cadastrar um iDFace

+ **Adicionar** (admin): nome, modelo, **IP**, porta (80), usuário e senha da tela web do equipamento. Em **Portas / leitoras**, defina para cada porta a **área de origem** → **área de destino**.

Somente leitura gerenciado

Todo equipamento novo entra em **SOMENTE LEITURA**: o JNAccess acompanha status e acessos, mas **não altera nada** no equipamento. Para gerenciar, use **Assumir gerenciamento...** — o sistema mostra antes quantos cadastros de outro sistema existem lá (ex.: iDSecure) e pede para digitar o nome do equipamento.

No envio normal de dados, o JNAccess preserva cadastros fora de sua faixa de identificadores. A ferramenta separada **Apagar usuários do equipamento**, no Launcher, permite excluir também cadastros de outros sistemas quando o administrador escolhe explicitamente esse escopo e confirma a operação.

Catraca iDFace

Para iDFace ligado a uma catraca, marque **Catraca** no cadastro. Um ícone de catraca aparece ao lado do modo (online) no card do equipamento.

Com a opção marcada, o **sentido de passagem é deduzido**:

- quem está **fora** da área de destino da porta está **entrando** (valem as regras, horários e lotação);
- quem já está **dentro** está **saindo** e volta para a área de origem. Se a origem é a área externa, a saída é liberada sem precisar de regra.

A porta precisa ter **as duas áreas** configuradas (ex.: Rua (externa) → Área Interna). Passar de novo não é bloqueado como dupla entrada — conta como saída. A dedução acontece no **modo online**. Os eventos mostram → **Entrada** / ← **Saída**.

Garagem controle de vagas

Marque **Garagem** no cadastro do equipamento que controla o portão da garagem (um ícone de garagem aparece no card). Configure as portas: **entrada** com destino na área da garagem e **saída** com destino na área externa (ou use **Catraca** para deduzir o sentido).

- Cada **entrada** autorizada ocupa uma vaga do morador; cada **saída** libera.
- Se o morador **não tem vaga** cadastrada ou **todas as vagas estão ocupadas**, a entrada é **bloqueada** ("Limite de vagas da garagem atingido (2/2)") e abre um **aviso na tela**, em qualquer página do sistema, com a foto, o nome, o motivo e as placas.

As regras de acesso continuam valendo (a pessoa precisa de regra para a área da garagem). O controle de vagas acontece no **modo online**.

Catraca iDBlock Next

Cadastre em **Dispositivos** > + **Adicionar** com o modelo **iDBlock Next** e o IP do equipamento **principal** (o secundário recebe tudo dele — nunca cadastre o secundário). Na porta, informe a área de **origem** (fora, ex.: Rua) e a de **destino** (dentro).

- **Giro de ENTRADA**: horário ou anti-horário — o sentido do braço de quem entra.
- **Leitora do lado de FORA**: qual iDFace fica do lado de quem entra (**principal** ou **secundário**). No modo online a catraca informa qual leitora reconheceu o rosto: a de fora libera o giro de entrada, a

de dentro libera o de saída. Escolha **Deduzir pela área** se preferir o comportamento do "iDFace com catraca" (quem está dentro está saindo).

- Ao liberar, o JNAccess manda a catraca girar **só no sentido da passagem** (ação catra).
- **Ativar modo online** também configura a catraca para avisar o JNAccess de cada **giro e desistência**. Se a pessoa foi liberada e não passou, o evento aparece como **Desistência** e ela volta para a área onde estava.
- Botões do card: **Liberar entrada**, **Liberar saída** e **Catraca** (papel principal/secundário, giro de entrada, tempo de liberação e contadores de giros; com o gerenciamento assumido, **Gravar configuração** grava o giro de entrada e o tempo de liberação no equipamento). No Monitoramento, a catraca tem os botões **Entrada** e **Saída**.
- O JNAccess não altera o papel principal/secundário: trocá-lo reinicia a catraca e apaga o banco dela.
- **Captura de face pela catraca**: na aba Face da pessoa, escolha **<catraca> — iDFace principal**. Para capturar pelo outro lado, informe no cadastro da catraca o **IP do iDFace secundário** (mesmo usuário e senha do principal; o IP precisa responder na rede do servidor) e escolha **<catraca> — iDFace secundário**. A foto fica no cadastro da pessoa e segue para a catraca no envio automático (o principal repassa ao secundário). Esse uso do secundário não consta na documentação da Control iD: se ele não responder, capture pelo principal.

Troca de servidor ou de IP reapontamento

No modo online o equipamento guarda o endereço do servidor que ele chama. Depois de trocar o servidor do JNAccess (ou se o IP dele mudar), o equipamento continua chamando o endereço antigo, entra em contingência e passa a **negar**.

- **Reapontar para este servidor** (topo da tela Dispositivos): regrava em todos os equipamentos **gerenciados e em modo online** o endereço deste servidor (e, nas catracas, o endereço de aviso de giros). Mostra quais foram reapontados e quais não responderam. Fica registrado na Auditoria.
- **Reapontar automaticamente** (só admin, desligado por padrão): na partida do servidor e a cada 5 minutos faz a mesma conferência sozinho. **Use só com UM servidor JNAccess na instalação** — dois servidores ligados tomariam os equipamentos um do outro.
- Equipamentos em **somente leitura** nunca são reapontados.
- Para não depender do IP, informe no instalador um **nome de rede** (ex.: jnaccess.empresa.local) em vez do IP e reserve IP fixo para o servidor.

Ações do card

Botão	O que faz
Testar conexão	Verifica se o equipamento responde e com que usuário/senha.
Diagnóstico	Checklist de instalação: conexão, relógio e fuso dos logs, modo online apontando para o servidor certo, modo de exceção, cadastros enviados, portas e armazenamento — cada item com a correção sugerida. Rode sempre que instalar um equipamento.
Abrir porta	Libera a porta/catraca remotamente (registra "Abertura via web").
Enviar dados	Envia ao equipamento só o que mudou: pessoas, cartões, faces, grupos, áreas, horários e regras. Enviar dados a todos faz isso em todos.
Ajustar hora	Acerta o relógio do equipamento pelo do servidor.
Modo: Normal / Emergência / Trancado	Modo de exceção só deste equipamento.
Ativar / Desativar modo online	No online, o iDFace pergunta ao JNAcess a cada rosto (regras mudam na hora, anti-dupla entrada global, alarme imediato). Se o servidor cair, só as pessoas em contingência passam.
Importar pessoas e eventos	Traz para o JNAcess quem já está cadastrado no equipamento (ex.: pelo iDSecure), com cartões, departamentos e, se quiser, fotos, e o histórico de acessos. Não altera o equipamento. As pessoas importadas não ganham acesso automaticamente — crie as regras.
Reiniciar	Reinicia o equipamento.
Editar / Remover	Altera o cadastro ou remove o equipamento do JNAcess.

Equipamentos Henry

A tela oferece modelos Henry conforme os drivers. Escolha o modelo correto, configure IP, porta de comunicação e portas lógicas. Para dois leitores, confira entrada, saída e IP da controladora conforme os campos apresentados.

Use Testar conexão e Diagnóstico antes de operar. Sentido e áreas continuam necessários para interpretar a passagem. Não copie protocolo ou credenciais de um Control iD sem conferir o modelo Henry.

JC 013

A Valle JC-013 tem configuração própria de seis acionamentos e sensores, explicada no próximo capítulo. Não utiliza envio de pessoas e faces de um iDFace. O reconhecimento no servidor identifica a pessoa e direciona a abertura para o relé vinculado.

Conferência da implantação

Confira modelo, IP, comunicação, gerenciamento, portas, áreas, direção e credenciais. Acompanhe uma passagem. Testar conexão comprova comunicação, mas não comprova a ligação física do relé à porta correta.

14 Placa Valle JC 013 e porta aberta

Onde acessar: Acesso → Dispositivos → Adicionar ou Editar → modelo Valle JC-013.

Função da placa

A JC-013 comunica pela rede e oferece saídas S1 a S6 e entradas A1 a A6. Cada relé habilitado pode atender uma porta lógica do controle geral. Um sensor opcional acompanha essa mesma porta. As aberturas usam pulso; a integração não apresenta botão para manter a saída permanentemente ligada.

A placa não cadastra pessoas nem reconhece faces. Recebe uma abertura decidida pelo servidor ou por operador autorizado. Equipamentos do refeitório possuem fluxo próprio e não entram nessa associação geral.

Cadastrar e configurar

1. Em Dispositivos, adicione uma Valle JC-013.
2. Informe Nome, IP e porta HTTP da placa; não use a senha de um leitor biométrico.
3. Confira as seis portas do formulário, seus nomes e áreas de origem e destino.
4. Na seção de acionamentos, marque somente os canais usados.
5. Para cada canal, escolha Porta associada, pulso e sensor.
6. Salve e use Testar conexão.
7. Confira no monitor uma porta aberta e fechada e acompanhe um acionamento físico por vez.

Ter um acionamento habilitado coloca a placa sob gerenciamento dessa integração. Canal desabilitado impede a abertura. A placa precisa estar habilitada e gerenciada.

Campos por acionamento

Campo	Significado
Habilitar acionamento S1 a S6	Permite usar o relé selecionado.
Porta associada	Escolhe a porta lógica, inclusive de outro equipamento do controle geral.
Tempo do pulso	100 a 10000 ms; padrão 2000 ms.
Entrada do sensor	Sem sensor ou A1 a A6 conforme a ligação.
Avisar se permanecer aberta	0 a 3600 s; padrão 30 s; 0 desativa.
Alerta de porta aberta	Liga ou silencia avisos sem desligar o sensor.
Inverter aberto e fechado	Troca interpretação das faixas.
Faixas de leitura	Limites dos estados aberto, fechado e intermediário.

Uma porta não pode estar associada a mais de um acionamento nessa integração. Se o canal atender uma porta de outro controlador, mantenha a porta lógica nas regras e na câmera; o sistema encaminha a abertura para a JC-013.

Vincular ao ponto de acesso facial

1. Habilite o canal e escolha a Porta associada na JC-013.

2. Salve a placa.
3. Abra Reconhecimento Facial → Câmeras → Editar.
4. Em Ponto de acesso, escolha a porta com a placa e o relé S; o sensor A aparece quando configurado.
5. Confira Sentido e modo teste e salve.

A seleção oferece acionamentos habilitados de placas habilitadas e gerenciadas. Canal desabilitado não aparece como opção disponível. Um vínculo anterior indisponível é indicado para correção. A seleção escolhe a porta de acesso; o sensor é configurado no canal que a atende.

Interpretar sensores

Dispositivos e Monitoramento mostram relé, nome da porta, entrada do sensor e estado. Aberta e Fechada correspondem às faixas configuradas; Indeterminada indica leitura entre limites; Sem leitura indica ausência ou invalidez da leitura. Sem sensor não existe monitoramento físico da porta.

O padrão do driver usa 0 a 200 como aberta e 801 a 1023 como fechada. A faixa intermediária é indeterminada. Confira com a porta fisicamente aberta e fechada e ajuste inversão e limites conforme a montagem. Ausência de comunicação não comprova porta fechada.

Popup e opção de desabilitar

O popup aparece quando a leitura fica continuamente aberta além do tempo configurado. Mostra porta, placa e início da abertura e pode aparecer em qualquer tela com sessão autenticada. Se houver várias portas, os avisos são apresentados em sequência.

- Entendi fecha o aviso daquele período contínuo de abertura.
- Desabilitar alerta desta porta silencia os próximos avisos do canal e registra a alteração. Exige alterar Dispositivos.
- Quando a porta fecha, a condição termina. Uma nova abertura prolongada pode gerar outro aviso.
- Sem comunicação, o sistema deixa de considerar o estado como leitura válida.

Para reativar, edite a JC-013 e marque Alerta de porta aberta. Confira também tempo maior que zero. A leitura do sensor e o acionamento continuam ativos quando somente o alerta é desabilitado.

Exemplo

Na placa Portas bloco A, configure S2 para Recepção, pulso 2000 ms, sensor A4 e alerta 30 s. Na câmera, escolha Recepção com essa placa e S2. A abertura usa S2 e a leitura usa A4; os números não precisam coincidir.

Diagnóstico

Se a porta não aparecer na seleção, confira placa, canal, gerenciamento e vínculo salvo. Se não abrir, confira relé, pulso e ligação física. Se leitura invertida, confira sensor e inversão. Se não alertar, confira entrada, limites, tempo maior que zero, alerta habilitado e comunicação.

O protocolo implementado consulta o estado via HTTP e utiliza S1ON a S6ON e S1OFF a S6OFF. Não é necessário digitar esses comandos no uso diário. A ligação elétrica deve ser conferida pelo responsável técnico conforme o equipamento instalado.

15 Monitoramento e abertura manual

É a tela inicial: o que está acontecendo agora.

- **Indicadores:** autorizados e negados hoje, **presentes agora**, visitantes válidos e equipamentos online. O selo **• Ao vivo** indica que a tela recebe os eventos em tempo real.
- **Últimos eventos:** cada acesso aparece na hora, com a **foto da pessoa**, o tipo de evento, a área, o equipamento e o motivo (ex.: "Regra: Colaboradores", "Cadastro inativo", "Fora do horário permitido"). Em equipamentos com **catraca**, aparece a etiqueta → **Entrada** ou ← **Saída**. Se a pessoa não tinha foto no JNAccess, o sistema busca a foto no próprio iDface na primeira passagem.
- **Alarme:** tentativa de alguém da lista de exceção aparece destacada em vermelho, com faixa de alarme no topo da tela.
- **Equipamentos:** situação de cada iDface (ponto verde = comunicando) e o botão **Abrir** para liberar a porta remotamente. A abertura aparece uma única vez como **Abertura via web**, com o nome do operador.
- **Modo de exceção** (todos os equipamentos de uma vez):
- **Emergência — liberar tudo:** todas as portas liberadas (incêndio, evacuação).
- **Trancar tudo:** tudo bloqueado, ninguém entra — nem com face (invasão).
- **Normalizar:** volta ao funcionamento normal.

Enquanto um modo de exceção estiver ativo, uma faixa amarela/vermelha fica visível em todas as telas. Toda mudança é registrada na auditoria e notificada.

- **Acessos por hora (hoje):** gráfico de autorizados × negados.

JC 013 no monitor

A placa mostra seis canais, porta e sensor. Acionar S1 a S6 envia um pulso; o botão fica indisponível quando o canal ou a placa não permitem abertura. Confira porta e motivo antes de acionar. A abertura registra o operador, mas não substitui identificação de uma pessoa.

Atender negativa

1. Leia nome, horário, equipamento e motivo.
2. Confira a condição no módulo indicado.
3. Corrija cadastro ou configuração apenas após conferir o problema.
4. Se usar abertura manual, siga o procedimento autorizado da instalação.
5. Acompanhe passagem e estados.

Modo de exceção é amplo nos controladores que o suportam. Não use para corrigir um cadastro. Não presuma que saídas por pulso da JC-013 permanecem liberadas como as de outro controlador.

16 Ocupação e presença

Mostra quantas pessoas e visitantes estão **agora** em cada área interna, com barra de lotação quando a área tem **capacidade** definida.

No modo online, quando a área atinge a capacidade, novas entradas são negadas ("Lotação máxima de Laboratórios (40/40)") e o sistema avisa. A contagem depende das passagens registradas: se alguém sair sem passar pela leitora, corrija em **Relatórios › Status atual › marcar saída**.

Conferir e corrigir

1. Abra Ocupação e veja contagem e capacidade por área.
2. Para uma inconsistência, consulte Relatórios → Status atual.
3. Confirme a saída física da pessoa.
4. Use Marcar saída com a permissão correspondente.
5. Confira o resultado na área.

A contagem vem das passagens e do sentido configurado. Sensor de porta informa estado da porta, não quantidade de pessoas. Garagem conta veículos por cota e não equivale à ocupação de pessoas.

17 Relatórios e auditoria

Relatório de acessos (primeira aba) — lista **quem entrou**, com o **horário da primeira entrada do dia** e o **dispositivo**, o **total de pessoas** e um gráfico de **entradas por dispositivo**.

- **Filtros**: data inicial e final (atalhos **Hoje**, **Ontem**, **7 dias**, **Este mês**), **hora de / até** (ex.: quem entrou depois das 08:00), **dispositivo**, **área**, **departamento/grupo**, **tipo** (pessoas, visitantes ou ambos) e **nome**.
- **Só a primeira entrada do dia** (marcado): uma linha por pessoa por dia. Desmarcado: todas as entradas.
- Conta só acessos **autorizados**; em catracas, só o sentido **entrada**.
- **Imprimir** gera a folha com o cabeçalho do JNAccess, o período, os filtros aplicados, a tabela e o total (o gráfico aparece só na tela). **Exportar CSV** abre no Excel.

Frequência: escolha o período (De/Até) e, se quiser, o departamento ou empresa, a **função** e a pessoa. Em **Gerar**, **Total por pessoa** mostra **Nome**, **Função**, **Dias** (dias com acesso), **Total de horas** e **Média de horas**; **Dia a dia (individual)** mostra, para cada pessoa, a data, o primeiro e o último acesso e as horas do dia, com subtotal. As horas de um dia vão do primeiro ao último acesso autorizado. Para plantões que passam da meia-noite (ex.: 19h às 7h), marque **Plantão com virada do dia** e informe a duração máxima do plantão (**Plantão de até (h)**, padrão 14): a jornada conta inteira no dia em que começou, e o último acesso no dia seguinte aparece com "(+1)". Marque **Incluir quem não teve acesso** para listar também quem ficou com 0 dias. **Exportar CSV** e **Imprimir**. A função é preenchida no cadastro da pessoa (campo **Função**).

Empresas: lista as empresas com **Empresa**, **Sala**, **CNPJ**, **Quantidade de vagas** e **Vagas numeradas** (em faixas, ex.: 65, 98-99, 101, com a garagem abaixo), e os totais de empresas e vagas. Há busca por empresa, sala ou CNPJ, **Exportar CSV** e **Imprimir**.

Pessoas por empresa: lista pessoas e visitantes com tipo, empresa · sala, matrícula, CPF, cartões, validade e situação (Ativo, Inativo, Vencido ou Lista de exceção). O visitante aparece na empresa visitada. Os filtros são: **Empresa** (inclusive "Sem empresa"), **Tipo**, **Situação** e busca por nome, matrícula ou CPF. Com **Agrupar por empresa** marcado, o relatório sai separado por empresa, com a quantidade de pessoas de cada uma; desmarcado, sai em lista única com a coluna Empresa. O operador só vê os tipos de cadastro que tem permissão para ver (Pessoas e/ou Visitantes). **Exportar CSV** e **Imprimir**.

Veículos (placa) — digite a placa inteira ou parte dela (com ou sem traço) para achar o **morador associado**: veículo, foto, nome, contato, departamento/unidade e vagas (veículos na garagem agora / vagas). Também busca por nome, marca ou modelo. **Exportar CSV** e **Imprimir**.

Eventos — filtre por período (De/Até), evento, dispositivo, área e pessoa; **Exportar CSV** abre no Excel com acentos corretos.

Status atual (presentes) — quem está em cada área agora. **marcar saída** corrige quem saiu sem passar na leitora (libera a anti-dupla entrada e a ocupação).

Auditoria — tudo o que os operadores fizeram (login, cadastros, aberturas, modo de exceção, importações...), com data, operador e detalhes.

Códigos de evento

Evento	Significado
Acesso autorizado	Liberado (face, cartão ou QR).
Acesso negado	Bloqueado — veja o motivo.
Não identificado	Rosto/cartão não cadastrado no JNAccess.

Evento	Significado
Abertura por botoeira	Botão de saída físico.
Abertura via web	Aberto pelo painel (mostra o operador).

Procedimento de consulta

1. Escolha a aba adequada ao objetivo.
 2. Defina período e filtros e confira primeira entrada ou todas as passagens.
 3. Gere e compare totais e detalhes.
 4. Exporte ou imprima o necessário.
 5. Para alterações e comandos, consulte data e operador na Auditoria.
- Frequência calcula intervalos observados em acessos e não comprova automaticamente jornada trabalhada. Status atual mostra presença, enquanto Eventos mostra histórico.

18 Reconhecimento facial por câmera IP

Onde acessar: Reconhecimento Facial → Painel e Câmeras e Reconhecimento Facial → Eventos.

Funcionamento e requisitos

Uma câmera IP fornece vídeo RTSP ao servidor. O serviço JNAccess-Facial detecta rostos, compara com templates válidos e envia o resultado. A câmera é fonte de imagem; a decisão de acesso é feita no JNAccess. Um leitor iDFace utiliza sua própria integração, diferente das câmeras IP.

São necessários câmera alcançável pelo servidor, RTSP habilitado, credenciais corretas, serviço facial em funcionamento e biometria válida. Para liberar, também é necessária uma porta habilitada, regra válida e câmera fora do modo teste.

Painel

Confira situação do serviço, câmeras ativas, pessoas na galeria, imagens válidas, pendências e erros. A tabela mostra conexão, quadros, rostos e diagnóstico. A pessoa na galeria deve ter pelo menos uma imagem processada válida; ter somente foto no cadastro não basta.

Se o serviço não responder, confira o serviço Windows JNAccess-Facial e o diagnóstico. Pendências podem aguardar seu retorno. JNAccess é o serviço do painel; JNAccess-Facial é o serviço do reconhecimento.

Cadastrar uma câmera

1. Na aba Câmeras, clique em Câmera.
2. Informe Nome e Local para identificar o ponto.
3. Informe IP, Porta RTSP, Usuário e Senha conforme a câmera. Padrão RTSP é 554, mas pode ser diferente.
4. Escolha fabricante; use URL RTSP somente quando o padrão não atender. Não escreva a senha dentro da URL.
5. Configure quadros por segundo, intervalo entre eventos e política de imagens.
6. Escolha Ponto de acesso e Sentido quando for usar liberação.
7. Configure Zona de reconhecimento, Habilitada e Reconhecimento ligado.
8. Mantenha Modo teste durante a primeira conferência e salve.
9. Use Testar conexão e Imagem antes de comparar o reconhecimento.

Campo de senha vazio em uma edição preserva a senha existente. Não copie credenciais para relatórios ou fotos da tela. A chave de acesso da câmera deve ser obtida no aplicativo/configuração do fabricante e informada no campo de autenticação utilizado pela instalação.

Parâmetros principais

Campo	Como usar
Quadros por segundo	Quantidade analisada; faixa da tela 0,5 a 15.
Limiar de similaridade	Vazio usa configuração global; maior é mais exigente.
Intervalo entre eventos	Evita repetição da mesma pessoa em curto período.
Guardar imagem	Nenhuma, desconhecidos ou todos conforme a política escolhida.
Ponto de acesso	Seleciona uma porta específica; JC-013 mostra relé habilitado e sensor.
Sentido	Entrada ou Saída conforme o ponto físico.
Modo teste	Identifica e registra sem liberar.
Habilitada	Permite que o serviço abra o vídeo.
Reconhecimento ligado	Ativa identificação; vídeo de diagnóstico pode ser usado separadamente.

Cadastrar biometria da pessoa

1. Abra Pessoas ou Visitantes e salve a ficha se ainda for nova.
2. Entre na aba Face e localize Biometria facial — câmeras IP.
3. Use Enviar arquivo, Usar a foto do cadastro ou selecione a câmera e Capturar.
4. Utilize imagem frontal, nítida e bem iluminada. Na captura, mantenha a pessoa sozinha, parada e de frente.
5. Aguarde o processamento. Processando indica pendência; válida permite uso; recusada mostra o motivo.
6. Cadastre outras imagens de boa qualidade se necessário, respeitando o máximo indicado pela tela.
7. Confira no painel a presença na galeria e observe os eventos.

A imagem é processada em um template cifrado; a galeria não expõe o template ao operador. Excluir um template reduz as amostras daquela pessoa. Excluir toda a biometria faz a pessoa deixar de ser reconhecida pelas câmeras IP. Revogação de biometria também impede esse acesso.

Monitor ao vivo e zona

Na aba Monitor ao vivo, selecione a câmera habilitada e aguarde Ao vivo. A imagem mostra a área de reconhecimento. Use Pausar ou Retomar conforme a tela. Atualizar câmeras recarrega a lista.

Para definir a área, edite a câmera e ajuste Esquerda, Direita, Topo e Base em porcentagens. Os valores 0, 0, 100, 100 usam a imagem inteira. A largura e altura precisam atingir o mínimo aceito. Confira em Imagem e no monitor que o rosto no ponto de passagem permanece dentro da zona.

O monitor não é gravação contínua de CFTV. A política Guardar imagem se aplica aos eventos conforme configurado. Abrir o vídeo não comprova que o reconhecimento está ativo.

Escolher a porta certa

Ponto de acesso lista portas dos controladores e os acionamentos JC-013 disponíveis. Na JC-013, configure e salve primeiro canal, Porta associada e sensor. Depois escolha a opção com nome da porta, placa, S e A.

A abertura utiliza exatamente a porta selecionada. Não é necessário que a porta seja número 1. Se o ponto vinculado ficar indisponível, edite e escolha um ponto válido. O monitoramento de porta aberta usa o sensor ligado ao canal dessa porta, não a câmera de vídeo.

Liberar após reconhecer

1. Confira reconhecimento correto no modo teste.
2. Confira regra, validade, credencial e a porta escolhida.
3. Confirme direção e configuração de vagas se for garagem.
4. Desative Modo teste na câmera quando a instalação estiver pronta para liberar.
5. Acompanhe um evento e uma passagem no local.
6. Confira resultado, motivo e confirmação de abertura no histórico.

Reconhecer a pessoa não garante abertura: o sistema ainda avalia cadastro ativo, biometria não revogada, similaridade suficiente, equipamento, porta, regras e condições de acesso. Garagem pode negar por cota. Uma falha de comando é registrada como erro, sem declarar a abertura confirmada.

Eventos e imagens

Consulte por período, câmera, pessoa e resultado conforme os filtros da tela. Confira nome, similaridade, motivo, modo teste e abertura. Imagens só existem quando a política e o processamento produziram um registro. A consulta de evidências é autenticada e auditada.

Configuração global

A aba Configuração é administrativa. Contém limiar, margem para a segunda pessoa mais parecida, quadros de confirmação, qualidade mínima, parâmetros de detecção e retenção de eventos e imagens. Alterações podem levar um intervalo de atualização do serviço para entrar em vigor. Use as faixas e padrões da tela e ajuste uma condição por vez.

Não reduza a exigência de comparação para compensar uma imagem escura ou um cadastro inválido. Primeiro confira foco, iluminação, tamanho do rosto, zona e qualidade dos templates.

Resolver falhas

Sintoma	Conferir
Sem vídeo	IP atual, RTSP habilitado, porta e credenciais, acesso pela rede do servidor.
Vídeo sem identificação	Reconhecimento ligado, zona, serviço e tamanho/qualidade do rosto.
Foto existe mas não reconhece	Template de câmera IP válido, galeria e resultado do processamento.
Identifica mas não abre	Modo teste, ponto de acesso, direção, regras, vagas e motivo do evento.
Porta errada	Porta selecionada e vínculo entre porta lógica e relé da JC-013.
Reconhecimento repetido	Intervalo entre eventos e permanência da pessoa no enquadramento.
Popup de vaga ausente	Evento de bloqueio por vaga, sessão ativa e condição da cota.

Na IM5-SC, após reconfiguração confira novamente IP e RTSP: o endereço pode mudar. Os procedimentos de rede e autenticação devem seguir a configuração real da câmera; não reutilize IP ou chave antiga sem verificar.

19 LPR e leitura de placas

Onde acessar: Gestão de garagem → LPR · Placas.

Finalidade e modos

O LPR lê a placa do veículo no vídeo RTSP e registra a decisão no servidor. A placa pode ser credencial da garagem. A leitura é distinta do reconhecimento facial e depende do enquadramento da placa, do serviço LPR e do cadastro do veículo.

Modo teste / somente leitura registra placas sem abrir a cancela. Não exige um proprietário ou ponto de abertura para monitorar. Controle de acesso usa o veículo, a pessoa, a porta/relé da cancela e as regras de autorização.

Cadastrar um veículo

1. Na aba Veículos, adicione e escolha Proprietário.
2. Digite a placa no formato antigo ou Mercosul; pode ser normalizada sem traço.
3. Preencha Tipo, Marca, Modelo, Cor e Observações quando necessários.
4. Defina Válido até se o vínculo tiver prazo.
5. Marque Ativo e salve.
6. Confira vaga, situação e regra de acesso do proprietário.

Veículo inativo não libera a cancela. A mesma placa não deve ser usada em proprietários diferentes. Placa reconhecida sem veículo ou pessoa válida pode aparecer no monitor sem autorização.

Configurar uma câmera LPR

1. Abra Câmeras e adicione Nome, Local, IP, Porta RTSP e autenticação.
2. Escolha fabricante ou informe URL RTSP quando necessário; mantenha senha fora da URL.
3. Comece em Modo teste / somente leitura.
4. Ajuste quadros por segundo, confiança mínima e cooldown por placa.
5. Escolha se deve guardar imagem de evidência.
6. Ative e salve; teste conexão e confira o monitor.
7. Para Controle de acesso, selecione Cancela, Porta/relé e Sentido e confira o cadastro do proprietário e a cota.

A confiança mínima impede abertura abaixo do valor configurado. Leituras repetidas no cooldown podem aparecer ao vivo sem novo acionamento. Guardar imagem salva evidência do evento, não vídeo contínuo.

Área de leitura e linha

Na aba de monitor LPR, escolha a câmera. Use Editar área de leitura para ajustar a região onde as placas devem ser procuradas. Salvar área aplica o recorte; Restaurar padrão e Usar imagem inteira permitem voltar a uma referência.

A linha de leitura ajuda a observar o ponto da imagem em que os veículos são lidos. Ajuste com os veículos no fluxo real. Não estreite a região a ponto de excluir a placa durante a aproximação.

O teste de alcance mostra tamanho real da placa, confiança e tempos. Testar desempenho da ROI compara a área com a imagem inteira. Essas informações são diagnóstico e não confirmação de liberação.

Homologação e controle

1. Faça leituras em teste com placas da instalação e iluminação habitual.
2. Confira texto, confiança e associação ao veículo correto.
3. Confira portão, relé, direção e regras.
4. Altere para Controle de acesso e confirme a mudança na tela.
5. Acompanhe uma passagem e confira abertura e ocupação.

Trocar de modo não apaga o histórico de teste. O controle depende da autorização e da resposta do equipamento. Na JC-013, uma porta já vinculada ao relé utiliza a associação da placa.

Eventos de placas

Na aba Eventos, selecione o período e consulte placa, câmera, pessoa, ponto de acesso, resultado e motivo. Ver decisão mostra o detalhamento disponível. Abra a imagem de evidência quando ela existir.

Se a placa for lida mas não abrir, confira confiança, formato, modo teste, cadastro, validade, regras, cota e resposta do controlador. Se a placa estiver incorreta, ajuste enquadramento e qualidade antes de mudar as condições de abertura.

20 Monitor de Eventos LPR

Onde acessar: Gestão de garagem → Monitor de Eventos LPR.

Acompanhar ao vivo

1. Abra a tela e selecione câmera e período conforme o atendimento.
2. Mantenha Atualização automática ativa para acompanhar novas leituras.
3. Veja placa, resultado, motivo, pessoa e ponto de acesso.
4. Use Ampliar imagem para conferir a evidência disponível.
5. Carregue eventos anteriores quando precisar investigar o histórico.

O monitor reúne leituras instantâneas e eventos gravados. As medições de quadros e tempos de leitura são diagnóstico; nem toda leitura repetida vira um novo registro ou comando por causa do cooldown. Use o histórico para comprovar a decisão registrada.

Procedimento da portaria

Quando houver negativa, leia o motivo e confirme o cadastro correspondente. Uma leitura de placa não deve ser confundida com autorização. Em caso de atendimento manual, confira a pessoa e utilize a rotina autorizada de abertura.

Sem imagem, confira a política de evidências. Sem eventos, confira câmera, período, serviço e filtro. Tela aberta com informação antiga não comprova leitura atual; confira data e estado de atualização.

21 Garagem cobranças e recebimentos

Preparação e permissões

O menu **Gestão de garagem** → **Garagem** reúne Cobranças, Recebimentos, Pessoas vinculadas, Modalidades e valores e Configurações. O administrador possui acesso inicial. Em **Permissões**, autorize os demais operadores conforme sua função: consultar, inserir ou alterar. Configurar integrações exige a permissão de alterar. A ação excluir está reservada; não disponibiliza cancelamentos nesta versão.

Antes de ativar, confira os cadastros das pessoas, configure o provedor de pagamentos e o e-mail, e faça uma homologação. O módulo começa desativado. O servidor precisa permanecer em funcionamento para gerar, emitir e consultar cobranças e enviar e-mails.

Modalidades valores e cotas

Abra **Modalidades e valores**, crie uma modalidade, informe seu nome, periodicidade, valor por cota, antecedência de geração e tolerância. Marque a opção de bloqueio por atraso quando aplicável.

Modalidade	Intervalo entre vencimentos
Diária	1 dia
Semanal	7 dias
Mensal	1 mês
Trimestral	3 meses
Semestral	6 meses
Anual	12 meses

Os meses seguem o calendário. Uma mensalidade ancorada em 31 de janeiro vence em 28 ou 29 de fevereiro e retorna a 31 em março. Uma diária é um ciclo de cobrança por data; não representa o passe de visitante com 24 horas de validade.

Exemplo: valor por cota de R\$ 150,00 e quantidade de 2 cotas produzem uma cobrança de R\$ 300,00 por ciclo. As cotas financeiras não alteram automaticamente o número físico de vagas nem as regras de acesso. Não há cálculo proporcional, juros ou multa pelo JNAccess; verifique também as condições da conta do provedor.

A mudança de preço vale para cobranças futuras. Cobranças já geradas mantêm os valores, quantidade e tolerância registrados. A periodicidade de uma modalidade que possui vínculos não pode ser alterada: crie outra modalidade e ajuste os vínculos.

Vincular pessoas

1. Abra **Pessoas vinculadas** e selecione a modalidade.
2. Selecione uma ou várias pessoas já cadastradas.
3. Informe a quantidade de cotas e o primeiro vencimento.
4. Salve e confira os vínculos criados.

Cada pessoa tem um vínculo financeiro próprio e recebe sua cobrança individual. Associar pessoas à modalidade não altera seus departamentos ou grupos de acesso. Confirme o e-mail no cadastro da pessoa; no Asaas, o CPF do pagador também é necessário.

Pausar o vínculo impede novas gerações, mas mantém as dívidas existentes. Para retomar, informe o novo primeiro vencimento. Trocar a modalidade preserva o histórico e usa o próximo vencimento nos novos ciclos. Confira datas antes de salvar: um primeiro vencimento antigo pode gerar cobranças de períodos anteriores.

Gerar e acompanhar cobranças

O servidor gera cobranças dos vínculos ativos conforme o vencimento e a antecedência definidos. Também é possível solicitar a geração na tela. A mesma pessoa vinculada não ganha outra cobrança para o mesmo vencimento apenas por repetir essa ação.

Em **Cobranças**, use a busca e os filtros, confira total, vencimento, saldo, integração e e-mail. A geração local vem antes da emissão no provedor. O link de pagamento fica disponível após a emissão. Use **Consultar / emitir no provedor** para tentar emitir ou atualizar a informação da cobrança.

O link oferece os meios de pagamento disponíveis na configuração e na conta do provedor. Cada ciclo gera uma cobrança ou link; não existe débito automático de cartão armazenado nesta versão.

Recebimentos e desbloqueio

A tela **Recebimentos** mostra pagamentos confirmados automaticamente pelo provedor e seus estornos. Não existe baixa manual nesta versão. O pagamento pode chegar por notificação automática ou por consulta periódica; comprovante apresentado pelo cliente, por si só, não equivale à confirmação no sistema.

Após o pagamento integral confirmado, o bloqueio financeiro daquela cobrança deixa de valer. Outra dívida vencida pode manter o bloqueio. Grupos, horários, validade, vagas e demais regras de acesso continuam sendo avaliados. Estornos ou contestações podem reabrir o saldo devedor.

O JNAccess não solicita cancelamentos nem reembolsos ao provedor nesta versão. Pausar um vínculo ou desligar o servidor também não cancela cobranças emitidas.

Tolerância e bloqueio de entrada

A tolerância é contada em dias corridos após o vencimento, no fuso do sistema. Exemplo: vencimento dia 10, tolerância de 2 dias; a dívida passa a bloquear novas entradas a partir do dia 13.

O bloqueio exige módulo ativo, cobrança emitida com sucesso, saldo pendente, tolerância encerrada e bloqueio habilitado naquela cobrança. Uma cobrança com falha de emissão, sem identificação no provedor, não causa bloqueio financeiro.

A saída identificada como saída não é bloqueada pela dívida. Isso não desativa outras regras do sistema. Confira a direção das portas e áreas da garagem. O controle financeiro depende do modo online: não é garantido quando o equipamento decide sozinho, em contingência ou sem consultar o JNAccess.

Configurar pagamentos e e mail

1. Em **Configurações**, escolha Asaas ou Mercado Pago. Outros bancos precisam de um conector específico.
2. Comece em uma instalação de homologação, com banco separado e credenciais de teste. Após emitir cobranças, a troca entre teste e produção é bloqueada nessa instalação.
3. Configure a credencial do provedor e a forma de pagamento. Campos secretos em branco preservam o valor já salvo. Uma nova chave deve pertencer à mesma conta.
4. Configure a URL pública HTTPS e a autenticação das notificações com apoio do responsável técnico. O Mercado Pago exige essa URL. Uma URL localhost, local ou apenas da VPN não é alcançada pelo provedor externo.

- Configure servidor de e-mail (SMTP), porta, conexão segura, usuário, senha e remetente. Ative o envio de e-mails.
- Salve, crie uma modalidade e uma pessoa de teste, ative o módulo e valide o ciclo completo antes da produção.

O e-mail contém valor, vencimento e link de pagamento. Ele é enviado após a emissão do link. **Aceito pelo SMTP** confirma a aceitação pelo servidor de e-mail, não a chegada à caixa de entrada nem a leitura. Confira spam e endereço do destinatário. Falhas são registradas e têm novas tentativas; uma interrupção durante o envio pode provocar reenvio.

Rotina e solução de problemas

Situação	Como conferir
Menu não aparece	Instalação atualizada, recarga do navegador e permissão do operador.
Cobrança não foi gerada	Módulo, modalidade e vínculo ativos; próximo vencimento e antecedência.
Sem link de pagamento	Erro de integração, credencial, ambiente e dados do pagador; tente consultar/emitir.
Pagamento ainda pendente	Consulte o provedor e verifique notificações; a consulta automática normalmente ocorre a cada 15 minutos, podendo levar mais tempo em falhas ou lotes grandes.
E-mail não enviado	Envio habilitado, e-mail da pessoa, link emitido, SMTP e mensagem de erro.
Entrada bloqueada após pagar	Saldo confirmado, outras dívidas, estorno e motivo apresentado no monitoramento.
Saída negada	Confira motivo e sentido das áreas; não atribua automaticamente a negativa ao financeiro.

Diariamente, confira falhas de emissão, e-mails e recebimentos. Faça backup do banco e preserve o histórico financeiro. As integrações passaram por testes simulados; pagamentos, SMTP e equipamento físico precisam de homologação na instalação.

Vagas e cobrança são controles diferentes

As vagas ficam nas pessoas, visitantes e empresas; as cotas financeiras determinam valor cobrado. Pagar uma cobrança não cria vaga física, grupo ou regra. Corrigir a ocupação não cancela dívida. Confira cada condição no módulo correspondente.

Aviso de garagem sem vaga

Uma entrada negada por falta de vaga ou cota ocupada pode exibir popup com pessoa, motivo e placas. O reconhecimento facial integrado também encaminha esse bloqueio. Leia o motivo e confira o responsável pela vaga antes de acionar manualmente. O aviso de vaga é diferente do popup de porta aberta, que depende de sensor.

22 Refeitório e alimentação

Onde acessar: menu Refeitório. As abas são liberadas conforme as permissões do operador.

Visão geral e sequência de implantação

O refeitório administra refeições, benefícios, cotas, acompanhantes, consumos e custos com regras próprias. Permissão de acesso ao prédio não concede refeição. Vínculo de benefício não altera automaticamente as regras do prédio.

1. Cadastre Refeitórios e pontos.
2. Configure Refeições e horários e o calendário.
3. Crie categorias, regras de benefício e preços.
4. Cadastre vínculos e escalas das pessoas.
5. Vincule os equipamentos aos pontos do refeitório.
6. Use Simular para conferir elegibilidade sem liberar nem consumir.
7. Acompanhe identificação, autorização, confirmação e consumo.
8. Confira custos, relatórios, estornos e fechamento.

Painel do dia

Use os indicadores e resumos para acompanhar atendimento, consumos e recusas do dia. Confira período e refeitório quando disponíveis. Use o monitor e os relatórios para investigar um total diferente do esperado.

Uma tentativa de identificação não é necessariamente consumo. A pessoa pode ser negada, desistir ou não passar durante a reserva. Compare a fonte do indicador antes de concluir que a cota foi consumida.

Monitor

Acompanhe as entradas, recusas e consumos em tempo real. Leia pessoa, ponto, refeição e motivo. Em falhas, confira se houve autorização e se o consumo foi confirmado. Consulte os registros quando o evento físico de giro chegar após a liberação.

Evite repetir atendimento manual sem verificar o consumo anterior: o mesmo atendimento pode já estar registrado ou reservado.

Refeitórios e pontos

1. Crie o refeitório e informe Nome, Código e Local.
2. Se necessário, associe um grupo de refeitórios para cota compartilhada.
3. Escolha o comportamento quando a catraca não alcança o servidor, conforme as opções da tela.
4. Crie os pontos de atendimento, informe Nome e Finalidade.
5. Configure Confirmação do consumo e Prazo da reserva.
6. Marque ponto ativo e salve.

O prazo de reserva aceita 5 a 600 s. Se a pessoa não passar no prazo, a reserva expira e a cota retorna, conforme a confirmação utilizada. Com iDBlock que informa giro, o consumo pode contar apenas na passagem. Sem esse evento, use o modo de confirmação na liberação, que aparece identificado nos relatórios.

A contingência Local limitado grava condições locais e reconcilia os consumos. Excessos podem aparecer como conflito. Não significa liberar sem qualquer limite.

Equipamentos do refeitório

1. Escolha Vincular equipamento ao refeitório.
2. Selecione equipamento e ponto e informe o motivo.
3. Confira comunicação e sincronização na aba Equipamentos.
4. Envie os dados e configure modo de comunicação conforme as ações disponíveis.
5. Teste identificação e confirmação de passagem.

O equipamento deixa de usar o fluxo do controle geral e passa ao domínio do refeitório. Não misture comandos e regras dos dois módulos. Para desfazer, utilize a rotina de desvinculação da tela e confira o destino.

Liberar refeição permite atendimento físico autorizado, com pessoa e motivo. A operação da aba Liberação e estorno é registro de atendimento e não abre sozinha a catraca; para abertura física use a ação do equipamento.

Refeições e horários

1. Crie tipos de refeição se os existentes não atenderem.
2. Clique em Nova janela de atendimento.
3. Selecione Refeitório e Refeição e informe Início e Fim.
4. Marque dias, vigência e se serve em feriados.
5. Defina quantidade por pessoa, escopo da cota e prioridade.
6. Ative e salve.

Campo	Efeito
Fim menor que início	Janela atravessa a meia-noite.
Fim igual ao início	Atendimento de 24 horas.
Quantidade por pessoa	Limite do período, de 0 a 20 na tela.
Escopo da cota	Define o âmbito de compartilhamento do consumo.
Prioridade	Resolve janelas sobrepostas.
Serve em feriados	Participação da janela no calendário de feriados.

A data de referência é o dia em que a janela começa. Uma ceia de segunda das 22h às 2h continua pertencendo à segunda à 1h30 de terça. Alterar a janela não zera automaticamente a cota por refeição e data de referência.

Em Exceção de calendário, escolha Data, Tipo, Refeitório e Refeição. Fechado interrompe atendimento; Feriado aplica essa condição; Horário especial utiliza a faixa informada. Confira se a exceção vale para todos ou para um ponto específico de configuração.

Benefícios e regras

1. Cadastre categorias e centros de custo quando necessários.
2. Crie regra com Nome, Categoria e Prioridade.
3. Escolha cobrança gratuita, subsidiada ou cobrada conforme as opções.
4. Se subsidiada, informe percentual ou valor fixo e o responsável pelo custo.
5. Marque refeições permitidas e cota por período.
6. Selecione os refeitórios em que vale; nenhum selecionado significa todos.

7. Se exigir escala/plantão, marque a condição e sua tolerância.
8. Ative e salve.

Maior prioridade vence quando há mais de um vínculo aplicável. O preço fica na seção de preços: escolha refeição, refeitório e regra quando aplicáveis, Valor e Vale a partir de. Confira vigência para não interpretar preço futuro como valor do atendimento atual.

Vínculos das pessoas

1. Busque a pessoa por identificação disponível na tela.
2. Clique em Conceder benefício.
3. Selecione Regra de benefício.
4. Preencha matrícula, vínculo, setor, empresa e centro de custo.
5. Defina início/fim, situação e prioridade própria se necessária.
6. Salve e use Simular.

Ativo, Suspenso e Encerrado controlam a participação do benefício. Registre motivo nas mudanças de situação. Observações devem ser administrativas; não inclua informações clínicas.

Exceção de cota permite escolher refeição, permissão, quantidade, validade e motivo com autorização específica. Escala/plantão permite informar Início, Fim e Descrição. Quem depende de plantão deve ter uma escala válida para o momento avaliado.

Simular escolhe pessoa, refeitório e momento, sem abrir catraca nem consumir cota. Leia o motivo e corrija a condição apontada antes do atendimento.

Acompanhantes

Cadastre a referência administrativa da internação, período, regra e máximo de acompanhantes simultâneos conforme a tela. Associe a pessoa acompanhante, limite de validade e motivo/responsável.

Para substituição, use Substituir no vínculo. Confira acompanhante anterior e novo, validade e cota da referência. Substituição não deve ser tratada como criação de uma refeição adicional. Ao encerrar, utilize a ação apropriada e confira os vínculos restantes.

As observações são administrativas. A referência identifica o vínculo sem exigir descrição clínica.

Liberação e estorno

Atendimento manual usa regras normais de benefício e cota, por exemplo quando não há atendimento pela catraca. Liberação excepcional dispensa o benefício conforme a operação autorizada e exige motivo. Escolha pessoa, refeitório e refeição; ao selecionar refeição explicitamente, informe a data de referência.

1. Localize a pessoa.
2. Escolha Atendimento manual ou Liberação excepcional.
3. Selecione refeitório e a refeição ou horário atual.
4. Confira Contar na cota da pessoa.
5. Informe motivo e registre.
6. Confira o consumo criado; para abrir fisicamente use Equipamentos → Liberar refeição.

Estornar mantém o registro original e cria um lançamento negativo. A devolução de cota depende de permissão separada e da opção confirmada. Sem devolver cota, não se autoriza automaticamente outro consumo.

Ajustar custo altera valores por lançamento com motivo. Tratar marca conflito como tratado após conferência. Não apague histórico para esconder uma correção; use essas ações e leia a situação final.

Custos e fechamento

1. Defina período e filtros.
2. Escolha agrupamento, como centro de custo, setor, empresa, categoria ou refeição.
3. Confira bruto, estornos, ajustes, líquido, subsídio e parte da pessoa.
4. Trate conflitos e correções antes de fechar.
5. Exporte CSV ou XLSX para conferência.
6. Use Fechar este período e confira operador e data.

Reabrir exige motivo e permite correções pelo fluxo autorizado. O arquivo de fechamento pode ser exportado. A exportação não envia valores automaticamente à folha ou ao faturamento externo.

Relatórios

Selecione o relatório e os filtros e use CSV ou XLSX. Existem fontes de consumos, tentativas, reservas e agregações conforme a lista da tela. Tentativas/identificações e consumos são fontes diferentes; não some como se fossem a mesma coisa.

Consumos utilizam a data de referência da refeição. Os filtros usam o fuso do módulo. Confira também origem offline, confirmação na liberação, confirmação no giro, estornos, exceções e conflitos quando essas informações forem apresentadas.

Configurações e integrações

Configure tolerância de giro tardio e janela de duplicidade de logs offline. Um giro recebido depois pode confirmar consumo como tardio, conforme a regra. Essa rotina reconcilia comunicação e não deve ser confundida com um novo atendimento manual.

Os adaptadores externos dependem de documentação e credenciais; a tela atual informa integrações desativadas. Use a importação manual quando não houver integração ativa.

1. Escolha RH, Escalas e plantões ou Acompanhantes.
2. Abra Colunas aceitas e prepare CSV ou XLSX com cabeçalho.
3. Use Validar, que não grava.
4. Corrija erros e use Importar.
5. Confira contagens, linhas com erro e Cargas anteriores.

A importação não cria pessoas e não encerra benefícios por ausência em uma carga. Arquivo já importado pode ser reconhecido sem produzir novas alterações.

Resolver negativas de refeição

Situação	O que verificar
Sem benefício	Vínculo, situação, validade e regra.
Fora de horário	Janela, dia, vigência, feriado e data de referência.
Cota esgotada	Consumos, reservas, escopo e exceções.
Exige plantão	Escala válida e tolerância.
Acompanhante negado	Referência, vínculo, limite e substituição.
Catraca libera mas consumo difere	Forma de confirmação, giro, reserva e reconciliação.
Relatório não confere	Tentativas versus consumos, estornos, filtros e fuso.

Use Simular para investigar sem provocar passagem nem consumo adicional.

23 Manutenção e saúde dos ativos

Onde acessar: Manutenção → Dashboard, Saúde dos Ativos, Inventário e Configurações.

Dashboard

O Health Center reúne equipamentos, câmeras, serviços, banco e integrações. A tela atualiza periodicamente e oferece filtros por estado. Use os indicadores para identificar falha de comunicação, serviço ausente, armazenamento ou envio pendente.

Estado	Interpretação operacional
ONLINE	Avaliação sem falha correspondente ao estado.
ATENÇÃO	Condição que merece conferência, incluindo comunicação antes do limite de offline.
CRÍTICO	Falha ou limite crítico apontado pela avaliação.
OFFLINE	Sem comunicação além do limite configurado.
MANUTENÇÃO	Ativo colocado em manutenção.
DESCONHECIDO	Sem informação suficiente para avaliar.
DESATIVADO	Fora do monitoramento conforme configuração.

Abra a ficha e leia o motivo. Estado online não é teste de qualidade da imagem, de reconhecimento ou da ligação física do relé.

Saúde dos Ativos

1. Filtre a lista e selecione o ativo.
2. Confira tipo, comunicação, último sinal e estado.
3. Veja quedas, eventos, histórico e dados de uso apresentados.
4. Registre ou retire manutenção com a permissão necessária.
5. Após intervenção, confira a próxima avaliação.

Colocar em manutenção identifica o contexto da indisponibilidade; não realiza reparo no equipamento. Não confunda desativar o monitoramento com desligar fisicamente o ativo.

Inventário

Equipamentos, câmeras, serviços e integrações podem entrar automaticamente. Para ativos sem integração, como câmera CFTV, use o cadastro manual.

1. Cadastre o ativo com Nome, Tipo e dados técnicos apresentados.
2. Preencha instalação, garantia, observações e foto quando úteis.
3. Defina Offline após se precisar de limite individual; mínimo 30 s na tela.
4. Marque Monitorar este ativo.
5. Salve e confira a ficha.

Fora do monitoramento não entra nas contagens, alertas e disponibilidade. Ativos manuais podem não produzir o mesmo tipo de telemetria de um equipamento integrado. Confira a origem do monitoramento antes de atribuir uma falha.

Configurações

Acesso administrativo. Escolha limites de offline por tipo e intervalos de avaliação. Há opções de 1, 5 e 10 minutos e personalizado. O limite individual do Inventário prevalece quando configurado.

Ajuste disco livre para Atenção e Crítico, latência do banco, quantidade de falhas de envio e idade máxima do backup. Leia faixas e padrões da tela antes de salvar. Restaurar padrão prepara os valores padrão; confira e salve.

O módulo utiliza os dados coletados pelo sistema. Mudar o intervalo da avaliação não necessariamente muda a consulta que um driver faz ao equipamento.

Rotina de manutenção

Ao receber uma falha, confira último sinal, motivo, rede, serviço e recurso indicado. Registre a intervenção pelo operador responsável. Após retorno, acompanhe estado e histórico. Para backup atrasado, confira também agendamento e pasta do Launcher.

24 Lista de restrição

Onde acessar: Cadastros → Lista de restrição. Exige permissão específica de consulta; incluir e remover exigem Alterar.

Registrar uma restrição

1. Pesquise nome, CPF, RG, solicitante ou empresa.
2. Clique em Incluir restrição.
3. Informe CPF ou RG, nome e quem solicitou.
4. Selecione empresa quando aplicável e registre motivo e observações.
5. Salve e confira a situação ativa.
6. Abra os detalhes e confira a propagação aos equipamentos quando houver visitante correspondente.

A lista é conferida no cadastro e na liberação do visitante. A portaria pode receber apenas a mensagem VISITANTE NÃO AUTORIZADO À ENTRADA. O motivo detalhado fica restrito a quem pode consultar o módulo.

Conferir equipamentos

Na ficha, veja ação, situação, mensagem e atualização. Pendente, erro e restrição pendente no equipamento indicam que a propagação ainda não foi concluída. Uma restrição no servidor não comprova que um dispositivo standalone já recebeu a alteração.

Use Atualizar situação e confira comunicação e envio quando necessário. Se não houver visitante cadastrado com aquele documento, a tela pode informar que não há nada a remover dos equipamentos.

Remover e manter histórico

Selecione a restrição e use Remover, informando motivo. O registro permanece no histórico com responsável e data; o filtro Todas inclui removidas. Confira também a restauração nos equipamentos. Remover uma restrição não concede regra, validade ou vaga que o visitante não possuía.

25 LGPD e privacidade

Onde acessar: Sistema → LGPD / Privacidade. As ações dependem da permissão correspondente.

Finalidade da tela

O módulo reúne informações de tratamento de dados, biometria, relatório do titular, solicitações e incidentes. Este capítulo explica os procedimentos do software. As escolhas de base legal, retenção, conteúdo público e comunicação de incidentes devem ser definidas pelo responsável da instituição; o preenchimento da tela não valida essas escolhas.

Configurar os dados institucionais

1. Informe controlador, documento, endereço e contato do encarregado.
2. Confira a base padrão apresentada para cadastros com face.
3. Escolha se o cadastro biométrico exige base registrada.
4. Revise retenções, justificativas, finalidades, compartilhamento e texto público.
5. Confira a opção de anonimizar histórico ao excluir pessoa.
6. Salve e revise a página de privacidade publicada pela instalação.

O texto público não deve conter dados pessoais de visitantes, senhas ou informações de segurança. Use as opções e limites da tela, com o conteúdo aprovado pela instituição.

Consultar um titular

Localize a pessoa e use o relatório do titular conforme a ação disponível. Confira identificação antes de exportar ou entregar. As consultas e ações são feitas pelo operador autenticado.

Base e biometria

Registre a base ou consentimento conforme a opção autorizada na ficha. Revogar biometria impede o uso correspondente e exige conferência dos leitores e das câmeras. Não confunda apagar a fotografia comum com eliminar todos os registros biométricos ou anonimizar o histórico.

Para exclusão ou anonimização, leia o efeito e a confirmação da tela. Confira vínculos, presença, veículo e pendências que possam impedir a conclusão. Preserve a rastreabilidade da ação pelo módulo.

Solicitações

1. Registre nome do titular/solicitante, contato, pedido, data e detalhes.
2. Acompanhe a situação.
3. Ao concluir ou negar, registre a resposta e o motivo exigido.
4. Confira o registro final para acompanhamento pelo responsável.

Use as informações necessárias ao pedido. Não preencha o campo de resposta com justificativas genéricas se a conclusão exigir esclarecimento específico.

Incidentes

Registre título, ocorrência, ciência, titulares aproximados, descrição, categorias de dados, riscos e medidas. Atualize a situação e, quando pertinente ao tratamento definido pelo responsável, as datas de comunicação.

26 Licenciamento

Onde acessar: Sistema → Licenciamento, disponível ao administrador.

Consultar e ativar

1. Abra a tela e confira situação, dados do titular e validade apresentados.
2. Para ativação ou renovação, use a chave fornecida para essa instalação.
3. Confira os dados exigidos e aplique pelo botão de ativação.
4. Aguarde a resposta e confira novamente situação e prazo.

Use apenas chaves fornecidas pelo responsável pelo licenciamento. Não coloque a chave em relatórios, mensagens públicas ou exemplos de configuração.

Quando o acesso é interrompido

Avisos podem aparecer no login e durante a sessão. Confira situação e endereço do servidor antes de concluir que os cadastros foram perdidos. Licença vencida ou inválida não deve ser corrigida alterando a data do Windows. Encaminhe os dados da instalação ao responsável e utilize a rotina de renovação.

A licença não configura equipamentos, cria biometria nem habilita uma integração externa. Após ativação, os módulos ainda precisam dos respectivos cadastros.

27 Relatórios automáticos

Onde acessar: Configurações → Relatórios automáticos, disponível ao administrador.

Preparar o envio

Confira o estado do e-mail mostrado na tela. O servidor precisa estar em funcionamento e o serviço SMTP da instalação deve estar configurado. Um agendamento salvo não garante recebimento de e-mail.

Criar um agendamento

1. Crie um nome que identifique público e finalidade.
2. Escolha Tipo de relatório.
3. Defina periodicidade diária, semanal ou mensal.
4. Escolha horário e dia quando necessário; dia mensal aceita 1 a 28.
5. Selecione o Período analisado.
6. Defina os filtros próprios do tipo de relatório.
7. Informe destinatários separados por vírgula, até o limite da tela.
8. Escolha formato e assunto; marque Ativo e salve.
9. Use Pré-visualizar PDF para conferir conteúdo sem enviar.

Cada agendamento tem seus próprios filtros, período e destinatários. Evite presumir que um filtro de outro relatório vale neste. Confira o conteúdo da prévia antes de incluir pessoas na distribuição.

Executar e acompanhar

Enviar agora gera e envia para o período configurado. Use quando for necessário o envio imediato e confirme destinatários antes da ação. No histórico, confira situação, geração, PDF, erro e responsáveis apresentados.

Reenviar usa a rotina do histórico com destinatários conferidos. Pausar mantém o agendamento salvo sem novas execuções automáticas. Remover exclui o agendamento conforme a confirmação da tela.

Identidade dos arquivos

Na configuração de identidade, preencha Empresa, Unidade, Empresa prestadora e logo quando disponível. Confira a prévia para verificar cabeçalho e rodapé.

Diagnóstico

Se não enviar, confira agendamento ativo, horário, fuso, servidor ligado, configuração de e-mail e histórico de erros. Aceitação pelo servidor SMTP não comprova entrega à caixa de entrada; confira endereço e spam. Se conteúdo estiver incorreto, revise tipo, período e filtros antes de reenviar.

28 Launcher backup e restauração

Onde acessar: Launcher no computador servidor. As rotinas dependem da versão instalada e dos componentes disponíveis.

Uso do Launcher

Use Abrir no navegador para acessar o painel no endereço configurado. Confira situação do servidor e opções de serviço quando oferecidas. O serviço JNAccess atende o painel e as decisões; o JNAccess-Facial executa reconhecimento por câmeras IP. Serviços de LPR e outros componentes devem ser conferidos conforme a instalação.

Rotinas como importar dados, redefinir senha, manutenção e apagamento de usuários são administrativas. Leia escopo e confirmação antes de executar. Apagar usuários de um equipamento pode afetar credenciais de outro sistema quando esse escopo for escolhido; não use como teste de conexão.

Configurar backup automático

1. No Launcher, abra Manutenção → Backup automático.
2. Ative e escolha a pasta de armazenamento.
3. Defina execução diária ou intervalo de 1 a 168 horas.
4. Salve; a aplicação pode levar até 30 s para aplicar a configuração.
5. Execute um backup imediato para conferir destino e resultado.
6. Confira arquivo e data do último backup.

O horário usa o fuso do servidor. O serviço precisa estar ligado, mas o Launcher pode ficar fechado. Horário diário perdido é tratado no retorno do servidor. No modo por intervalo, o primeiro backup pode ocorrer logo após a ativação.

Pasta e armazenamento

A conta do serviço deve poder gravar na pasta. Em armazenamento de rede, use caminho UNC e as permissões corretas. A pasta também é usada nas rotinas manuais de backup. Guarde os arquivos com acesso restrito.

O backup automático descrito cobre o banco PostgreSQL em arquivos .backup. A rotina verifica a estrutura e evita execuções simultâneas. Backups antigos não são removidos automaticamente; confira espaço. Configurações e arquivos externos precisam de cópia própria. Em falha, a rotina tenta novamente conforme seu agendamento de recuperação.

Backup antes de manutenção

Gere uma cópia antes de atualizar, importar grande carga, alterar a implantação ou restaurar dados. Confira nome, tamanho, data e resultado. Um arquivo existente na pasta não comprova que o último backup terminou bem. O módulo Manutenção também pode apontar backup atrasado.

Restauração

1. Identifique o backup correto e o período dos dados que serão recuperados.
2. Gere uma cópia do estado atual antes de substituir o banco.
3. Planeje a parada e use a rotina de restauração oferecida pela instalação.
4. Confira a mensagem de conclusão antes de reiniciar a operação.
5. Valide login, cadastros, regras, eventos, vínculos e comunicação.
6. Reconfira configurações externas que não fazem parte do arquivo do banco.

29 Aplicativo móvel de cadastros

O aplicativo JNAccess Cadastros complementa os cadastros pelo celular. Sua versão e compatibilidade devem ser conferidas com o servidor; o instalador Windows não atualiza automaticamente o aplicativo.

Preparar e conectar

1. Instale o aplicativo autorizado pela instituição.
2. Informe o endereço HTTPS do servidor alcançável pelo celular.
3. Confira o certificado da instalação pelo procedimento do administrador.
4. Entre com um operador autorizado e confirme o ambiente antes de cadastrar.

O celular precisa alcançar o servidor por rede ou acesso remoto autorizado. Não troque HTTPS por conexão sem proteção para contornar um problema de certificado.

Cadastro e fotografia

Consulte antes de criar, preencha identificação e dados disponíveis, capture ou selecione uma fotografia nítida e confira o resultado salvo no servidor. Quando houver opções de vaga, escolha pessoa ou empresa conforme o uso.

A foto enviada pelo app é fotografia do cadastro. O reconhecimento das câmeras IP ainda exige template processado na seção de Biometria facial. Confira também o envio aos equipamentos quando essa credencial for usada no leitor.

Sessão e privacidade

Use a conta própria do operador e saia em aparelhos compartilhados. Se o app não cadastrar, confira rede, certificado, endereço, sessão e permissões. Consulte o aviso de privacidade apresentado pela instalação e não deixe fotografias de pessoas em pastas ou compartilhamentos desnecessários.

30 Rotinas recomendadas e implantação

Sequência do controle geral

1. Defina operadores e permissões.
2. Cadastre empresas e grupos.
3. Crie áreas externa e internas.
4. Crie horários e regras.
5. Cadastre dispositivos e confira portas, origem e destino.
6. Cadastre pessoas, visitantes e credenciais.
7. Assuma o gerenciamento e envie dados conforme o equipamento.
8. Configure online quando as verificações do servidor forem necessárias.
9. Acompanhe uma entrada e uma saída e confira os eventos.

Sequência da câmera com JC 013

1. Cadastre a placa, nomeie as portas e configure as áreas.
2. Habilite o relé usado e escolha a porta lógica.
3. Configure sensor, faixas, inversão e tempo de alerta.
4. Teste comunicação e confira a leitura com porta aberta e fechada.
5. Cadastre câmera RTSP e template válido da pessoa.
6. Em Ponto de acesso, selecione a porta com o relé habilitado.
7. Confira regra, direção e reconhecimento em modo teste.
8. Depois da conferência, utilize o modo de controle e acompanhe a passagem.

Abertura do turno

Confira servidor, comunicação, serviços de reconhecimento, pendências de sincronização e alertas. Verifique exceção ativa, portas abertas, ocupação e agenda de atendimento. Não normalize uma exceção sem saber por que foi aplicada.

Durante o turno

Leia os motivos das negativas, corrija apenas dados conferidos e use conta própria nas aberturas. Acompanhe fila de alertas, consumos e falhas. Em atendimento manual de refeição, confira registro anterior e cota.

Encerramento do turno

Confira portas, eventos pendentes, visitantes, presença e veículos que exigem conferência. Registre ocorrências e ações tomadas. Não zere ocupação ou presença somente para deixar a tela sem pendências.

Rotina administrativa

Diariamente confira backup e saúde dos serviços. Periodicamente revise operadores, credenciais temporárias, vagas, benefícios, cobranças e agendamentos. Antes de manutenção, garanta cópia recuperável e registre a intervenção.

Validar a recuperação do backup

Restauração substitui o estado dos dados pelo do backup. Não é uma função de desfazer seletivamente um cadastro. Uma prova de recuperação em ambiente separado é a forma adequada de verificar a utilidade de uma cópia sem substituir a produção.

31 Solução de problemas por módulo

Acesso e cadastro

Problema	Verificação inicial
Menu não aparece	Conta, Ver, ação própria da aba e recarga.
Pessoa não entra	Situação, validade, exceção/restrição, credencial, grupo e regra.
Fora do horário	Faixa, dia, fuso e regra selecionada.
Dupla entrada	Presença atual, direção e registro de saída.
Área lotada	Capacidade e passagens registradas.
Visitante não autorizado	Restrição por documento e validade.

Equipamentos câmeras e sensores

Problema	Verificação inicial
Dispositivo offline	IP, rede, porta, energia e último sinal.
Dado não chegou ao leitor	Gerenciamento, envio pendente, erro e comunicação.
Online chama servidor antigo	Reapontamento e endereço alcançável pelo equipamento.
Ponto JC-013 não aparece	Placa/canal habilitados, gerenciados e Porta associada salva.
Relé errado	Associação da porta ao canal e ponto da câmera.
Porta aparece invertida	Entrada física, faixas e inversão.
Sem popup de porta aberta	Sensor, leitura contínua, tempo, alerta e sessão.
Sem vídeo facial/LPR	RTSP, IP, porta, autenticação e serviço.
Reconhece mas não libera	Modo teste, regra, porta, cota e resposta do comando.

Garagem refeitório e administração

Problema	Verificação inicial
Sem vaga após cadastrar	Responsável e cota na aba Vagas.
Vaga ocupada indevidamente	Saída não registrada e veículo efetivamente dentro.
Bloqueio após pagamento	Confirmação do provedor, saldo e outras dívidas.
Refeição negada	Benefício, janela, cota, reserva e escala.
Consumo não confere	Confirmação no giro/liberação, data de referência e estorno.
Relatório não enviado	Agendamento, histórico, servidor e SMTP.
Backup atrasado	Agendamento, permissão da pasta, espaço e resultado.
Licença impede login	Situação, validade e chave da instalação.

Dados para encaminhar um problema

Registre horário, módulo, pessoa ou identificador necessário, dispositivo, mensagem e ação esperada. Inclua a configuração relevante sem senhas nem tokens. Consulte eventos e auditoria para distinguir falta de reconhecimento, negativa de autorização, falha do comando e falha física.

32 Referência de telas e revisão do manual

Mapa dos módulos

Menu	Caminho interno
Monitoramento	/
Ocupação	/ocupacao
Relatórios e Auditoria	/relatorios
Pessoas	/pessoas
Visitantes	/visitantes
Pré-cadastro	/pre-cadastro
Empresas	/empresas
Departamentos e grupos	/grupos
Lista de restrição	/restricoes
Garagem	/financeiro
LPR Placas	/garagem-lpr
Monitor de Eventos LPR	/garagem-lpr-monitor
Refeitório	/refeitorio
Áreas	/areas
Horários	/horarios
Regras	/regras
Dispositivos e JC-013	/dispositivos
Painel e Câmeras facial	/facial
Eventos facial	/facial-eventos
Manutenção Dashboard	/manutencao
Saúde dos Ativos	/manutencao-saude
Inventário	/manutencao-inventario
Configuração Manutenção	/manutencao-configuracoes
LGPD	/lgpd
Operadores	/operadores
Permissões	/permissoes
Licenciamento	/licenciamento

Menu	Caminho interno
Relatórios automáticos	/relatorios-automaticos

Os caminhos não concedem permissão por serem digitados no navegador. A sessão e as ações continuam validadas pelo servidor.

Base de elaboração

Manual elaborado a partir do menu e das telas atuais do JNAccess, dos fluxos de cadastro e autorização, da documentação de uso existente e das integrações publicadas de JC-013, reconhecimento facial e ponto de acesso. Referência: distribuição 0.3.15 de 09 de outubro de 2026.

Os nomes de abas e botões foram conferidos no projeto. Não foram incluídas senhas, chaves de licença, chaves de câmera ou dados pessoais reais. As rotinas físicas e integrações externas devem ser conferidas na instalação utilizada.

Quando revisar

Revise este manual quando novas telas, campos, permissões, drivers ou regras forem publicados. Ao receber uma atualização, confira especialmente o campo Ponto de acesso, configuração de sensores, comportamento de confirmação de passagem e os módulos que usam decisões no servidor.