K-Monitor Center

Manual de operação e administração

Guia para consultar eventos, verificar evidências, organizar atendimentos e administrar os recursos de uma central de monitoramento integrada.

Como utilizar este manual

Operadores podem começar pelos capítulos de Monitor, atendimento, câmeras e gravações. Supervisores devem consultar também indicadores e relatórios. As rotinas de cadastros, IA, automação e permissões destinam-se aos responsáveis autorizados pela administração.

Os recursos exibidos variam conforme os módulos habilitados, a empresa vinculada e o perfil de acesso. A presença de um botão não significa que sua ação esteja liberada ou que o serviço associado esteja configurado.

Exemplos para treinamento

Todas as situações de exemplo usam identidades e dados fictícios. Empresa Demo, Cliente Demo, Conta DEMO001, Câmera Demo 01, Pessoa Demo 01 e placa DEM1A23 não representam clientes ou ocorrências reais. Os recortes de interface mostram somente controles sem dados de clientes.

Edição 2.0
Interface consultada em 2 de novembro de 2026
Idioma português do Brasil

Acesso ao sistema: https://k-monitorcenter.app/login

Sumário

Selecione um capítulo para abrir a página correspondente. Os marcadores do PDF também permitem navegar pelos módulos.

01 Acesso e navegação 4

02 Monitor e leitura da ocorrência 5

03 Filtros e localização de eventos 6

04 Atendimento do início à conclusão 7

05 Anotações contatos e evidências 8

06 Transferência e estados da ocorrência 9

07 Ordens de serviço 10

08 Mosaico de câmeras 11

09 Gravações e reprodução 12

10 Dashboard e relatórios 13

11 Empresas e clientes 14

12 Dispositivos e conectividade 15

13 Regras de detecção de IA 16

14 Automações e comunicação 17

15 Usuários e perfis de acesso 18

16 Mapa de dispositivos 19

17 Cadastro de empresa e personalização 20

18 Centrais de alarme 21

19 Leitores faciais e biométricos 22

20 Integrações de API e webhooks 23

21 Listas de reconhecimento facial 24

22 Cadastro de identidades e matrículas 25

23 Painel de reconhecimento e acessos 26

24 Listas de placas LPR 27

25 Painel de leitura de placas 28

26 Rastreabilidade de percurso 29

27 Consulta forense 30

28 Frequência e gestão de faltas 31

29 Turnos tolerância e notificações 32

30 Omnichannel e chamados 33

31 Movimentações e alertas de PDV 34

32 Servidor armazenamento e continuidade 35

33 Licenças desktop e recursos 36

34 Configurações e cadastros de apoio 37

35 Implantação e validação da operação 38

36 Entradas de vídeo e validação do sinal 39

37 Diagnóstico e suporte 40

38 Exercícios e listas de conferência 41

39 Glossário e referência 42

40 Abrangência e validação desta edição 43

01 Acesso e navegação

1. Abra **https://k-monitorcenter.app/login** no navegador e confira o endereço antes de informar credenciais.

2. Preencha **E-mail** e **Senha** com seu acesso individual e selecione **Acessar central**.

3. Confira a identificação da sessão e abra o menu lateral pelo ícone de três linhas.

4. Escolha o módulo necessário. Use **Navegação rápida** ou **Ctrl + K** para localizar recursos disponíveis.

Controles da entrada

Lembrar de mim é opcional e deve seguir a política da estação. **Esqueci minha senha** inicia a recuperação do acesso. A tela permite selecionar português ou inglês. Não inclua senhas, tokens ou códigos de recuperação em registros de atendimento.

Estrutura da operação

Recurso	Finalidade
Dashboard	Resumo executivo, volume de eventos, TMT e SLA.
Monitor	Fila de ocorrências, contexto, vídeo, evidências e ações.
Mosaico Câmeras e Gravação	Visualização simultânea e consulta histórica.
Clientes e Dispositivos	Vínculos operacionais e configuração dos ativos.
AI e Automação	Lógica de detecção e ações disparadas por eventos.
Usuários e Perfis de Acesso	Identidade, escopo da empresa e permissões por módulo.

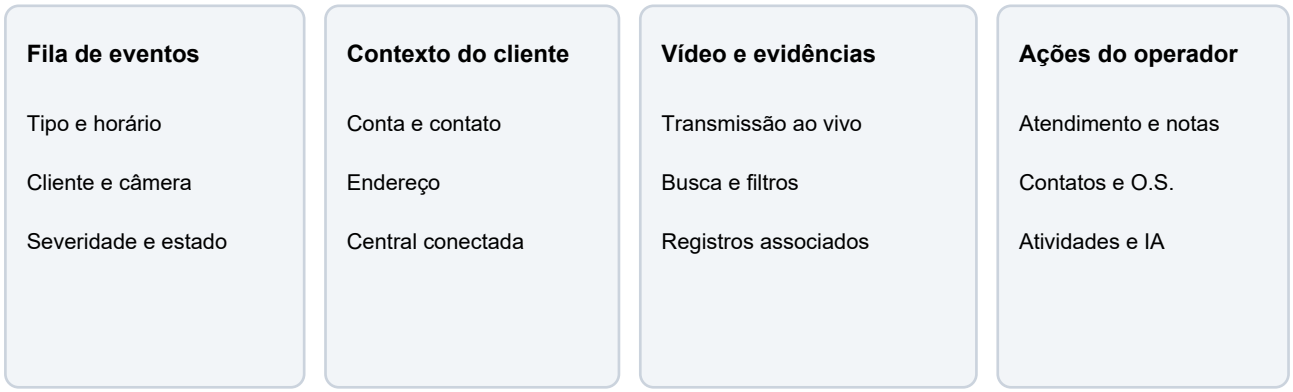
Se um módulo não aparecer

Solicite ao administrador que confira o perfil, a empresa e os módulos contratados ou habilitados. Não utilize a conta de outro operador para contornar a restrição. Ao encerrar o turno, utilize a opção de saída da sessão no menu do usuário.

02 Monitor e leitura da ocorrência

Caminho: Monitor

O Monitor reúne a fila de eventos e os recursos para verificar a ocorrência selecionada. A leitura do evento, a decisão operacional e a ação de atendimento são momentos diferentes; confira o contexto antes de assumir ou concluir uma ocorrência.



Esquema didático da tela em desktop. Não contém registros ou imagens de clientes.

O que observar na fila

• **Tipo e horário**: identificam o que foi recebido e quando ocorreu.

• **Cliente e câmera**: indicam o local e a origem associados.

• **Severidade**: representa a classificação configurada; não substitui a verificação visual e o procedimento da central.

• **Estado**: diferencia registros não lidos, em atendimento ou em tratamento, além das filas de espera e despacho.

Contexto e evidências

Ao selecionar uma ocorrência, confira cliente, conta, contato principal e endereço. Na área central, verifique a transmissão ao vivo e a lista de **Evidências e detecções**. A imagem ao vivo mostra o momento atual; uma evidência histórica pode mostrar outro instante.

Use **Atividades do Atendimento** para acompanhar os registros associados à ocorrência. Uma indicação de bloqueio ou tratamento exige verificar o responsável e evitar ações simultâneas conflitantes.

Atenção Não interprete ausência de imagem ou de detecção como confirmação de que o local está seguro. Verifique comunicação, horário, dispositivo e registros disponíveis.

03 Filtros e localização de eventos

Caminho: Monitor → Filtrar eventos

Abra o ícone de filtro no Painel de Eventos. Combine os campos e selecione **Aplicar Filtros**. Use **Limpar** para remover a restrição da consulta.



Recorte dos controles reais de filtro. Seletores fechados sem nomes ou registros de clientes.

Exemplo fictício de consulta

Para procurar uma intrusão do Cliente Demo, escolha a empresa e o cliente correspondentes, origem Câmeras, analítico Intrusão e o período da investigação. Se necessário, restrinja a severidade e o estado de leitura.

A busca aceita informações como placa, câmera, cliente ou código. O limite controla a quantidade apresentada na consulta: há opções de 20, 50, 100, 200 e 500 eventos. Uma lista vazia pode indicar filtros incompatíveis, e não ausência de eventos.

04 Atendimento do início à conclusão

Caminho: Monitor → ocorrência → Ações Rápidas

1. Selecione e confira. Verifique cliente, origem, horário, severidade e responsável. Confirme que está tratando a ocorrência correta.

2. Analise o contexto. Observe a transmissão e as evidências históricas. Compare o tipo de evento com o que é possível constatar.

3. Assuma quando autorizado. Use o controle principal de atendimento quando ele oferecer a opção de iniciar. Não assuma um registro já tratado por outro operador sem alinhamento.

4. Execute o procedimento. Consulte contatos e instruções da operação. Quando aplicável, registre contato, diagnóstico, encaminhamento técnico ou apoio operacional.

5. Documente. Registre observações e associe evidências necessárias. Se houver pendência, utilize o estado correspondente e informe o motivo.

6. Conclua somente após conferência. Quando o controle mostrar **Em Atendimento • Finalizar**, siga a etapa de conclusão apresentada pelo sistema. Revise o resultado e as informações solicitadas antes de confirmar.

Critério para decisão humana

Intrusões, situações de risco e dúvidas que exigem julgamento devem seguir a prioridade e o escalonamento definidos pela central. Automações podem comunicar rotinas e eventos não críticos quando regras, canais e responsáveis estiverem previamente configurados.

Exemplo fictício

Uma detecção de pessoa é recebida na Câmera Demo 01. O operador confere o instante da evidência, compara com o vídeo ao vivo, identifica a área envolvida e segue o procedimento de contato do Cliente Demo. O resultado deve registrar fatos observados, contatos realizados e encaminhamentos, sem afirmar conclusões que a imagem não permite.

Atenção Clicar em finalizar, transferir ou atualizar estado modifica a operação. Faça isso apenas no exercício real da função e conforme o procedimento aprovado.

05 Anotações contatos e evidências

Caminho: Monitor → Ações Rápidas

Registrar uma anotação

1. Selecione **Fazer Anotações**.

2. Escolha o **Tipo de Registro**: Observação Geral, Contato / Ligação com Cliente, Alerta de Segurança / Emergência, Diagnóstico Técnico ou Despacho Operacional / Viatura.

3. Preencha **Anotação do Operador** com descrição objetiva. Confira o histórico existente antes de repetir um registro.

4. Revise e utilize **Salvar Anotação**. Para abandonar o formulário, use **Cancelar**.

Exemplo fictício: “14h32 - Evidência da Câmera Demo 01 verificada. Contato Demo informado sobre a ocorrência. Aguardando retorno para definição do encaminhamento.” Evite registrar senhas, rotas de vídeo com credenciais ou dados pessoais desnecessários.

Consultar evidências

Use a busca da seção **Evidências e detecções** e os filtros de tipo: Detecções IA, Placas, Facial, Pânico & Alarmes ou Técnicos / Conexão. O filtro de mídia permite alternar entre Todos, Com Foto e Sem Foto. Confira a câmera e o horário do item antes de utilizá-lo como evidência.

Outras ações da ocorrência

• **Lista de Emergência e Pessoas de Contato**: consulte os responsáveis apropriados antes de efetuar comunicação.

• **Salvar Evidência e Anexar Arquivos**: utilize somente material relacionado à ocorrência e autorizado para a operação.

• **Agente de Voz IA**: depende da configuração do serviço e das permissões. A abertura do recurso não autoriza uma ligação.

• **Analisar com IA e Ver Análise da IA**: diferencie solicitar uma análise de consultar o resultado existente. A decisão operacional permanece vinculada ao procedimento humano.

06 Transferência e estados da ocorrência

Caminho: Monitor → Transferir / Status

Transferir para outro operador

1. Abra **Transferir / Status** e escolha **Transferir Atendente**.

2. Selecione o novo operador responsável.

3. Preencha **Motivo / Justificativa da Transferência**. A interface informa que o motivo é registrado em nota.

4. Confira a ocorrência e o destinatário antes de selecionar **Transferir Atendimento**.

Alterar o estado com justificativa

Na aba **Alterar Status**, selecione o estado e preencha **Detalhes / Nota do Status**. O comando **Atualizar Status & Gravar Nota** aplica a alteração e registra a informação associada.

Estado	Quando utilizar
Em Espera	Aguardando retorno do cliente, contato telefônico ou informação adicional.
Despacho / Apoio Tático em Ronda	Equipe de apoio, fiscal ou viatura em deslocamento, de acordo com o procedimento da central.
Em atendimento	Ocorrência sob tratamento de um operador. Confira o responsável antes de agir.
Tratamento com bloqueio	Indicação de tratamento protegido. Evite disputa de atendimento e consulte a supervisão.

Conferência após a mudança

Verifique a fila correspondente, o estado exibido e as atividades do atendimento. Uma transferência deve explicar o que já foi feito e o que permanece pendente. Colocar em espera não substitui definir quem acompanhará o retorno.

Exemplo fictício: “Transferência para Operador Demo 02: contato realizado às 14h32; falta retorno do responsável do Cliente Demo para concluir a verificação.”

07 Ordens de serviço

Caminho: Monitor → Ordem de Serviço ou menu Ordens de Serviço

A ordem de serviço organiza um encaminhamento operacional ou técnico. Ao abrir pelo Monitor, a interface apresenta o formulário vinculado ao evento e pode preencher informações da ocorrência automaticamente.

1. Selecione **Ordem de Serviço** no evento correto.

2. Defina **Setor Responsável** e confira o **Cliente**. O setor determina quem acompanhará a O.S.

3. Revise o **Endereço de Atendimento**. Não considere o preenchimento automático como prova de que o endereço está completo.

4. Escolha **Categoria** e **Subcategoria**, de acordo com os cadastros da empresa.

5. Informe o **Nível de Urgência**: Baixa, Normal, Alta ou Crítica. Se aplicável, selecione o responsável.

6. Complete **Descrição do Problema / Observações** com sintomas, verificações, evidências e encaminhamento desejado.

7. Revise e confirme no botão de emissão da O.S. Se não for emitir, utilize **Cancelar**.

Exemplo fictício de descrição

“Cliente Demo - Câmera Demo 01. Imagem indisponível no Monitor às 14h32. Conectividade da estação conferida. Solicita-se diagnóstico de alimentação, rede e configuração do stream. Evidência de indisponibilidade vinculada à ocorrência.”

Acompanhar o serviço

Acesse **Ordens de Serviço** para acompanhar os registros disponíveis ao seu perfil. O relatório **Ordem de Serviços** reúne histórico e estados de O.S. abertas e fechadas. Categorias e problemas de O.S. são administrados em Configurações.

Atenção Não crie uma nova categoria ou subcategoria durante um atendimento sem a autorização administrativa adequada. Evite duplicar um chamado já aberto para o mesmo problema.

08 Mosaico de câmeras

Caminho: Mosaico Câmeras

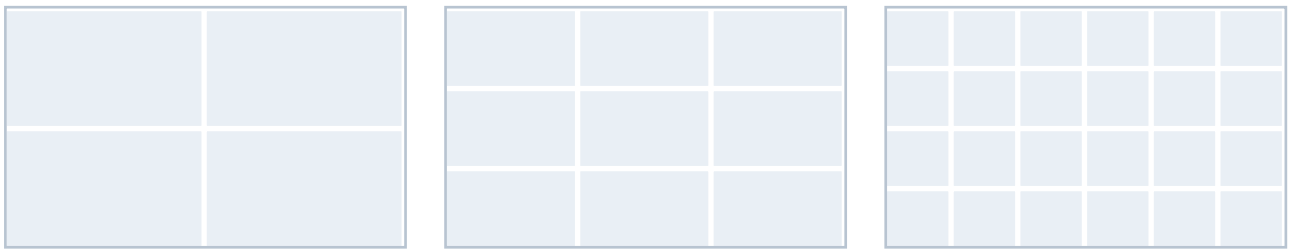
1. Selecione o contexto de câmeras disponível no seletor superior. Confira se está no cliente ou conjunto correto.

2. Abra o seletor de mosaico e escolha a quantidade de canais adequada à estação.

3. Localize a câmera na lista lateral e arraste para o espaço indicado. A tela também oferece **Preencher Mosaico**.

4. Use **Maximizar** para ampliar a grade ou o controle de uma câmera para destacá-la.

2 x 2 | 4 canais **3 x 3 | 9 canais** **6 x 4 | 24 canais**



Esquemas didáticos de três matrizes disponíveis. Cada retângulo representa um canal fictício.

Matrizes disponíveis: 1 câmera; 2 × 2 com 4; 3 × 3 com 9; 4 × 4 com 16; 6 × 4 com 24; 8 × 4 com 32; 8 × 8 com 64. Layouts dinâmicos incluem Destaque Principal 1+5, Visão Expandida 1+7 e Foco Central 1+8.

Controles por câmera: Diagnóstico / Probe, qualidade SUB ou MAIN, gravações quando configuradas, maximizar, zoom digital e PTZ quando suportado. O diagnóstico apresenta campos como codec, FPS e bitrate. Uma câmera fixa pode indicar PTZ indisponível.

Atenção Mais canais exigem mais recursos da estação e da rede. A indicação SUB / MAIN informa o fluxo selecionado. Use o detalhamento de uma câmera para investigar; não conclua que o sistema está gravando apenas porque há vídeo ao vivo.

09 Gravações e reprodução

Caminho: Gravação

Localizar a câmera e o período

1. Na lista de gravações, pesquise a câmera e confira cliente, retenção, volume gravado e estado.

2. Abra a ação **Assistir Gravações 24h**.

3. No player, escolha a câmera e a data no calendário.

4. Clique ou arraste na régua de tempo para localizar o horário. Confira se existe material para o intervalo escolhido.

Controles do player

O player oferece reproduzir / pausar, velocidades 0,5×, 1×, 2× e 4×, avanço e retrocesso com intervalo de salto, **Preencher Tela**, **Corte**, **Baixar**, **Compartilhar** e **Marcadores**. Alguns comandos permanecem desabilitados até que existam mídia e seleção válidas.

A legenda distingue gravação contínua, ocorrência de IA / movimento, trecho selecionado e marcador. Use o recurso de corte para delimitar o intervalo necessário e confira o resultado antes de baixar ou compartilhar. Siga a política da operação quanto a destino, finalidade e guarda das imagens.

Retenção e estado de gravação

O prazo é configurado por câmera ou serviço; não existe um único valor universal neste manual. Consulte o campo **Retenção** do registro. Um canal ao vivo pode estar disponível sem possuir gravação histórica. Volume exibido e retenção contratada não garantem, isoladamente, que todos os instantes estejam gravados.

Atenção Ativar / pausar gravação, forçar reconexão e sincronizar são ações operacionais diferentes de consultar o player. Execute-as somente quando autorizado e após avaliar o impacto.

10 Dashboard e relatórios

Caminho: Dashboard ou Relatórios

Interpretar os indicadores

No Dashboard, selecione **Hoje**, **7 Dias** ou **30 Dias** antes de comparar números. Os cartões permitem consultar clientes, câmeras, alarmes, atendimentos, ocorrências atrasadas, eventos processados e notificações WhatsApp.

Indicador	Leitura prática
TMT	Tempo médio da entrada até a conclusão, conforme indicação da interface.
Eficiência SLA	Proporção tratada no prazo configurado.
Distribuição temporal	Horários com maior frequência de ocorrências.
Dispositivos mais ativos	Ranking de acionamentos no período selecionado.
Distribuição por categoria	Volume por origem operacional, como CFTV, alarmes e notificações.

Consultar o histórico e exportar

1. Abra **Relatórios** → **Histórico de Eventos**.

2. Defina categoria, cliente e período nos campos **De** e **Até**.

3. Confira data / hora, empresa, cliente, ocorrência, origem, categoria, código, evento e detalhes.

4. Use **Imprimir** ou **Exportar CSV** somente após conferir o escopo e a finalidade da saída.

Outros relatórios incluem clientes, fornecedores, produtos, códigos e eventos, grupos de alarme, categorias e ordens de serviço, painéis de alarme, dispositivos de vídeo, empresa, colaboradores, departamentos e planos de assinatura.

Atenção Considere o período, o escopo da empresa e os filtros ao comparar relatórios. Preserve a confidencialidade dos arquivos exportados e confira se a consulta contém somente os dados necessários.

11 Empresas e clientes

Caminho: Empresas ou Clientes

A empresa organiza o contexto administrativo. O cliente representa a conta ou unidade vinculada à operação. Os registros devem manter vínculos consistentes com os dispositivos, usuários, planos e regras.

Cadastrar um cliente

1. Abra **Clientes** → **Novo**.

2. Selecione **Empresa Pertencente**, **Grupo de Cliente** e **Plano de Serviço**.

3. Informe a **Conta** e o **Nome Fantasia**. Quando aplicável, complete razão social e CPF / CNPJ.

4. Preencha e-mail comercial, contato de suporte, telefone e WhatsApp. A interface permite múltiplos números de WhatsApp separados por vírgula.

5. Complete o endereço de cadastro, incluindo CEP, logradouro, número, bairro, cidade e UF. Revise o endereço de cobrança se utilizado.

6. Confira logo, estado de acesso e recebimento de alertas. Revise os vínculos antes de **Registrar Cliente**.

Busca e atualização

Na listagem, use pesquisa e filtros avançados. Confira empresa, conta, nome, contato, localidade e estado. Abra **Visualizar** para consulta ou **Editar** quando houver autorização para alterar o cadastro.

Atenção Os comandos **Testar & Verificar E-mail** e **Testar & Verificar WhatsApp** podem iniciar comunicações. Utilize apenas destinatários de teste autorizados. Alterar o estado de acesso ou o recebimento de alertas pode afetar a operação.

Exemplo fictício: Empresa Demo, Cliente Demo, conta DEMO001 e e-mail contato@example.com. Use ambientes de treinamento para testes; não substitua informações de clientes reais por dados de exemplo.

12 Dispositivos e conectividade

Caminho: Dispositivos

Categoria	Ativos ou integração
Painéis de Alarme	Centrais, partições, zonas e receptores.
Dispositivos de Vídeo	Câmeras IP, DVRs, NVRs e canais de streaming.
Integrações de API	Plugins, gateways, IA e webhooks.
Reconhecimento Facial	Terminais faciais, controle de acesso e catracas.

Preparar o cadastro de vídeo

1. Abra **Dispositivos de Vídeo** → **Novo**.

2. Defina empresa, cliente quando aplicável, grupo do dispositivo e nome. Um equipamento pode pertencer à própria empresa, sem cliente específico.

3. Escolha o tipo de entrada: **ONVIF**, **RTSP Manual**, **RTMP Servidor**, **Webcam via Navegador** ou **Arquivo de Vídeo MP4**.

4. Avance pelas etapas **Conectividade**, **Parâmetros & Conexão** e **Geolocalização**, preenchendo somente os parâmetros compatíveis com o equipamento.

5. Antes de registrar e ativar, confira o vínculo e valide o funcionamento pelo procedimento técnico da empresa.

A listagem apresenta tipo, nome, rota de origem / RTSP, localização, estado e conexão. O estado cadastral e a conexão são informações distintas. Uma câmera cadastrada como ativa pode ter falha de comunicação.

Cuidados com os parâmetros

Não inclua endereços reais, usuários, senhas de câmeras ou URLs com credenciais em manuais, chamados de circulação ampla ou mensagens automáticas. Integrações exigem rotas, permissões e formatos compatíveis, definidos pelo responsável técnico.

13 Regras de detecção de IA

Caminho: AI → Regras de Detecção → Novo

A regra relaciona câmera, área observada, alvo, lógica e agenda. Ela define o contexto em que uma detecção deve produzir um evento; não é a mesma coisa que a automação que comunicará ou encaminhará esse evento.

1. Selecione o **Cliente** quando aplicável e a **Câmera Alvo**.

2. Carregue a imagem de referência no **Visualizador IA**. Use **Atualizar Snapshot** quando necessário.

3. Configure a **Zona 1** e adicione outras zonas quando o projeto exigir. A interface permite mover e redimensionar a área pelas alças.

4. Escolha a categoria de alvo: **Objetos**, **EPI**, **Comport.**, **Avançados** ou **Integração**, e selecione o alvo compatível.

5. Associe o **Evento Contact ID** e escolha a lógica: **Intrusão**, **Ausência**, **Aglomeração** ou **Excedido**.

6. Ajuste **Tempo na Área** com unidade correta, horário, sensibilidade, taxa de processamento FPS e dias da semana.

7. Revise zonas, horários e alvos antes de **Criar Regra**. Valide a resposta em cenário controlado e autorizado antes de considerar a configuração operacional.

Exemplo fictício de permanência

Na Câmera Demo 01, uma área controlada utiliza lógica Excedido e tempo de 30 minutos. A configuração deve usar a unidade Minutos, não Segundos. O código do evento e o procedimento de tratamento devem corresponder ao projeto. O exemplo não determina qual valor será adequado para outra área.

Atenção Maior sensibilidade ou FPS não significa automaticamente melhor resultado. Iluminação, oclusão, enquadramento, capacidade de processamento e calibração influenciam a detecção. Revise falsos positivos e falhas em condições representativas.

14 Automações e comunicação

Caminho: Automação → Novo

Uma automação relaciona um gatilho a uma ação e a uma janela de execução. A página separa **Regras de Automação** de **Histórico & Logs de Execuções**. Consulte o histórico para conferir o que foi executado, em vez de supor sucesso pela existência da regra.

Etapa 1 Gatilho

Informe nome, cliente vinculado, origem do evento e descrição. Revise o estado operacional: a regra ativa pode processar eventos. Os gatilhos disponíveis dependem do contexto, incluindo integrações por webhook, detecções de IA e estados de câmera ou gravação.

Etapa 2 Ação

Escolha a ação apresentada pelo sistema. A interface contempla configuração de WhatsApp e descreve também notificação mobile, API externa e O.S. No WhatsApp, confira instância remetente, destinos e mensagem. Um destino vazio pode usar os responsáveis do cadastro; não equivale a impedir o envio.

O editor permite inserir variáveis como **{cliente}**, **{conta}**, **{camera}**, **{evento}** e **{data_hora}**. Há modelos prontos e variáveis específicas para outros contextos. Revise se cada variável está disponível no evento de origem.

Etapas 3 e 4 Horários e resumo

Defina início e fim da janela; a interface informa que campos de horário vazios correspondem a 24 horas. Ajuste o intervalo anti-flood de 0 a 30 minutos para controlar repetição de ações. Revise o **Resumo Gráfico** antes da confirmação final do fluxo.

Mensagem fictícia: “Cliente Demo: recebemos um evento de câmera indisponível às 14h32. A equipe técnica foi informada. Protocolo DEMO001.” A frase “equipe informada” só deve ser usada se esse encaminhamento fizer parte do fluxo executado.

Atenção Não habilite uma regra real apenas para testar o manual. Valide conta, origem, destinatários e comportamento de falha em ambiente controlado. Eventos críticos devem preservar o escalonamento humano definido pela central.

15 Usuários e perfis de acesso

Caminho: Usuários ou Perfis de Acesso

Preparar um perfil

Em **Perfis de Acesso** → **Novo**, informe nome, empresa vinculada e descrição. A matriz separa permissões de **Acesso**, **Inserir**, **Atualização** e **Excluir** por aplicação ou módulo. Use a busca da matriz e os controles de expandir / recolher para localizar o recurso.

A opção global não corresponde a um vínculo restrito a uma única empresa. Revise o escopo antes de registrar o perfil. Conceda apenas as funções necessárias ao cargo; não utilize “marcar tudo” como padrão de configuração.

Preparar um usuário

1. Abra **Usuários** → **Novo** e informe nome, e-mail e telefone / WhatsApp.

2. Associe o **Grupo** e a **Empresa** corretos.

3. Quando necessário, restrinja o acesso a um **Cliente Específico**. A opção de acesso a todos os clientes da empresa tem escopo diferente.

4. Siga os requisitos de senha exibidos: mínimo de 12 caracteres, número, letra maiúscula e minúscula, além de confirmação idêntica. Nunca use a senha de exemplo de um manual.

5. Revise os demais campos e opções, inclusive criação automática de cliente quando apresentada, antes da confirmação do cadastro.

Revisão periódica

Confira usuários ativos, grupo, empresa e último login. Mudanças de equipe devem ser refletidas no acesso autorizado. Os **Logs de Usuários**, em Configurações, oferecem uma trilha de atividades para a supervisão.

Atenção A concessão de permissões é uma decisão administrativa. Não registre novos acessos, amplie escopos ou altere credenciais durante uma simples consulta de documentação.

16 Mapa de dispositivos

Caminho: Mapa de Dispositivos

O mapa relaciona a posição dos ativos à situação de comunicação. Ele permite alternar o contexto sem abrir individualmente cada câmera, central ou leitor. A posição depende da geolocalização cadastrada; um ponto no mapa não é uma medição automática da posição física atual.

Consultar o conjunto de ativos

1. Escolha Empresa e Cliente para delimitar o conjunto.

2. Selecione o tipo: Todos os Dispositivos, Câmeras, Centrais de Alarme ou Leitores Faciais.

3. Escolha Todos os Status, Online ou Offline e utilize a busca quando precisar localizar um equipamento.

4. Use Enquadrar para ajustar a visualização aos pontos do conjunto. A opção Satélite alterna a camada, e os controles de zoom aproximam ou afastam o mapa.

5. Selecione o agrupamento ou ponto desejado e confira a identificação do dispositivo antes de seguir para outra consulta.

Resultado esperado

A contagem de ativos e os pontos devem corresponder ao escopo selecionado. Quando o ativo não aparece, confira filtros, vínculo e coordenadas do cadastro. Uma posição genérica ou repetida exige revisão cadastral, não deslocamento físico presumido.

Exemplo fictício: Empresa Demo → Cliente Demo → Centrais de Alarme → Offline. A consulta identifica quais centrais precisam de verificação de comunicação; ela não confirma invasão, falha de energia ou causa da indisponibilidade.

17 Cadastro de empresa e personalização

Caminho: Empresas → Novo

O cadastro da empresa define a propriedade administrativa, os módulos e os limites de serviço. A interface informa que o salvamento pode criar automaticamente um acesso administrativo com o e-mail comercial; por isso, registrar empresa é também um ato de provisionamento de acesso.

1. Escolha o Tipo de Empresa: Master, Filial ou Terceirizada, conforme a estrutura autorizada.

2. Defina a Empresa Responsável quando houver vínculo de gestão. Confira o alcance de uma empresa sem responsável definido.

3. Informe nome fantasia, razão social quando aplicável, CNPJ, e-mail comercial, WhatsApp e contatos.

4. Cadastre endereço e website e selecione a logo. A interface recomenda 240 × 80 pixels, proporção aproximada 3:1, PNG transparente ou SVG, com limite informado de 2 MB.

5. Revise Habilitar IA e os Módulos Contratados. Não confunda habilitação do módulo da empresa com permissão individual do usuário.

6. Confira permissão de gravação, retenção, recebimento de alertas e estado de acesso antes de Registrar Empresa.

Conferência de implantação

Após um cadastro autorizado, valide identidade visual, empresa responsável, módulos, acesso administrativo e clientes vinculados. As credenciais iniciais devem ser tratadas pelo administrador conforme a política de acesso, sem transcrevê-las em documentos ou mensagens de treinamento.

Atenção Não use contatos reais para demonstrar Testar & Verificar E-mail ou WhatsApp. Uma logo ou um nome de empresa fictício não tornam os destinatários do cadastro fictícios.

18 Centrais de alarme

Caminho: Dispositivos → Painéis de Alarme

Consultar o painel

A listagem mostra identificação, localização, indicação de armado, estado cadastral e ações. Leia separadamente conexão, cadastro ativo e estado armado: eles respondem a perguntas diferentes e não são prova isolada de recepção de eventos.

Preparar o cadastro

1. Abra Novo e selecione empresa e cliente, quando o painel não for da própria sede.

2. Informe Nome do Painel, IP, marca e modelo compatíveis.

3. Preencha MAC / Identificador obrigatório e número de série quando disponível. Use os valores do equipamento correto.

4. Defina Tempo Verificação e Teste Periódico de acordo com o projeto, observando a unidade em minutos.

5. Cadastre localização física, latitude e longitude; confira o resultado de Buscar GPS antes de aceitá-lo.

6. Revise Equipamento Ativo e a indicação Painel ARMADO antes de Registrar Painel.

Verificar a integração

Em uma implantação autorizada, confira um evento de teste recebido no histórico, sua conta, origem, código e horário. A existência do cadastro não comprova a recepção. Compare os dados com os códigos e grupos de alarme usados pela central.

Atenção A interface exibe uma chave de estado armado no cadastro. Este guia não a trata como confirmação de comando remoto ao equipamento. O procedimento de arme e desarme deve seguir a integração e a autorização específicas.

19 Leitores faciais e biométricos

Caminho: Dispositivos → Reconhecimento Facial → Novo

1. Informe Nome do Leitor / Local, fabricante e modelo do hardware.

2. Selecione Empresa Gestora e Cliente / Local Vinculado quando aplicável.

3. Informe IP ou Host DDNS, Porta API e as credenciais técnicas autorizadas.

4. Escolha Modo de Comunicação e Sentido de Acesso. A opção Push Server indica que o dispositivo notifica o K-Monitor; confirme se esse é o modo previsto para a instalação.

5. Confira Relé da Porta, Limite Faces e localização física. Esses campos devem refletir o equipamento instalado.

6. Marque somente os recursos efetivos: reconhecimento facial, biometria digital, cartão / RFID e QR Code.

7. Revise Dispositivo Habilitado e salve somente após a conferência técnica.

Entrada e saída

O sentido configurado influencia a leitura de percurso e frequência. Uma entrada cadastrada como saída pode produzir histórico incoerente mesmo quando a comunicação está online. Revise o sentido do leitor e a identidade associada antes de investigar permanências.

Resultado esperado

O leitor deve constar no cliente correto, com comunicação compatível e capacidade coerente. Na operação, confira recepção de uma leitura de teste autorizada e a identificação do ponto de acesso. Não presuma que marcar um recurso cria capacidade inexistente no hardware.

Exemplo fictício: Leitor Demo Entrada, Cliente Demo, sentido Gate IN. Identificação técnica e segredos permanecem no ambiente de configuração; o manual não utiliza IPs, números de série ou senhas de instalações reais.

20 Integrações de API e webhooks

Caminho: Dispositivos → Integrações de API → Novo

A integração representa a conexão com um serviço externo. O tipo cadastrado organiza o conector; a URL, o escopo e o mecanismo de autenticação determinam a comunicação efetiva. Não há um endpoint universal para todos os fornecedores.

1. Escolha Tipo da API e informe um Nome da Integração que identifique sua finalidade.

2. Preencha URL Base com o endereço aprovado para o serviço. Para exemplos, utilize apenas domínios reservados, como https://api.example.com.

3. Defina Empresa Matriz e Cliente Final. Uma integração global tem alcance diferente de uma integração exclusiva de cliente.

4. Selecione Sem Autenticação, Basic Auth, Bearer Token / JWT ou API Key Customizada somente conforme a especificação do serviço.

5. Preencha os campos de autenticação que o tipo selecionado apresentar, mantendo segredos fora do manual e dos registros de circulação ampla.

6. Confira Cadastrar como Ativa e Escutando Eventos antes de Salvar Integração.

Validação controlada

A listagem oferece Testar Conexão e Ver detalhes. Um teste de conexão pode transmitir dados ao endpoint; faça-o apenas contra o destino aprovado. Confirme autenticação, vínculo, recepção, classificação e tratamento de duplicidade antes de liberar a integração em produção.

Referência técnica

O menu do usuário oferece Documentação da API. Use a versão vigente para métodos, parâmetros e respostas. Este manual não cria rotas ou payloads não demonstrados pela documentação. Utilize identificadores de demonstração nos exemplos de homologação.

21 Listas de reconhecimento facial

Caminho: ID Control → Cadastro de Listas

Uma lista organiza identidades para consulta e alertas. A listagem relaciona ID, ID API, nome, quantidade de cadastros, empresa, conta, cliente e estado. Os botões de sincronização e salvamento podem interagir com a integração facial.

1. Pesquise a lista e confira empresa, cliente e ID API antes de criar outra com nome semelhante.

2. Para um novo agrupamento, escolha Novo e informe Nome da Lista.

3. Selecione empresa e cliente. A opção em nível de empresa não restringe a lista a um único cliente.

4. Quando disponível ao seu perfil, confira Vincular a ID Facial existente. A tela informa que deixar essa seleção vazia pode criar uma nova lista automaticamente no sistema facial ao salvar.

5. Preencha descrição e revise o estado Ativa. A lista ativa aparece nos seletores do painel.

6. Revise os vínculos e confirme Salvar Lista somente no contexto administrativo autorizado.

Resultado esperado

A lista deve aparecer no escopo correto e estar disponível para associar identidades. Se a sincronização produzir dúvida sobre duplicidade, compare IDs e propriedade em vez de confiar apenas no nome.

Exemplo fictício: Lista Equipe Demo, Empresa Demo, Cliente Demo. Categorias como colaboradores e visitantes são escolhas da operação; não são evidência de que uma pessoa esteja autorizada em qualquer instalação.

22 Cadastro de identidades e matrículas

Caminho: ID Control → Cadastros → Novo

1. Abra Novo Cadastro Facial e informe Nome Completo.

2. Preencha Matrícula / ID com o identificador aprovado para o cadastro. No treinamento, utilize Pessoa Demo 01 e KOM2025.

3. Selecione a Lista Facial correta. Se precisar de nova lista, revise o procedimento do capítulo anterior antes de criá-la.

4. Confira Status e Descrição / Observação.

5. Preencha os responsáveis, telefones / WhatsApp e e-mails de notificação quando fizerem parte da finalidade do cadastro.

6. Selecione as fotos faciais autorizadas. A interface aceita JPG, JPEG, PNG e WEBP e permite múltiplas fotos com diferentes ângulos e iluminações.

7. Revise nome, identificador, lista e contatos antes de Salvar Cadastro.

Qualidade e consistência

Use imagens nítidas e pertinentes à finalidade do cadastro. A fotografia de referência e o nome devem corresponder à mesma identidade. Evite duplicar uma pessoa com IDs diferentes ou associá-la a uma lista incorreta.

Importação e ações em lote

A página oferece Importar, seleção de registros e controle de Status. Antes de qualquer lote, confira escopo, origem dos dados, autorização e resultado esperado. Não aplique uma mudança geral por ter selecionado apenas a página atual; leia o alcance informado pelo sistema.

Atenção Este manual não contém fotografias de pessoas reais. Não use rostos ou contatos de clientes como material de demonstração nem realize inclusão biométrica apenas para reproduzir um exercício.

23 Painel de reconhecimento e acessos

Caminho: ID Control → Reconhecimento Facial

O ID Control reúne eventos de câmeras e leitores, com indicadores de reconhecimento facial, placas, colete / EPI, biometria e QR Code. A existência de um indicador não garante que aquela tecnologia esteja habilitada no ponto de acesso selecionado.

1. Confira os pontos de acesso e sua situação online / offline.

2. Escolha Todos, Confirmados, Suspeitos / Alertas ou Desconhecidos para delimitar os registros.

3. Utilize busca e filtros de Cliente, Câmera, Lista, Data e Horário.

4. Confira origem, instante, identidade apresentada e associação de lista antes de relacionar o registro a uma ocorrência.

5. Use Limpar filtros para retornar ao conjunto amplo quando houver dúvida sobre uma lista vazia.

Leitura de um resultado

Diferencie identidade cadastrada, reconhecimento recebido e decisão operacional. Uma similaridade ou indicação de lista exige contexto e conferência. Uma leitura ausente pode decorrer de comunicação, enquadramento, agenda, cadastro ou filtro; não conclua automaticamente que a pessoa não passou pelo local.

Resultado esperado

O painel deve exibir o conjunto correspondente aos filtros e o instante da atualização. Para investigar deslocamento, prossiga para Rastreabilidade com o alvo e o período corretos, sem misturar homônimos ou matrículas.

Exemplo fictício: Pessoa Demo 01, lista Equipe Demo, Câmera Demo 01 e data de treinamento. As categorias do painel orientam consulta; não substituem o procedimento de acesso físico da instalação.

24 Listas de placas LPR

Caminho: ID Control → Gestão de Listas e Placas LPR

A lista de placas organiza a associação de leituras e a política de alertas. A tabela apresenta nome, descrição, quantidade de placas, auto-ocorrência e estado. A função de cadastro da lista não deve ser confundida com o painel de leituras ao vivo.

1. Pesquise se já existe a lista correspondente à finalidade.

2. Selecione Criar Nova Lista LPR.

3. Informe Nome da Lista e Descrição da Lista.

4. Defina Confiança Mínima em percentual e a cor do card / insígnia conforme o projeto.

5. Revise a opção Disparar auto-ocorrência / alerta Kanban em leitura. Habilitá-la muda o comportamento de tratamento de eventos.

6. Confirme Criar Lista apenas após revisar a finalidade e o escopo.

Placas e validação

Utilize a gestão disponibilizada para a lista selecionada e confira a placa associada antes da validação. A formação e os campos podem depender da integração e da versão. O passo de inclusão de placa dentro de uma lista deve ser conferido na implantação, antes de um carregamento em lote.

Exemplo fictício

Lista Frota Demo, placa DEM1A23. O valor de confiança deve ser calibrado com o enquadramento e a qualidade reais da instalação, em homologação. A cor de um card é uma identificação visual e não demonstra, por si só, autorização ou risco.

Atenção Não use placas de veículos de clientes nas ilustrações. Uma automação ou auto-ocorrência de lista precisa de procedimento definido para confirmação, encaminhamento e duplicidade.

25 Painel de leitura de placas

Caminho: ID Control → Leitura de Placas LPR

1. Abra o painel e confira a indicação de atualização.

2. Escolha Todas as Leituras, Confirmadas ou Desconhecidas.

3. Use a busca para localizar a placa e restrinja Câmera, Lista e Data conforme a investigação.

4. Confira imagem, leitura e instante antes de associar o resultado ao veículo.

5. Use Limpar filtros se o conjunto não corresponder ao esperado.

Indicadores

O painel apresenta totais de leituras, leituras confirmadas, desconhecidas e câmeras LPR online. Os números correspondem ao contexto e período consultados. Não compare totais de períodos ou filtros diferentes.

Quando a leitura estiver incorreta

Compare a placa na imagem com o texto reconhecido e o enquadramento do veículo. Verifique iluminação, movimento, resolução e ponto de captura com o responsável técnico. Não atribua uma identidade ao veículo apenas porque parte dos caracteres é semelhante.

Relacionar à rastreabilidade

Com a placa confirmada e o intervalo definido, utilize Rastreabilidade para consultar registros de percurso. O resultado depende dos pontos que efetivamente receberam eventos; o sistema não preenche deslocamentos em áreas sem registro.

Exemplo fictício: DEM1A23 aparece na Portaria Demo às 14h00 e na Saída Demo às 14h25. O exemplo orienta comparação de registros, sem provar o trajeto entre os dois pontos ou a identidade do condutor.

26 Rastreabilidade de percurso

Caminho: ID Control → Rastreabilidade

A página de reconstituição permite consultar deslocamento por pessoa, placa ou nome em um intervalo. O objetivo é organizar registros cronologicamente, não inferir presença contínua em todo o período.

1. Selecione a Empresa correta no filtro.

2. Informe ou selecione o alvo no campo de busca. Use o ID ou matrícula quando houver risco de homônimos.

3. Defina De e Até de acordo com o intervalo da investigação.

4. Selecione Rastrear e confira a sequência retornada, identificando origem e horário de cada registro.

5. Compare entradas e saídas apenas quando o sentido dos pontos e a correlação de identidade estiverem configurados e validados.

Exemplo fictício de permanência

Pessoa Demo 01 tem registro de entrada às 12h00 e saída às 12h35 em pontos previamente configurados. O intervalo entre os registros é 35 minutos. Um limite de 30 minutos resulta em 5 minutos excedidos nesse exemplo. Sem confirmação do par de eventos e da identidade, não trate a diferença como permanência comprovada.

Resultado esperado

Os resultados devem corresponder à empresa, ao alvo e às datas selecionadas. Se não houver registros, revise filtros, relógio, sentidos de acesso, cadastro e recepção dos dispositivos. Não amplie o escopo para dados de outras empresas para preencher lacunas da consulta.

27 Consulta forense

Caminho: ID Control → Detecção Forense

A consulta forense apresenta registros de identificação e evento e pode conter dados sensíveis. O manual utiliza apenas rótulos de controles e exemplos fictícios; a consulta operacional deve permanecer restrita à finalidade autorizada.

1. Defina o objeto e a finalidade da consulta antes de iniciar.

2. Abra Filtros Avançados e selecione Empresa, Cliente e Câmera.

3. Use a pesquisa e a quantidade de registros por página adequada.

4. Revise as Colunas Visíveis. A tela oferece Identificação / Evento / Data, Endereço, Telefone, E-mail e Ações.

5. Consulte somente os detalhes necessários e confira a origem da informação antes de utilizá-la no atendimento.

6. Quando houver exportação autorizada, limite os campos e o conjunto de dados ao necessário para o destinatário.

Importação e captura

A página oferece ferramentas de importação de fotos, exportação e captura por webcam. Importar uma fotografia ou usar a câmera do navegador envolve dados de identidade e permissões adicionais. Não execute essas ações para ilustrar um manual ou para testar com imagens de pessoas sem autorização.

Conferência do resultado

Preserve a distinção entre dado cadastral, evento, associação e conclusão. Não use endereço ou contato encontrado isoladamente para determinar acesso, emprego, matrícula ou qualquer outro resultado sobre a pessoa.

28 Frequência e gestão de faltas

Caminho: ID Control → Frequência

O painel reúne total esperado, presentes, ausentes e atrasados / justificados. A interface permite consulta diária e mensal e pode usar nomenclatura escolar ou corporativa. Os resultados dependem de vínculos de cadastro, turnos e recepção de entradas.

1. Escolha Diário ou Mensal e confira a Data.

2. Restrinja Empresa, Unidade, Curso, Turma e Status quando esses campos estiverem presentes.

3. Use a busca para localizar o cadastro correto.

4. Confira Horário de Entrada, estado e indicadores de notificação antes de tratar uma ausência.

5. Revise atrasos e justificativas de acordo com o procedimento da instituição e com o responsável autorizado.

Ações que modificam a operação

Verificar Entradas, Sincronizar, Enviar ActiveSoft, Notificar Faltas e Justificar têm finalidades distintas. Não acione envio nem alteração de frequência para confirmar apenas a leitura da tela. A ausência de registro não é, por si só, prova de falta real.

Resultado esperado

Os indicadores e as linhas devem corresponder aos filtros. Antes de notificar, confira turno, tolerância, corte, contatos e eventual atraso de integração. Uma justificativa deve ter fundamento e responsável, sem alterar registros para corrigir artificialmente o indicador.

Exemplo fictício: Colaborador Demo 01, turno Demo, situação a conferir. O treinamento deve explicar a diferença entre sem registro de entrada, falta apurada e falta justificada, sem usar cadastros escolares ou de colaboradores reais.

29 Turnos tolerância e notificações

Caminho: ID Control → Turnos e Horários → Novo

1. Informe Nome do Turno e escolha Empresa / Cliente Vinculado.

2. Confira se a opção de vincular automaticamente todos os cadastros faciais ativos está marcada e avalie seu alcance antes de salvar.

3. Defina Horário de Entrada, Tolerância e Horário de Corte. A tolerância é apresentada como um horário, e não simplesmente uma quantidade de minutos.

4. Revise os canais Disparar WhatsApp e Disparar E-mail para Responsáveis. Desmarcar WhatsApp não desmarca necessariamente o e-mail.

5. Configure a mensagem, quando utilizada, e confira as tags disponíveis, como {nome}, {responsavel}, {empresa}, {data} e {horario_limite}.

6. Revise vínculos, horários e canais antes de Criar Turno.

Campo	Exemplo fictício	Efeito a conferir
Entrada	07h30	Horário previsto de chegada.
Tolerância	07h45	Após o horário, a interface indica atraso.
Corte	08h15	Horário de disparo de ausência configurado.

Modelos rápidos

A tela oferece sugestões Matutino, Vespertino, Integral e Noturno. São preenchimentos de referência; não substituem o calendário e o regime efetivos da unidade.

Atenção Antes de testar um turno, verifique ambos os canais e o conjunto vinculado. Uma seleção geral de todos os clientes ou todos os cadastros pode ter alcance maior que o previsto para o treinamento.

30 Omnichannel e chamados

Caminho: Omnichannel

O painel oferece Chat WhatsApp, Dashboard Chamados e Extrato de Eventos. Essas telas relacionam a comunicação ao tratamento operacional, mas a configuração dos canais, a disponibilidade do serviço e o perfil determinam quais funções podem ser utilizadas.

Consultar a central de atendimento

1. Abra Chat WhatsApp e confira os indicadores de Chamados, Urgências, SLA Vencido e Escalados.

2. A orientação da tela diferencia clicar para selecionar e dar duplo clique para abrir. Confira o chamado e o destinatário antes de abrir uma interação.

3. Consulte o histórico e a responsabilidade do atendimento conforme os controles disponíveis na versão da empresa.

4. Somente depois de confirmar canal, cliente e finalidade execute uma comunicação autorizada. Não use conversas reais como exercício do manual.

Quadro e extrato

Use Dashboard Chamados para acompanhamento e Extrato de Eventos para consulta do histórico relacionado. Os nomes de estados e ações devem ser conferidos na tela carregada; não se deve presumir que o quadro utilize os mesmos estados do Monitor.

Quando aparecer Carregando chamados

Aguarde a consulta inicial e utilize uma atualização normal da página se houver falha persistente. Confira sessão, perfil, conexão e disponibilidade do serviço. Compare com outra sessão autorizada e registre o erro para suporte. Enquanto o conteúdo não carregar, não trate indicadores vazios como zero chamados.

Atenção Os passos internos de envio, transferência, encerramento e Kanban requerem conferência na sessão funcional do módulo. Nenhuma ação de comunicação é necessária para ler este guia.

31 Movimentações e alertas de PDV

Caminho: Arius PDV

O painel relaciona movimentações comerciais, telemetria da integração e configuração de alertas. A consulta mostra NSU, tipo, loja, PDV, data / hora, valor e situação de cancelamento. Um registro comercial deve ser interpretado com a regra de negócio e os registros associados.

1. Na aba Movimentações e Painel, selecione o período: histórico, hoje, ontem, últimos 7 dias, últimos 30 dias ou mês, conforme a tela.

2. Confira os indicadores de vendas canceladas, valor cancelado, latência e estabilidade da API.

3. Pesquise e filtre a movimentação, conferindo loja, PDV, NSU e horário.

4. Consulte o registro relacionado apenas quando houver autorização e finalidade operacional.

5. Compare indicadores somente com o mesmo período e escopo.

Configuração de alertas

A seção Disparo de Alertas e Notificações apresenta opções de alarme VMS e WhatsApp, destino e mapeamento de PDVs para ID da regra de alarme. Revise cada associação de número do PDV, descrição / câmera e ID antes de salvar. Um ID correto para um caixa pode ser incorreto para outro.

Terminal e diagnóstico

A aba Terminal de Testes e Logs é destinada a diagnóstico técnico. Testar Conexão consulta a integração; salvar opções pode mudar o envio de alertas. Não execute testes com cupons, valores ou destinatários reais apenas para produzir exemplos.

Exemplo fictício: Loja Demo, PDV Demo 01, NSU DEMO001. Cancelamento é um fato comercial a verificar; o registro não comprova fraude ou responsabilidade de uma pessoa.

32 Servidor armazenamento e continuidade

Caminho: Servidor

A tela técnica reúne desempenho geral, armazenamento, discos, diretórios de gravação e snapshots, pool de armazenamento, histórico de backup, alertas e consumo por cliente. As consultas de capacidade são distintas dos comandos que mudam o funcionamento do servidor.

Rotina de consulta

1. Abra o painel e utilize Atualizar Dados para consultar o estado atual.

2. Confira capacidade e ocupação por volume e a relação com gravações e snapshots.

3. Revise consumo por cliente sem alterar ativação ou retenção durante uma simples consulta.

4. Confira a existência e a data do histórico de backup conforme a rotina técnica aprovada. Não considere a presença de um arquivo como prova de restauração bem-sucedida.

5. Registre a necessidade de intervenção com horário, impacto e responsável técnico.

Alterações administrativas

Salvar Configurações de diretórios, mesclar e montar disco, alterar retenção e ativar ou pausar gravações em lote afetam a operação. Execute somente em mudança técnica autorizada, com avaliação do armazenamento, janela, validação e retorno previsto.

Proteção do histórico

A área também apresenta limpeza de snapshots e logs. Este manual não solicita nem executa purga. A retenção e o descarte exigem política própria e avaliação dos registros que precisam ser preservados.

Atenção Não compartilhe backups de banco, caminhos internos, tokens ou contatos técnicos reais em um manual de circulação geral. O teste de restauração deve ocorrer no ambiente e no procedimento definidos pela administração.

33 Licenças desktop e recursos

Caminho: Licenças Desktop

A gestão de licenças controla o uso do Integrator / Switch e apresenta cliente, tipo, estado, máquinas, validade e último check-in. Ocultar ou copiar uma chave não equivale a ativar uma instalação.

1. Consulte a licença e confira empresa, cliente, modalidade, validade e quantidade de máquinas utilizadas.

2. Para emissão autorizada, abra Novo e confira o token apresentado sem divulgá-lo em materiais de treinamento.

3. Defina Empresa Responsável, Cliente Vinculado, nome do cliente final e contatos pertinentes.

4. Escolha Tipo, Status, Limite de Máquinas e validade. A interface informa condições em que a licença não terá expiração.

5. Revise os módulos habilitados e as cotas técnicas de câmeras, PDVs e workers de IA.

6. Confirme Emitir Licença somente após a aprovação comercial e técnica correspondente.

Diagnóstico de ativação

Confira validade, suspensão, limite de máquinas, check-in e módulos antes de investigar a aplicação desktop. Não altere a associação de uma máquina ou amplie cotas apenas para contornar uma falha. Registre o contexto e encaminhe ao responsável pelo licenciamento.

Exemplo fictício: Licença Demo, Cliente Demo, chave representada por [CHAVE_DEMO], uma estação de treinamento e módulos definidos para o exercício. Nenhum token real está incluído neste documento.

34 Configurações e cadastros de apoio

Caminho: Configurações

Área	Conferência principal
Setores e departamentos	Destino de triagem e acompanhamento das O.S.
Categorias e problemas de O.S.	Classificação e relação entre setor, categoria e subcategoria.
Códigos e grupos de alarme	Correspondência do código recebido com descrição, grupo e severidade.
Planos da empresa	Vínculo comercial e limites associados ao serviço.
Produtos fornecedores e categorias	Identificação e organização de materiais e serviços.
Módulos e menus	Disponibilidade comercial e estrutura de navegação.
Logs de usuários	Quem executou qual ação e em que contexto.
Manutenção e licenciamento	Janelas técnicas e permissões de uso da plataforma.

Procedimento administrativo comum

1. Pesquise se o registro já existe no escopo correto.

2. Confirme o relacionamento com empresa e demais cadastros antes de criar outro.

3. Preencha os campos obrigatórios e revise descrições que serão utilizadas por operadores.

4. Salve somente com autorização e confira a disponibilidade no formulário que utiliza esse cadastro.

5. Registre a mudança no procedimento interno e revise os acessos quando a alteração tiver impacto no trabalho da equipe.

Alterar um rótulo de código ou grupo pode modificar a interpretação de eventos sem mudar a origem do sinal. Valide uma amostra controlada e mantenha a referência entre código, descrição e ação operacional.

35 Implantação e validação da operação

Sequência recomendada de preparação

1. Defina empresa, estrutura de gestão, módulos, plano e retenção.

2. Organize clientes, contatos, setores e procedimentos de atendimento.

3. Prepare perfis e usuários com escopo compatível.

4. Cadastre dispositivos e integrações; valide comunicação e identificação de origem.

5. Configure regras de IA e códigos de evento, calibrando zonas e agenda.

6. Configure listas, identidades e turnos quando necessários.

7. Prepare automações e destinatários de homologação antes de liberar disparos.

8. Valide Monitor, mosaico, gravação, relatórios e continuidade com cenários controlados.

Critérios de aceite

Teste fictício	Resultado a comprovar
Evento Demo	Cliente, dispositivo, código, horário e fila corretos.
Atendimento Demo	Responsável, nota, encaminhamento e conclusão registrados.
Vídeo Demo	Imagem ao vivo e histórico conferidos separadamente.
Automação Demo	Destino aprovado, variáveis válidas e execução rastreável.
Acesso Demo	Usuário vê apenas o escopo e as ações aprovadas.
Falha Demo	Operador identifica a indisponibilidade e sabe escalar.

Registre evidência de cada aceite com identificadores de treinamento. Não considere uma configuração concluída apenas porque o formulário foi salvo. A validação deve verificar o resultado ponta a ponta e o comportamento de falha.

36 Entradas de vídeo e validação do sinal

Caminho: Dispositivos → Dispositivo de vídeo → Novo

O assistente separa identificação, conexão e localização. Cadastre uma origem de treinamento antes de associar a câmera às regras e às rotinas de gravação.

1. Informe o nome da câmera, a empresa e o cliente quando aplicável. Escolha o tipo de origem oferecido no assistente.

2. Para RTSP Manual, avance à configuração de conexão. Revise IP ou host, porta RTSP, caminho do stream e usuário e senha próprios do dispositivo. A porta apresentada inicialmente é 554; confirme a porta efetivamente configurada.

3. Quando utilizar URL RTSP completa, confira o endereço e o canal. Não publique a URL se ela contiver credenciais.

4. Use os recursos de validação de conexão, snapshot ou descoberta ONVIF somente no equipamento autorizado. Observe o estado informado e, quando disponível, a latência.

5. Confira marca e modelo. Avance à localização e revise os dados exigidos na sua versão antes de salvar.

6. Após um cadastro autorizado, confira imagem ao vivo, horário, SUB/MAIN e disponibilidade no mosaico. Valide gravação e retenção separadamente.

Conferência técnica

Imagem ao vivo não comprova gravação histórica. Falha de descoberta ONVIF não demonstra, por si só, que o RTSP está indisponível. Confira rede, porta, canal, permissões e codec com o responsável técnico.

Atenção A interface pode tentar obter uma imagem ao preencher a conexão. Utilize endereços de dispositivos autorizados mesmo antes de salvar o cadastro.

37 Diagnóstico e suporte

Situação	Primeiras verificações
Evento não aparece	Revise empresa, cliente, período, origem, analítico e estado. Limpe filtros e consulte o histórico antes de concluir que não houve recepção.
Sem vídeo ou erro de mídia	Confira câmera, conexão da estação e estado do dispositivo. Compare SUB / MAIN e consulte Diagnóstico / Probe. Encaminhe ao técnico sem expor credenciais.
Gravação não encontrada	Confira câmera, data, horário, retenção e estado da gravação. Ausência de trecho histórico não é resolvida apenas abrindo vídeo ao vivo.
Botão indisponível	Verifique seleção da ocorrência, responsável, perfil e configuração do serviço. Não force o comando com outra conta.
Mensagem automática não chegou	Confira regra ativa, gatilho, cliente, janela, anti-flood, instância, destinatários e logs. Não repita disparos indiscriminadamente.
Muitos alertas repetidos	Revise lógica, zona, tempo, horário e repetição. Diferencie ajuste de detecção de controle anti-flood da automação.
Indicadores divergentes	Compare período e filtros. Confira escopo da empresa e situação dos atendimentos antes de confrontar totais de telas diferentes.

Informações para solicitar suporte

Registre data e hora, módulo, ação realizada, mensagem de erro, alcance do problema, identificação operacional necessária e verificações já feitas. Anexe somente evidências pertinentes e autorizadas. Use o recurso **Reportar Bug** quando previsto pela política da empresa.

Exemplo fictício: “02/11/2026, 14h32 - Mosaico: Câmera Demo 01 sem mídia em SUB e MAIN. Outros canais abrem na mesma estação. Solicita-se verificar o stream. Sem alteração de parâmetros.”

38 Exercícios e listas de conferência

Exercício 1 Verificação de evento

Em ambiente de treinamento, localize uma intrusão fictícia do Cliente Demo. Confirme origem e horário, examine as evidências, redija uma observação objetiva e explique qual situação exige decisão humana. Não use um evento real para simular atendimento.

Exercício 2 Permanência na área

Planeje uma regra da Câmera Demo 01 com lógica Excedido e tempo de 30 minutos. A Pessoa Demo 01 entra às 12h00 e sai às 12h35: o exemplo tem 35 minutos de permanência e 5 minutos acima do limite. A correlação entre entrada e saída depende da configuração e integração adotadas; a regra de área, isoladamente, não comprova esse vínculo de identidade.

Exercício 3 Comunicação não crítica

Desenhe o fluxo de câmera indisponível: evento → validação da regra → mensagem ao contato de teste → acompanhamento nos logs → escalonamento técnico quando previsto. Defina quem receberá a mensagem e como a falha de envio será acompanhada antes de habilitar qualquer disparo.

Conferência do início do turno

• Sessão individual, empresa e perfil corretos.

• Filas Novos / Andamento, Espera e Despachado revisadas.

• Ocorrências em tratamento e responsáveis identificados.

• Câmeras e gravações necessárias conferidas.

• Contatos, procedimentos e suporte disponíveis.

Conferência antes de concluir ou passar o turno

• Resultado e evidências coerentes com a ocorrência.

• Contatos e encaminhamentos registrados de forma objetiva.

• Pendências com responsável e estado adequado.

• Nenhuma mensagem ou automação de teste ativa na produção.

• Sessão encerrada segundo a política da central.

39 Glossário e referência

Termo	Significado neste manual
Evento	Registro recebido de uma origem, como câmera, analítico ou alarme.
Ocorrência	Contexto apresentado para tratamento operacional e associação de atividades.
Evidência	Imagem ou registro usado para verificar e documentar uma ocorrência.
SLA	Prazo ou nível de serviço configurado para a operação.
TMT	Tempo médio entre entrada e conclusão, conforme Dashboard.
O.S.	Ordem de serviço para encaminhamento técnico ou operacional.
FPS	Quantidade de quadros processados por segundo.
SUB / MAIN	Fluxos de vídeo alternativos disponíveis conforme dispositivo.
LPR	Leitura e reconhecimento de placas veiculares.
Contact ID	Código de evento utilizado na classificação ou integração.
Webhook	Interface pela qual um sistema pode receber ou enviar informações de um evento.
Anti-flood	Intervalo entre disparos para controlar ações repetitivas.

Referência da edição

Interface web K-Monitor Center consultada em 2 de novembro de 2026. As rotas de referência são o login e os módulos Monitor, Dashboard, Clientes, Dispositivos, Mosaico, Gravação, Relatórios, AI, Automação, Usuários, Perfis de Acesso, Configurações, Omnichannel e ID Control.

As telas podem evoluir após esta edição. Consulte os rótulos apresentados na sua versão e a orientação do administrador quando houver diferenças. Os procedimentos internos de emergência, contato e escalonamento devem complementar este guia.

Endereço de acesso: https://k-monitorcenter.app/login

40 Abrangência e validação desta edição

Este manual reúne procedimentos operacionais e administrativos identificados na interface web consultada em 2 de novembro de 2026. Os exemplos são fictícios. A consulta para sua elaboração foi realizada sem cadastrar, excluir, editar registros ou enviar comunicações de teste.

Área	Abrangência
Operação	Monitor, filtros, atendimento, anotações, transferências, estados, evidências e ordens de serviço.
Vídeo	Mosaico, diagnóstico de sinal, reprodução, dispositivos e mapa.
Identificação	Listas e cadastros faciais, reconhecimento, LPR, percurso, consulta forense, frequência e turnos.
Administração	Empresas, clientes, usuários, perfis, integrações, regras de IA, automações, servidor, licenças e configurações.
Gestão	Dashboard, relatórios, PDV, implantação, diagnóstico e exercícios.

Procedimentos que exigem homologação

Os formulários e controles foram consultados sem executar salvamentos, disparos, alterações de estado de equipamentos ou testes de comunicação. Os resultados descritos orientam a conferência após uma execução autorizada; não constituem certificação de funcionamento de cada integração. Operações com mídia dependem da disponibilidade do stream e das permissões.

Pendências de verificação da interface

O Chat Omnichannel permaneceu em carregamento no navegador de consulta, embora tenha sido informado que abre normalmente na operação. A abertura, resposta, transferência e conclusão internas do chat, assim como o quadro de chamados, precisam de conferência nessa sessão funcional. O capítulo correspondente delimita o fluxo e não atribui comandos não observados. A documentação técnica de API também não carregou; endpoints e contratos devem ser obtidos na referência técnica vigente.

A inclusão de placas dentro de uma lista LPR e as etapas condicionadas a cadastros efetivos devem ser validadas em ambiente de treinamento. Esta edição não substitui a documentação técnica das integrações nem os procedimentos internos de emergência e escalonamento.