

ZOOX Wi-Fi

Smart Wi-Fi, autenticação segura, dados acionáveis e experiência digital no captive portal.

Portal cativo

Autenticação gov.br

Analytics

Campanhas

Integrações por API



Insight to act

Conheça, segmente e ative seus usuários.

23

países

3.900

clientes

+20M

conexões

+200

variáveis

O que a solução entrega

O Zoon Wi-Fi transforma a rede visitante em um canal de autenticação, relacionamento, analytics e ativação de dados.

Conectividade com identificação

Portal cativo para liberar acesso Wi-Fi com regras de sessão, autenticação personalizada, aceite de termos e coleta consensual de dados.

Engajamento e mídia

Campanhas por imagem, vídeo, tags JavaScript, e-mail, SMS, cupons, pesquisas, NPS e landing pages segmentadas.

Conhecimento do usuário

Registro de novos e recorrentes, perfil do usuário, dispositivo, local de conexão, idioma, tráfego, horários e histórico de interações.

Integração operacional

APIs e integrações com CRM, PMS, PDV, gateways, disparadores, bases externas, login corporativo e hardware homologado.

Fluxo simplificado da experiência

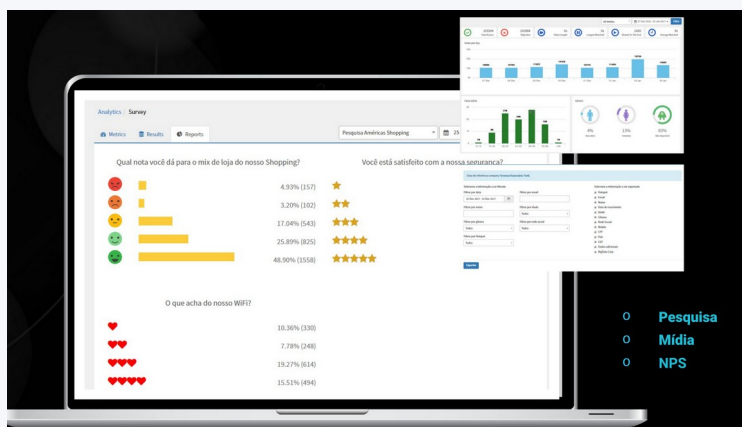
Seleciona Wi-Fi

Portal Zoon

Autentica

Libera internet

Ativa dados



Dashboard, relatórios, segmentação e ações de marketing são operados no ambiente administrativo Zoon.

Funcionalidades principais do Zoox Wi-Fi

Módulos disponíveis para conectividade, personalização, marketing, analytics, localização e integrações.

Portal cativo	Template base ou customizado com HTML/CSS/JavaScript, logos, backgrounds, formulários e landing pages.
Dados de login	Nome, e-mail, telefone, CPF, documento, idade, gênero, país, idioma e campos adicionais configuráveis.
Login progressivo	Coleta gradual dos dados em conexões futuras para reduzir fricção e melhorar a jornada.
Planos de uso	Tempo de sessão, idle timeout, velocidade de download/upload e regras por perfil ou local.
Campanhas	Imagem, vídeo, GIF, JavaScript, VAST/VPAID, banners, pesquisas, NPS, e-mail, SMS e cupons.
Relatórios	Dashboards, CSV, PDF, relatórios automáticos por e-mail e envio via integração.
Localização ZMX	Mapa de calor, dispersão, fluxo, trajeto de usuários e análise de áreas internas.
Wi-Fi Analytics	Saúde da rede, APs online/offline, clientes por AP e nível de sinal recomendado.
Integrações	CRM, PMS, PDV, gateway de pagamento, e-mail/SMS, bases externas, APIs e login corporativo.
Segurança	HTTPS, logs de auditoria, criptografia, AWS, WAF, backup diário e perfis administrativos.

Como o gov.br entra no fluxo Wi-Fi

A Zoox pode incluir o botão/fluxo de login gov.br no portal cativo, desde que o órgão público disponibilize a integração oficial e credenciais.

Pré-requisito essencial

Para configurar autenticação via gov.br, o órgão público deve fornecer API/credenciais, autorização formal, escopos permitidos, URLs de homologação/produção e regras de privacidade aplicáveis ao serviço.

Fluxo técnico esperado

- 1 Usuário seleciona SSID e abre o portal Zoox
- 2 Portal exibe a opção de autenticação gov.br
- 3 Usuário é redirecionado ao provedor gov.br
- 4 gov.br autentica e retorna autorização/tokens
- 5 Zoox valida retorno e libera sessão Wi-Fi
- 6 Dados autorizados alimentam relatórios/integrações

Responsabilidade do órgão público

- Formalizar adesão e autorizar uso do Login Único.
- Fornecer client_id/client_secret ou método equivalente.
- Informar escopos, dados autorizados, URLs e contatos técnicos.

Responsabilidade Zoox

- Configurar portal e botão gov.br.
- Implementar redirects, callback e validação técnica.
- Mapear dados recebidos para relatórios e integrações.

Observação comercial/técnica: a autenticação gov.br depende da liberação e documentação do órgão responsável. Sem API e credenciais válidas, a Zoox não consegue autenticar o cidadão diretamente em nome do órgão.

Informações necessárias para implantação gov.br

Checklist para reduzir retrabalho entre órgão público, time técnico Zoxx e responsáveis pelo ambiente de rede.

Adesão e autorização	Confirmação formal do órgão público para uso do Login Único no serviço digital.
Credenciais	Client ID, segredo/chave, ambiente de homologação e produção, e método de rotação/renovação.
URLs	Authorization URL, token URL, userinfo/serviços disponíveis, callback/redirect URI, logout URL quando aplicável.
Escopos e dados	Quais atributos poderão ser consumidos: CPF, nome, e-mail, telefone, nível de conta, selos/confiabilidade etc.
Políticas e LGPD	Base legal, termo de uso, aviso de privacidade, consentimento, retenção e finalidade do tratamento.
Homologação	Massa de testes, usuários de teste, cenários de erro, SLA de suporte e critérios de aceite.
Rede Wi-Fi	SSID, controlador/APs homologados, captive portal, redirect, Radius e regras de liberação de navegação.
Operação	Contato técnico do órgão, contato Zoxx, janela de implantação, plano de rollback e suporte pós-go-live.

Escopo da integração Zoxx

- Inserção de gov.br como opção no fluxo de login do portal cativo.
- Validação do retorno da autenticação conforme documentação recebida.
- Mapeamento de atributos permitidos para conexão, relatórios e integrações.
- Fallback para outros métodos de login quando o gov.br estiver indisponível, se aprovado.

Critério de sucesso

Usuário autentica com gov.br, retorna ao captive portal Zoxx, recebe liberação de internet, e os atributos autorizados ficam disponíveis em relatórios ou integrações acordadas.

Coleta consensual e uso acionável de dados

A plataforma registra eventos de acesso e permite transformar as conexões Wi-Fi em dados para análise, segmentação e operação.

Dados técnicos de acesso

MAC address, IP privado, dispositivo, tipo de sistema operacional, local de conexão, horário de conexão/desconexão e consumo de banda.

Dados cadastrais

Nome, e-mail, telefone, idade, gênero, CPF/documento, país, idioma e campos adicionais configuráveis.

Consentimento e termos

Opt-ins específicos para campanhas, pesquisas e usos permitidos, com jornada ajustada para a finalidade de coleta.

Exportação e integração

CSV, PDF, relatórios automáticos por e-mail, dashboards e integrações com sistemas terceiros.

Exemplos de aplicação dos dados

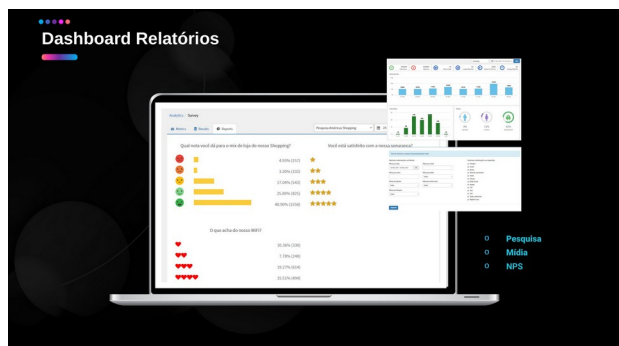
- Identificar novos vs. recorrentes e comportamento por local/unidade.
- Segmentar campanhas por perfil, horário, sistema operacional, recorrência e região.
- Acionar pesquisas e NPS no login ou por e-mail após X horas/dias.
- Enviar dados para CRM, PMS, PDV, marketing automation ou base externa.

Governança recomendada

Definir finalidade, minimização de dados, retenção, campos obrigatórios/opcionais, base legal, texto de consentimento, logs de auditoria e responsáveis por atendimento aos titulares.

Dashboards para operação, marketing e gestão

Relatórios em tempo real e históricos para acompanhar conexão, perfil, mídia, pesquisas, NPS e saúde da rede.



Indicadores de conexão

- Total de conexões no dia/período.
- Novos usuários e recorrentes.
- Ranking de conexões e últimas conexões em tempo real.
- Consumo de banda, horário, local e jornada até conectar.

Pesquisas

Respostas consolidadas ou por usuário, data/hora exata, exportação CSV/PDF e envio automatizado.

Mídia

Visualizações, skips, quartis de vídeo, impactos por campanha e monetização por visualização.

NPS

Detratores, neutros, promotores, comentários, comparativos e segmentação por unidade/grupo.

Saídas de dados

- Dashboard administrativo.
- Arquivos CSV e PDF.
- Relatórios automáticos via e-mail.
- Integrações para envio de eventos e atributos a sistemas terceiros.

Benefício: unificar dados de conectividade, comportamento e engajamento em uma base acionável para CRM, atendimento, mídia e inteligência comercial.

Ativação no captive portal e pós-conexão

Campanhas segmentadas para comunicar, pesquisar, monetizar inventário e acionar o usuário no momento certo.

Formatos suportados	Imagem, vídeo MP4, GIF, banners, mosaico, modal, tags JavaScript, VAST/VPAID, e-mail, SMS e cupons.
Segmentação	Dia/hora, local, hotspot, novo/recorrente, gênero, idade, sistema operacional, região anterior e listas customizadas.
Regras de exibição	Obrigatória/opcional, amostragem, limite total ou diário, período de vigência e tempo mínimo de visualização.
Pesquisa e NPS	Perguntas condicionais, respostas livres/listas/checkbox/radio, notas, smiles, estrelas, comentários e call-to-action.
Relatórios	Impactos, cliques, aberturas, skips, visualização por quartis, respostas, exportações e envio automático.



Exemplo de jornadas

- Campanha institucional antes da liberação de internet.
- Pesquisa rápida pós-login por perfil de usuário.
- NPS disparado por e-mail após a visita.
- Cupom enviado a usuários de uma área específica.

Monetização de mídia Wi-Fi

A plataforma permite precificação por visualização, relatórios de performance e formatos de impacto compatíveis com o fluxo de autenticação.

Leitura do espaço físico e saúde da rede

Módulos opcionais para visão de fluxo, permanência, mapas e indicadores de qualidade da infraestrutura Wi-Fi.

Mapa de calor

Densidade de dispositivos/usuários por hora, setor, perfil, gênero, idade e recorrência.

Mapa de dispersão

Posição aproximada dos dispositivos no mapa, com variação conforme o hardware utilizado.

Mapa de fluxo

Movimentação entre zonas, entradas/saídas, permanência média e deslocamento entre áreas.

Trajeto

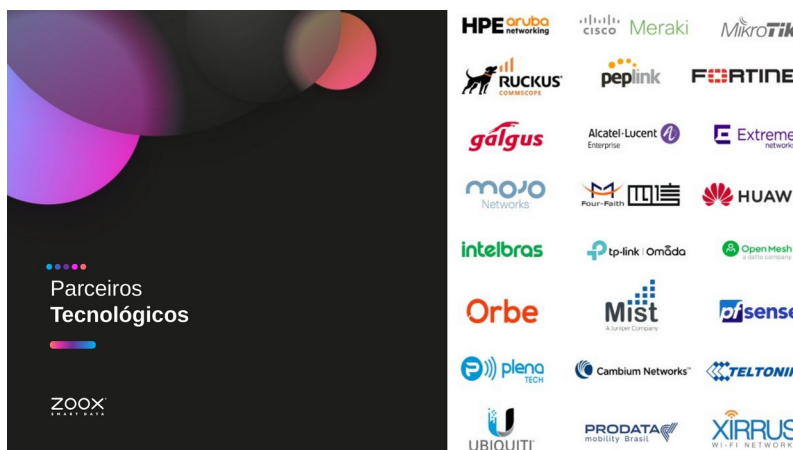
Rotas realizadas internamente a partir de zonas selecionadas do estabelecimento.

Wi-Fi Analytics

APs online/offline, clientes por AP e recomendação de nível de sinal.

Hardwares

Suporte informado para Aruba, Cisco Meraki e Cisco DNA Spaces no módulo ZMX.



Importante: dados de localização dependem da capacidade do fabricante/controlador, qualidade da planta baixa, calibração, densidade de APs e permissões técnicas do ambiente.

Integrações, operação e segurança da plataforma

A solução é baseada em software, integra-se a controladores/APs homologados e opera em arquitetura cloud escalável.

Arquitetura lógica

Usuário > SSID > AP/controlador > RADIUS/captive portal Zoxx > autenticação > internet > dashboards, campanhas e integrações.

Software	Portal cativo Zoxx, console administrativo, dashboards, campanhas, APIs e perfis de acesso.
Hardware	APs e controladores homologados; integração pode variar conforme fabricante, cloud/local controller e recursos disponíveis.
Login corporativo	LDAP/Active Directory, Azure AD/SAML 2.0, OpenID/OAuth 2.0 e Google LDAP para redes específicas.
Segurança	HTTPS, SSL, logs de auditoria, criptografia em trânsito/repouso, AWS WAF, backup diário e segregação lógica.
Operação	Monitoramento de principais clientes, perfis administrativos e licenciamento por número de APs ativos.

Premissas de projeto

- Lista de APs/controladores e topologia.
- SSID, VLAN, DHCP, DNS e regras de firewall.
- Fluxo de autenticação aprovado.
- Política LGPD e termos do cliente/órgão.

Entregáveis típicos

- Portal configurado e testado.
- Relatórios e permissões administrativas.
- Integrações validadas em homologação.
- Documentação de operação e aceite.

Próximo passo recomendado: validar requisitos gov.br e ambiente Wi-Fi, confirmar dados autorizados pelo órgão público e iniciar homologação com credenciais oficiais.