



RMS — Romma Monitoring System

Datasheet Técnico

Sistema de Monitoramento de Controle de Acesso

Versão 1.0 · 2026 · Romma Segurança Eletrônica

1. Visão Geral do Produto

O RMS (Romma Monitoring System) é uma plataforma web de monitoramento e gerenciamento de dispositivos de controle de acesso, desenvolvida pela Romma Segurança Eletrônica. Oferece supervisão em tempo real, gerenciamento de alertas, auditoria completa e notificações automáticas via WhatsApp.

Identificação do Produto

Fabricante	Romma Segurança Eletrônica
Produto	RMS — Romma Monitoring System
Versão	1.0
Tipo	Sistema de Monitoramento Web
Acesso	https://rms.rommaeletronica.com.br
Idioma	Português (Brasil)

Principais Benefícios

- Monitoramento contínuo 24/7 de todos os dispositivos de controle de acesso
- Notificações instantâneas via WhatsApp para eventos críticos
- Registro completo de auditoria com rastreabilidade total
- Interface web responsiva acessível de qualquer dispositivo
- Bloqueio automático de tentativas de acesso não autorizado

2. Especificações Técnicas

2.1 Requisitos de Servidor

Sistema Operacional	Windows 10/11 ou Windows Server 2019/2022
Processador	Intel Core i3 (6ª geração ou superior)
Memória RAM	Mínimo 4 GB (recomendado 8 GB)
Armazenamento	Mínimo 20 GB disponíveis (SSD recomendado)
Rede	Conexão de internet com IP fixo ou DDNS, porta 80/443
Banco de Dados	PostgreSQL 13 ou superior

2.2 Compatibilidade com Dispositivos

Fabricante	Intelbras
Modelos Testados	SS 5532 MF W
Protocolo	HTTP / HTTPS — Modo Online 1.0 e Modo Online 2.0
Porta Padrão	80 (HTTP) / 443 (HTTPS)
Autenticação	Digest Authentication

2.3 Capacidades

Dispositivos Monitorados	Ilimitado (limitado pelo hardware do servidor)
Frequência de Verificação	A cada 30 segundos por dispositivo
Latência de Notificação	Inferior a 5 segundos após detecção
Notificações WhatsApp	Até 10 números simultâneos por evento

3. Segurança

3.1 Segurança de Acesso

Protocolo	HTTPS com TLS 1.2/1.3
Autenticação	Expiração configurável
Senhas de Dispositivos	Criptografadas
Bloqueio por Tentativas	5 falhas: 5 min 10 falhas: 30 min 15 falhas: permanente
Sessão	Invalidada imediatamente ao remover usuário

3.2 Permissões por Perfil

Funcionalidade	Admin. Protegido	Administrador	Operador
Dashboard	Sim	Sim	Sim
Alertas (ver/tratar/reportar)	Sim	Sim	Sim
Relatórios	Sim	Sim	Sim
Gerenciar Dispositivos	Sim	Sim	Nao
Gerenciar Usuários	Sim	Sim	Nao
Auditoria	Sim	Sim	Nao
Configurações do Sistema	Sim	Nao	Nao
Whitelist / Lista Negra	Sim	Nao	Nao

4. Monitoramento e Alertas

4.1 Métodos de Monitoramento

Verificação de Porta	Varredura de porta TCP a cada 30 segundos
Verificação de API	Consulta à API do equipamento — detecta travamentos
Webhook de Eventos	Recebimento em tempo real dos eventos do dispositivo
Keepalive	Resposta ao dispositivo confirma que o servidor está ativo

4.2 Tipos de Alertas

Tipo de Alerta	Severidade	WhatsApp Auto.
Dispositivo Offline	Critico	Sim
Credencial de Coação	Critico	Sim
Violação Física	Critico	Sim
Arrombamento de Porta	Critico	Sim
Queda de Energia	Critico	Sim
Acesso Negado (múltiplas tentativas)	Critico	Manual
Reinicialização	Atenção	Nao
Queda de Rede	Atenção	Nao
Possível Travamento	Atenção	Nao

5. Conectividade e Integração

5.1 Arquitetura de Comunicação

Proxy Reverso	Nginx com TLS 1.2/1.3
CDN / Proxy Externo	Cloudflare (Full Strict SSL)
Backend	FastAPI + PostgreSQL
Domínio	rms.rommaeletronica.com.br
Porta HTTPS	443
Porta HTTP Interna	80 (rede local para dispositivos)

5.2 Integração WhatsApp

Serviço	API para possível integração com Whatsapp
Variáveis Suportadas	{dispositivo} — nome do dispositivo {data} — data e hora
Envio Automático	Offline, Coação, Violação Física, Arrombamento, Bloqueio de IP