



Manual do Usuário

RMS — Romma Monitoring System

Sistema de Monitoramento

Versão 1.0 · 2026 · Romma Segurança Eletrônica

Sumário

1. Primeiros Passos	3
1.1 Acesso ao Sistema	3
1.2 Realizando o Login	3
1.3 Perfis de Acesso	3
1.4 Navegação	3
2. Dashboard	4
2.1 Visão Geral	4
2.2 Cards de Estatísticas	4
2.3 Feed de Alertas	4
3. Dispositivos	5
3.1 Lista de Dispositivos	5
3.2 Cadastrando um Dispositivo	5
3.3 Editando um Dispositivo	6
3.4 Limpando o Cache	6
4. Alertas	6
4.1 Central de Alertas	6
4.2 Tipos de Alertas	7
4.3 Tratando um Alerta	7
4.4 Reportando via WhatsApp	7
5. Relatórios	7
5.1 Filtros Disponíveis	8
5.2 Exportando para CSV	8
6. Auditoria	8
6.1 Principais Ações	8
6.2 Filtros	8
7. Usuários	8
7.1 Criando um Usuário	8
7.2 Remoção de Usuário	9
7.3 Política de Senhas	9
8. Segurança	9
8.1 Bloqueio Automático	9
8.2 Abas da Tela de Segurança	9
9. Configurações	9
9.1 Interface do Usuário	9
9.2 Configurações do Sistema (Admin. Protegido)	9
9.3 Templates de Mensagem WhatsApp	9

1. Primeiros Passos

1.1 Acesso ao Sistema

O RMS é acessado exclusivamente por navegador web. Não é necessário instalar nenhum aplicativo.

URL de Acesso	https://rms.rommaeletronica.com.br
Navegadores	Google Chrome, Firefox, Edge (versões recentes)
Dispositivos	Computadores, notebooks, tablets e smartphones

1.2 Realizando o Login

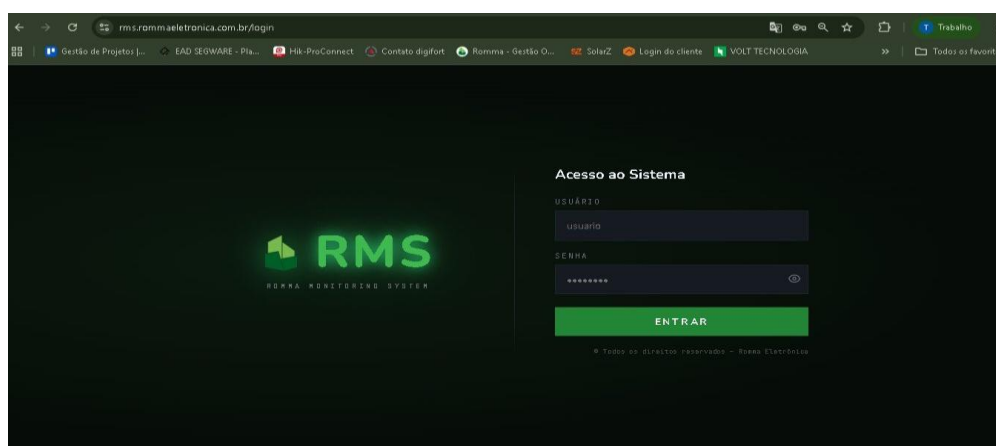


Figura 1 — Tela de login do RMS

Como fazer login

1. Abra o navegador e acesse <https://rms.rommaeletronica.com.br>
2. Informe seu Usuário e Senha
3. Clique no botão ENTRAR

INFO: Após 5 tentativas incorretas, o acesso é bloqueado temporariamente. Aguarde ou contate o administrador.

1.3 Perfis de Acesso

Perfil	Acesso Disponível
Operador	Dashboard, Alertas, Relatórios, Configurações de interface
Administrador	Todas as telas — exceto configurações sensíveis do sistema
Admin. Protegido	Acesso total: configurações do sistema, WhatsApp, bloqueios, whitelist

1.4 Navegação

O menu lateral dá acesso a todas as seções:

-  Dashboard — Visão geral em tempo real
-  Dispositivos — Gerenciamento dos pontos de acesso
-  Alertas — Central de alertas ativos e resolvidos
-  Relatórios — Histórico e exportação CSV

-  Auditoria — Registro de todas as ações
-  Usuários — Contas e permissões
-  Segurança — IPs bloqueados e whitelist
-  Configurações — Preferências e parâmetros

2. Dashboard

2.1 Visão Geral

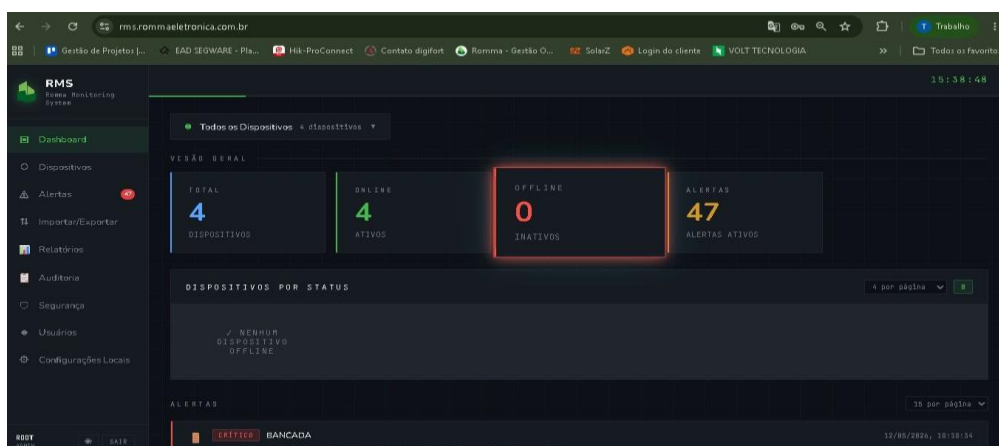


Figura 2 — Dashboard com estatísticas e feed de alertas

O Dashboard é a tela principal. Exibe status de dispositivos e alertas em tempo real, atualizados a cada 10 segundos.

2.2 Cards de Estatísticas

- Total — Quantidade total de dispositivos cadastrados
- Online — Dispositivos com comunicação normal
- Offline — Dispositivos sem comunicação
- Alertas — Número de alertas ativos

Clique em qualquer card para filtrar os dispositivos pelo status correspondente.

2.3 Feed de Alertas

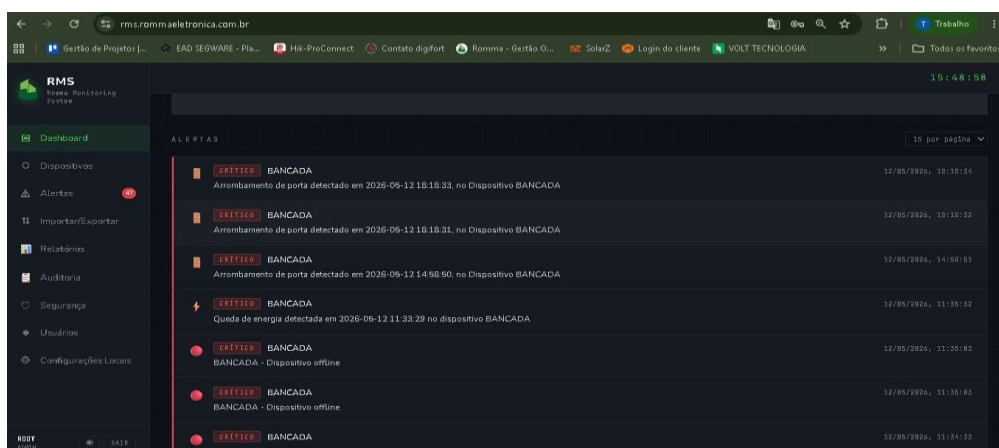


Figura 3 — Feed de alertas no Dashboard

O feed exibe alertas e eventos recentes: vermelho para críticos, âmbar para atenção, azul para informativos.

3. Dispositivos

INFO: Esta seção está disponível apenas para Administradores.

3.1 Lista de Dispositivos

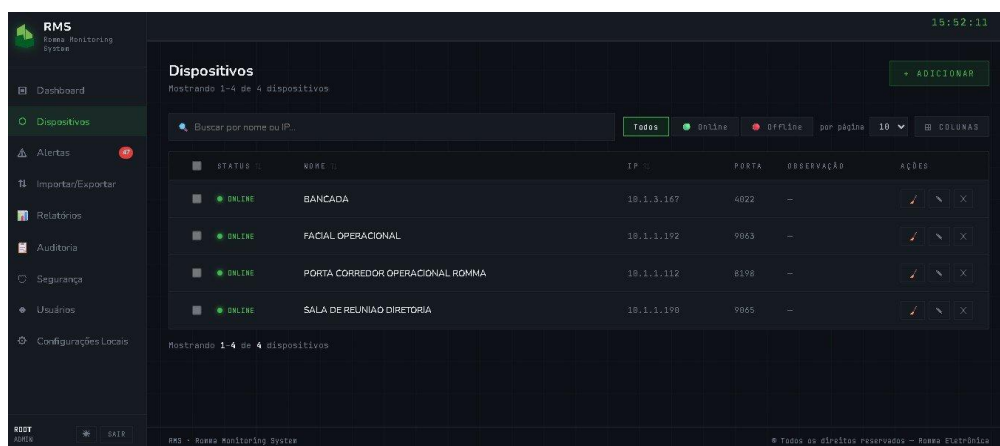


Figura 4 — Lista de dispositivos com status em tempo real

Exibe todos os equipamentos com status, IP, porta e observações. Use a busca e filtros Online/Offline para localizar dispositivos.

3.2 Cadastrando um Dispositivo

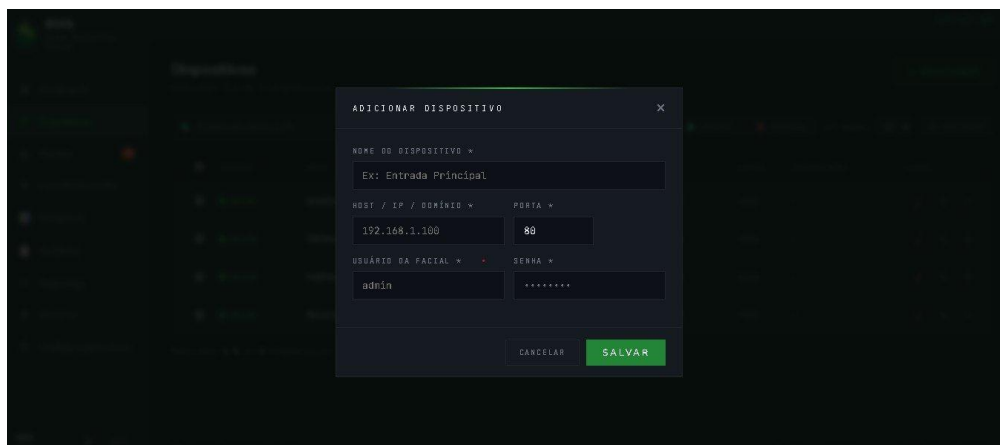


Figura 5 — Modal de adição de novo dispositivo

Como adicionar dispositivo

1. Clique em + ADICIONAR no canto superior direito
2. Preencha o Nome do Dispositivo (ex: Entrada Principal)
3. Informe o Host/IP do dispositivo (ex: 192.168.1.100)
4. Informe a Porta (padrão: 80)
5. Informe o Usuário e Senha do equipamento
6. Clique em SALVAR

3.3 Editando um Dispositivo

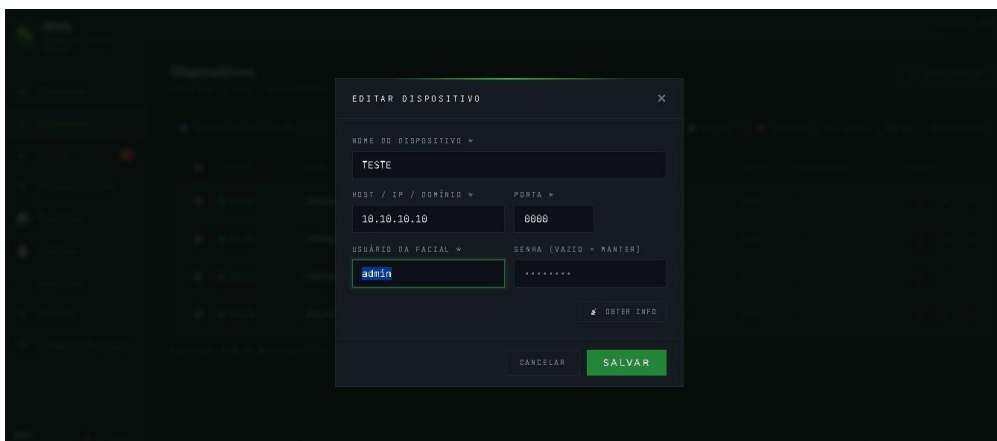


Figura 6 — Modal de edição com botão Obter Info

Clique no ícone de edição ✎. O botão "Obter Info" busca automaticamente o endereço MAC do dispositivo. Deixe a Senha em branco para manter a atual.

3.4 Limpando o Cache

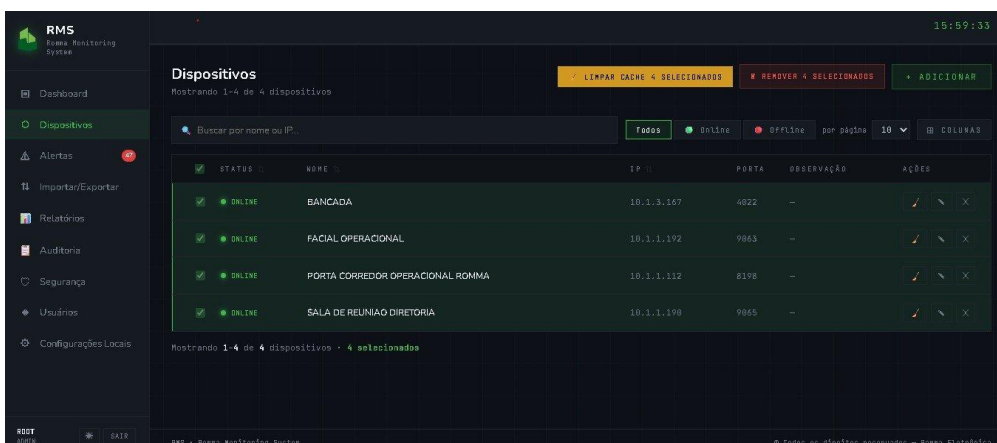


Figura 7 — Seleção múltipla para limpeza em massa

- Individual — Clique no ícone de vassoura na linha do dispositivo
- Em massa — Selecione vários com os checkboxes e clique em "LIMPAR CACHE X SELECIONADOS"

4. Alertas

4.1 Central de Alertas

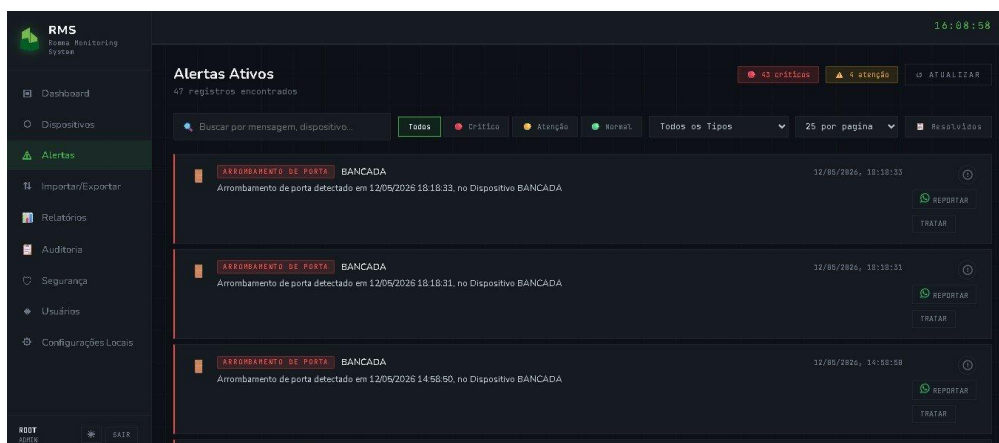


Figura 8 — Central de alertas com filtros e ações

4.2 Tipos de Alertas

Tipo	Severidade	WhatsApp Auto.
Dispositivo Offline	Crítico	Sim
Credencial de Coação	Crítico	Sim
Violação Física	Crítico	Sim
Arrombamento de Porta	Crítico	Sim
Queda de Energia	Crítico	Sim
Acesso Negado (múltiplas tentativas)	Crítico	Manual
Reinicialização	Atenção	Não
Queda de Rede	Atenção	Não

4.3 Tratando um Alerta

Como tratar um alerta

1. Localize o alerta na lista de Alertas Ativos
2. Clique no botão TRATAR
3. Descreva as ações tomadas
4. Clique em CONFIRMAR E TRATAR
5. O alerta move para a aba Resolvidos com seu nome e horário

4.4 Reportando via WhatsApp

Clique em REPORTAR (ícone WhatsApp) para enviar notificação imediata. Cada alerta pode ser reportado apenas uma vez para evitar duplicatas.

INFO: O Reporte só funcionará caso tenha um servidor para o envio de mensagens Whatsapp

5. Relatórios

Consolida alertas e eventos com filtros avançados e exportação para CSV.

5.1 Filtros Disponíveis

Dispositivo	Todos ou um equipamento específico
Tipo de Ocorrência	Alertas, eventos, offline, acesso negado, etc.
Período	Últimas 24h, 7 dias, 30 dias, todo histórico ou datas personalizadas

5.2 Exportando para CSV

Como exportar

1. Configure os filtros desejados
2. Clique em Exportar CSV
3. O arquivo é baixado automaticamente
4. Abra no Excel, Google Sheets ou similar

Colunas exportadas: Data, Dispositivo, Tipo, Severidade, Mensagem, Status, Resolvido Em, Tratado Por, Ações Tomadas.

6. Auditoria

INFO: Disponível apenas para Administradores.

Registra todas as ações: logins, alterações de dispositivos e usuários, tratamento de alertas, bloqueios e desbloqueios de IP.

6.1 Principais Ações

- Login com Sucesso / Login Falhou / Login Bloqueado
- Dispositivo Criado / Editado / Removido
- Alerta Resolvido / Reportado
- Usuário Criado / Editado / Removido
- IP Desbloqueado / Whitelist Adicionado ou Removido

6.2 Filtros

Busque por usuário ou filtre por tipo de ação. Clique em Ver (🔍) para detalhes completos incluindo IP e navegador.

7. Usuários

INFO: Disponível apenas para Administradores.

7.1 Criando um Usuário

Como criar usuário

1. Acesse Usuários no menu lateral
2. Clique em + NOVO USUÁRIO
3. Informe nome de usuário, perfil e senha
4. Clique em CRIAR

7.2 Remoção de Usuário

Ao remover um usuário, qualquer sessão ativa é encerrada imediatamente, independentemente do token ainda estar válido.

7.3 Política de Senhas

O admin. protegido configura em Configurações > Segurança: comprimento mínimo (4, 6, 8 ou 12 caracteres), maiúscula, número e caractere especial.

8. Segurança

INFO: Disponível apenas para Administradores.

8.1 Bloqueio Automático

1 — Leve	5 tentativas em 1 hora: bloqueio por 5 minutos
2 — Moderado	10 tentativas em 1 hora: bloqueio por 30 minutos
3 — Permanente	15 tentativas em 1 hora: bloqueio permanente

INFO: Caso tenha um servidor configurado para Whatsapp, um alerta é enviado automaticamente ao bloquear um IP.

8.2 Abas da Tela de Segurança

- IPs Bloqueados — Desbloquear IP ou apenas o usuário vinculado
- Usuários Bloqueados — Desbloquear usuário independente do IP
- Lista Negra — IPs bloqueados permanentemente (somente admin. protegido)
- Whitelist — IPs confiáveis que nunca serão bloqueados automaticamente

9. Configurações

9.1 Interface do Usuário

Inatividade	Encerra sessão após 15, 30 ou 60 min sem uso
Tema	Modo Escuro ou Claro
Itens por Página	Padrão de registros (10, 25, 50 ou 100)

9.2 Configurações do Sistema (Admin. Protegido)

Limiar de Negadas	Quantidade de acessos negados em 2 min para alertar (2/3/5/10)
Política de Senhas	Comprimento mínimo, maiúscula, número, caractere especial
URL da API WhatsApp	Endereço do servidor
Instância WhatsApp	Nome da instância configurada
API Key	Chave de autenticação do serviço
Números de Contato	Um por linha, formato: 55DDD9XXXXXXXXX

9.3 Templates de Mensagem WhatsApp

{dispositivo}	Substituído pelo nome do dispositivo
{data}	Data e hora no formato DD/MM/AAAA HH:MM:SS

Templates disponíveis: Dispositivo Offline, Credencial de Coação, Violação Física e Arrombamento de Porta.
Deixe em branco para usar o template padrão (com emojis).