

Panduan Broadcast Aman

WA Gateway - cara mengirim pesan ke banyak nomor tanpa membuat nomor pengirim diblokir WhatsApp

Diperbarui: 14 September 2026

1. Cara Broadcast

Broadcast dikirim lewat satu endpoint yang sama dengan kirim pesan tunggal, bedanya field "target" berisi banyak nomor sekaligus, dipisah koma. Endpoint ini butuh header X-API-Key (bukan X-Admin-Key dashboard).

```
POST /send
Header: X-API-Key: <api key milik akun/sistem pemanggil>
Content-Type: application/json

Body:
{
  "device": "dev_ab12cd34",
  "target": "628111111111|Budi|Rapat jam 10,628222222222|Siti|Rapat jam 10",
  "message": "Halo {name}, {var1}. Mohon konfirmasi kehadiran.",
  "delay_min_detik": 8,
  "delay_max_detik": 20
}
```

Format field "target"

Format mirip Fonnte: satu baris per nomor, dipisah koma antar nomor, dan dipisah "|" untuk nomor|nama|variabel1.

- nomor: wajib, nomor WhatsApp tujuan (contoh 628111111111, tanpa tanda +).
- nama: opsional, mengganti {name} di template pesan.
- var1: opsional, mengganti {var1} di template pesan (bebas isinya, misal jam rapat, nomor invoice, dll).

Kirim terjadwal (opsional)

Kalau field "schedule" diisi unix timestamp (detik) di masa depan, pesan TIDAK langsung dikirim -- masuk antrian dan baru diproses saat waktunya tiba (dicek tiap 5 detik oleh gateway). Kalau tidak diisi (atau sudah lewat), pesan langsung dikirim saat itu juga.

Membagi target dalam jumlah besar (batching)

Satu request "/send" dibatasi maksimal 25 nomor tujuan (bisa diubah lewat MAX_TARGET_PER_REQUEST di .env). Kalau daftar penerima lebih dari itu, pecah jadi beberapa request/batch dari sisi pemanggil (n8n, script, dsb) -- misal 200 penerima menjadi 8 request berisi 25 nomor.

Catatan penting: batas 25 ini hanya membatasi JUMLAH NOMOR PER REQUEST, bukan jumlah request per menit. Kalau memecah 200 nomor jadi 8 request dan mengirim ke-8 request itu SEKALIGUS dalam beberapa detik, jeda anti-blokir per nomor tetap berjalan (baca bagian 2), tapi sebaiknya beri jarak antar BATCH juga (contoh 1-2 menit antar batch), jangan menembakkan semua batch dalam waktu bersamaan.

2. Proteksi Anti-Blokir yang Sudah Berjalan di Gateway

a) Jeda acak antar nomor

Setelah kirim ke satu nomor, gateway menunggu waktu ACAK (bukan tetap) sebelum mengirim ke nomor berikutnya, meniru pola manusia mengetik dan mengirim satu per satu -- ini yang paling penting untuk mencegah akun ditandai bot.

- Default saat ini di server (.env): 10-20 detik.
- Bisa dioverride per-request lewat `delay_min_detik` / `delay_max_detik` di body POST /send atau dari n8n.

TEMUAN & PERBAIKAN: sebelumnya, `override delay_min_detik/delay_max_detik` dari luar TIDAK ada batas bawahnya -- kalau ada yang mengirim `delay_min_detik: 0` (sengaja atau salah konfigurasi workflow), jeda anti-blokir bisa MATI TOTAL. Ini sudah diperbaiki: sekarang berapa pun yang diminta dari luar, jeda TIDAK PERNAH lebih cepat dari 8 detik (bisa diubah lewat `JEDA_MIN_MUTLAK_DETİK` di .env). Ini pagar terakhir supaya insiden blokir kemarin tidak terulang meski ada salah konfigurasi di sisi pemanggil.

b) Kuota harian per nomor (device)

Setiap device/nomor pengirim punya batas jumlah pesan terkirim per hari (default 100, field "batas_harian", direset otomatis tiap pergantian hari WIB). Kalau broadcast yang diminta melebihi sisa kuota hari itu, gateway MENOLAK request itu (kirim langsung) atau MENUNDA-nya otomatis ke hari berikutnya (kirim terjadwal/antrean) -- bukan memaksakan kirim.

Kuota ini bisa diatur per device lewat dashboard admin (PATCH /admin/devices/:id, field batas_harian) sesuai umur & kepercayaan nomor tersebut -- nomor baru sebaiknya diberi kuota kecil dulu (lihat bagian 3, "warming up").

c) Validasi nomor tujuan sebelum kirim

Sebelum mengirim, gateway mengecek dulu apakah nomor tujuan benar-benar terdaftar di WhatsApp (lewat `onWhatsApp()`). Kalau sudah pasti TIDAK terdaftar, gateway TIDAK memaksakan kirim -- langsung ditandai gagal. Ini mengurangi jumlah pesan "bounce" ke nomor mati/salah, yang juga ikut memengaruhi reputasi nomor pengirim di mata WhatsApp.

d) Maksimal target per request

Dibatasi 25 nomor per panggilan /send (lihat bagian 1) supaya satu request tidak bisa dipakai untuk "menembak" ratusan nomor sekaligus tanpa jeda yang wajar.

3. Rekomendasi Supaya Tetap Aman (Tanggung Jawab Pemanggil/Admin)

Sistem sudah punya pagar teknis di atas, tapi keamanan broadcast WhatsApp juga bergantung pada POLA PEMAKAIAN. Ikuti rekomendasi berikut, terutama karena nomor ini PERNAH terkena blokir:

- Jangan pakai delay lebih cepat dari default (10-20 detik) untuk nomor yang belum lama "pulih" dari blokir atau nomor baru. Kalau perlu lebih cepat karena volume besar, tambah JUMLAH DEVICE (nomor pengirim) yang dipakai bergantian, bukan mempercepat jeda satu nomor.
- "Warming up" nomor baru: mulai dengan volume kecil (puluhan pesan/hari) selama 1-2 minggu pertama, naikkan bertahap. Atur lewat batas_harian per device di dashboard, jangan langsung set besar.
- Beri jarak antar BATCH, bukan cuma antar nomor dalam satu batch -- kalau broadcast dipecah jadi beberapa request (bagian 1), beri jeda beberapa menit antar batch, bukan menembak semua batch bersamaan.
- Isi pesan sebaiknya bervariasi (pakai {name}/{var1}), hindari mengirim teks yang 100% identik ke ratusan nomor dalam waktu singkat -- pesan yang sangat seragam dan cepat adalah pola khas spam di mata sistem deteksi WhatsApp.
- Pastikan penerima memang pernah/berhak dihubungi (bukan nomor hasil scraping/beli list) -- laporan "spam" dari penerima (ditekan tombol Report) jauh lebih berbahaya bagi reputasi nomor dibanding kecepatan kirim itu sendiri.
- Pantau notifikasi admin WhatsApp dari gateway ini (perlu nomor admin diisi di dashboard /admin > Pengaturan) supaya begitu ada device terputus/butuh scan ulang, admin langsung tahu -- bukan baru sadar setelah banyak pesan gagal terkirim.
- Cek dashboard /admin secara berkala untuk melihat status tiap device (terhubung/terputus) dan jumlah terkirim hari ini vs kuota, terutama sebelum menjalankan broadcast besar.

Ringkasan: apakah broadcast ini sudah aman?

Dengan perbaikan pagar minimum jeda (poin 2a) ditambah kuota harian, validasi nomor, dan batas jumlah target per request yang SUDAH berjalan di kode, risiko blokir akibat KESALAHAN TEKNIS/konfigurasi sudah ditutup. Sisanya adalah disiplin pemakaian: jaga kecepatan wajar, jangan kirim ke nomor yang tidak relevan, dan naikkan volume secara bertahap -- ini yang paling menentukan apakah nomor akan diblokir lagi atau tidak, bukan hanya kode.