interweb

Generated on 21/10/2026 17:23

KNOWLEDGE BASE · PUBLIC DOCUMENT

Securing Evolution API: key, HTTPS and the open port

WhatsApp & APIs

CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-994	v2026.10.10	Mozambique · English

Interweb Mozambique
RLX Holdings, S.A. · Group RLX Holdings
Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

https://www.meu.interweb.co.mz/knowledgebase/994

Securing Evolution API: key, HTTPS and the open port

WhatsApp & APIs · Created on **October 10, 2026** · 3 min read



An exposed Evolution API is an open door to your WhatsApp number: whoever reaches it and holds the key sends messages in your name. You protect it with four things: a **strong, secret key**, **HTTPS** in front, the **right ports** closed and **nothing extra** exposed (database, Redis). The order matters: do them before linking a number you care about.

Step by step

1. **A random key.** `AUTHENTICATION_API_KEY` should be long and generated at random, for example with `openssl rand -hex 32`. Never a word, never the one from the example. Keep it in a password manager.

2. **Never publish it.** It does not go in repositories, screenshots, chats or help requests. If it leaked, change it in the settings file, restart and update everywhere that uses it.

3. **Put a reverse proxy with HTTPS in front**, on a domain or subdomain of yours. See **Nginx in front of a container** and **HTTPS for a container**. Without HTTPS the key travels in the clear.

4. **Let the API listen on the server itself only.** In the compose file the published port can be tied to the `127.0.0.1` address, so that only the proxy reaches it. Then the server's address plus the API port stops answering from outside.

5. **Do not publish the database or Redis.** They only need to see each other inside the Docker network. A database with an open port is a well-known target.

6. **Restrict SSH access** and keep the system updated. See **keeping your VPS secure**.

Docker gets around many firewalls.
When you publish a port, Docker edits the network rules itself, and an ordinary firewall may not hide it. Do not assume the port is closed: confirm it from outside, from another computer. See **ports and firewall on a VPS**.

What each measure protects against

Measure	Against what
A strong key	Anyone who guesses or finds the default one.
HTTPS	Anyone listening on the network between your server and whoever calls the API.
A local-only port	Anyone scanning the internet for open ports.
A closed database	Anyone trying to get straight at the data and the sessions.
A secret on the webhook	Anyone who finds your receiver's address and invents messages.

After installing

1. **Test from outside.** From a computer that is not the server, confirm that the API port, the database port and the Redis port do not answer, and that the domain with HTTPS does.
2. **Test the key.** A request with no key, or the wrong one, must be refused.
3. **Review the logs** now and then. Requests you do not recognise, from odd addresses, are the warning.

The risk is not only technical. Whoever has the key has the number, and a number used to send junk to others is a banned number. For context, see **the risks of WhatsApp for business**. VPS security is yours, as the **Support Policy** explains.

NEED A HAND?
Want help choosing the server this will run on?
Open a support ticket →

SEE ALSO

- **Keeping your VPS secure: the six that matter**
- **Ports and firewall on a VPS**
- **The Evolution API settings that matter**

interweb

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-MZ-KB-994 · v2026.10.10 · Generated on 21/10/2026 17:23