interweb

Gerado a 15/11/2026 00:27

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Proteger a Evolution API: chave, HTTPS e a porta aberta

Evolution API

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-976	v2026.10.28	Angola · Português

Interweb Angola
RLX Angola, Lda. · Grupo RLX Holdings
NIF 500 260 5724 · Matrícula 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/976

Proteger a Evolution API: chave, HTTPS e a porta aberta

Evolution API · Criado em **10 de outubro de 2026** · Atualizado em **28 de outubro de 2026** · 3 min de leitura



Uma Evolution API exposta é uma porta aberta para o seu número de WhatsApp: quem a alcançar e tiver a chave envia mensagens em seu nome. Protege-se com quatro coisas: uma **chave forte e secreta**, **HTTPS** à frente, as **portas certas** fechadas e **nada a mais** exposto (base de dados, Redis). A ordem importa: faça-as antes de ligar um número que lhe interesse.

Passo a passo

1. **Chave aleatória.** A `AUTHENTICATION_API_KEY` deve ser longa e gerada ao acaso, por exemplo com `openssl rand -hex 32`. Nunca uma palavra, nunca a do exemplo. Guarde-a num gestor de senhas.

2. **Nunca a publique.** Não vai para repositórios, capturas de ecrã, conversas ou pedidos de ajuda. Se vazou, troque-a no ficheiro de definições, reinicie e actualize todos os sítios que a usam.

3. **Ponha um proxy inverso com HTTPS à frente**, num domínio ou subdomínio seu. Veja **Nginx à frente de um contentor** e **HTTPS para um contentor**. Sem HTTPS, a chave viaja às claras.

4. **Deixe a API ouvir só no próprio servidor.** No compose, a porta publicada pode ficar presa ao endereço `127.0.0.1`, e só o proxy lhe chega. Assim, o endereço do servidor com a porta da API deixa de responder de fora.

5. **Não publique a base de dados nem o Redis.** Eles só têm de se ver dentro da rede do Docker. Uma base de dados com a porta aberta é um alvo conhecido.

6. **Limite o acesso por SSH** e mantenha o sistema actualizado. Veja **manter o VPS seguro**.

O Docker contorna muitas firewalls.
Ao publicar uma porta, o Docker mexe ele próprio nas regras de rede, e uma firewall comum pode não a esconder. Não assuma que a porta está fechada: confirme-o de fora, de outro computador. Veja **portas e firewall num VPS**.

O que protege cada medida

Medida	Contra quê
Chave forte	Quem adivinha ou encontra a chave por defeito.
HTTPS	Quem escuta a rede entre o seu servidor e quem chama a API.
Porta só local	Quem varre a internet à procura de portas abertas.
Base de dados fechada	Quem tenta entrar directamente nos dados e nas sessões.
Segredo no webhook	Quem descobre o endereço do seu receptor e inventa mensagens.

Depois de instalar

1. **Teste de fora.** A partir de um computador que não seja o servidor, confirme que a porta da API, a da base de dados e a do Redis não respondem, e que o domínio com HTTPS responde.
2. **Teste a chave.** Um pedido sem chave, ou com a chave errada, tem de ser recusado.
3. **Reveja os registos** de vez em quando. Pedidos que não reconhece, vindos de endereços estranhos, são o aviso.

O risco não é só técnico. Quem tem a chave tem o número, e um número usado para enviar lixo a outros é um número bloqueado. Para o contexto, veja **os riscos do WhatsApp para empresas**. A segurança do VPS é sua, como explica a **Política de Suporte**.

PRECISA DE AJUDA?

Quer ajuda a escolher o servidor onde isto vai correr?

Abrir um pedido de suporte →

VEJA TAMBÉM

- **Manter o VPS seguro: os seis que importam**
- **Portas e firewall num VPS**
- **As definições da Evolution API que interessam**

interweb

Interweb Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF	500 260 5724
MATRÍCULA	26464-25/250724
SEDE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACTOS	info@interweb.ao · +244 942 011 191 · www.interweb.ao
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

Versão online deste documento

RLX-AO-KB-976 · v2026.10.28 · Gerado a 15/11/2026 00:27